Easy Intruder Deduction Problems with Homomorphisms

Stéphanie Delaune

France Télécom, Division R&D – LSV, CNRS & ENS de Cachan – France

Abstract

We present complexity results for the verification of security protocols. Since the perfect cryptography assumption is unrealistic for cryptographic primitives with visible algebraic properties, we extend the classical *Dolev-Yao* model by permitting the intruder to exploit these properties. More precisely, we are interested in theories such as *Exclusive or* and *Abelian groups* in combination with the homomorphism axiom. We show that the intruder deduction problem is in PTIME in both cases, improving the EXPTIME complexity results presented in [10].

Key words: automatic theorem proving, formal methods, security protocols

1 Introduction

In security protocol analysis, the knowledge of an attacker is often described in terms of deduction: Given some messages T and a message s, can the intruder deduce s from T? This problem, called the *intruder deduction problem*, corresponds to the security decision problem in presence of an eavesdropper and is a cornerstone for the verification problem and for the search of attacks.

This deduction problem depends on the equational theory that governs the function symbols appearing in messages. In several works, the underlying cryptographic primitives are based on the *Dolev-Yao* model [8] which may be too strong in some situations. Recently, a number of results [7] have been obtained for including algebraic properties by the means of equational theories.

In this paper, we are interested in Associative and Commutative (AC) theories such as *Exclusive or* (ACUN) and *Abelian groups* (AG) in combination with

Email address: delaune@lsv.ens-cachan.fr (Stéphanie Delaune).

the homomorphism axiom (h). Some protocols relying on these algebraic properties are described in [7]: Bull's protocol, Wired Equivalent Privacy (WEP) protocol... For instance, in the WEP protocol, a checksum function having the homomorphism property over an (ACUN) symbol is used. Another well-known example is the TMN protocol [15] on which an attack, due to Simmons, makes use of the homomorphic property of RSA encryption. Such a protocol, in which RSA encryption is only used with the public key of the server, can be modelled in our settings assuming that the decryption key of the server is a trusted key. The homomorphism property is also crucial in the field of electronic voting protocols [3].

In [1], the authors state a general decidability result for the intruder deduction problem, by providing some hypotheses under which the deduction problem is decidable. However, they do not give any complexity result and it seems it is difficult to check that a particular theory satisfies the hypotheses. In this paper, we show that the intruder deduction problem in the equational theory ACUNh (resp. AGh) is decidable in PTIME, improving the EXPTIME complexity results of [10]. The techniques used are rather similar. Nevertheless, the introduction of a rule scheme to treat $\oplus$ and h at the same time allows us to obtain simpler proofs and better complexity results.

2 Intruder Deduction Problem

2.1 Basic Definitions

We use classical notation and terminology on terms, unification and rewrite systems. We write $\mathcal{T}(\mathcal{F}, \mathcal{X})$ for the set of terms built over the finite (ranked) alphabet $\mathcal{F}$ of function symbols and the set $\mathcal{X}$ of variables. $\mathcal{T}(\mathcal{F}, \emptyset)$ is also written $\mathcal{T}(\mathcal{F})$. The set of positions of t is written $\mathcal{O}(t)$. The subterm of t at position $p \in \mathcal{O}(t)$ is written $t|_p$. The term obtained by replacing $t|_p$ with u is denoted $t[u]_p$. The set of variables occurring in t is noted $vars(t)$.

A *substitution* σ is a mapping from a finite subset of $\mathcal{X}$, called its domain and written $dom(\sigma)$, to $\mathcal{T}(\mathcal{F}, \mathcal{X})$. Substitutions are extended to endomorphisms of $\mathcal{T}(\mathcal{F}, \mathcal{X})$ as usual. We use a postfix notation for their application. If E is a set of equations (unordered pair of terms), we note $sig(\mathsf{E})$ for the set of function symbols occurring in E and by $=_\mathsf{E}$ the least congruence on $\mathcal{T}(\mathcal{F}, \mathcal{X})$ such that $u\sigma =_\mathsf{E} v\sigma$ for all pairs $u = v \in E$ and substitutions σ. An E-*context* is a λ-term $\lambda x_1, \ldots, x_n.t$ with $t \in \mathcal{T}(sig(\mathsf{E}), \{x_1, \ldots, x_n\})$, also written $t[x_1, \ldots, x_n]$. The application of $t[x_1, \ldots, x_n]$ to arguments $u_1, \ldots, u_n$ is written $t[u_1, \ldots, u_n]$.

A *term rewriting system* (TRS) is a finite set of *rewrite rules* $l \to r$ where

$l \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ and $r \in \mathcal{T}(\mathcal{F}, vars(l))$. Given a TRS $\mathcal{R}$ and a set of equations E, the relation $\rightarrow_{\mathcal{R}/\mathsf{E}}$ (*rewriting modulo* E) is defined as follows: $s \rightarrow_{\mathcal{R}/\mathsf{E}} t$ if and only if $s =_{\mathsf{E}} u[l\sigma]_p$ and $u[r\sigma]_p =_{\mathsf{E}} t$, for some context u, position p in u, rule $l \rightarrow r \in \mathcal{R}$, and substitution σ. The rewrite system $\mathcal{R}/\mathsf{E}$ is *strongly terminating* if there is no infinite chains $t_1 \rightarrow_{\mathcal{R}/\mathsf{E}} t_2 \rightarrow_{\mathcal{R}/\mathsf{E}} \ldots$ and it is *locally confluent* if for every 3 terms t, s_1 and s_2 such that $t \rightarrow_{\mathcal{R}/\mathsf{E}} s_1$, $t \rightarrow_{\mathcal{R}/\mathsf{E}} s_2$, there exists a term s such that $s_1 \xrightarrow{*}_{\mathcal{R}/\mathsf{E}} s$, $s_2 \xrightarrow{*}_{\mathcal{R}/\mathsf{E}} s$ where $\xrightarrow{*}_{\mathcal{R}/\mathsf{E}}$ is the reflexive and transitive closure of $\rightarrow_{\mathcal{R}/\mathsf{E}}$. A rewrite system $\mathcal{R}/\mathsf{E}$ is said to be E-*convergent* if it is both strongly terminating and locally confluent. A term t is in *normal form* (w.r.t. $\rightarrow_{\mathcal{R}/\mathsf{E}}$) if there is no term s such that $t \rightarrow_{\mathcal{R}/\mathsf{E}} s$. If $t \xrightarrow{*}_{\mathcal{R}/\mathsf{E}} s$ and s is in normal form then we say that s is a normal form of t.

2.2 Dolev-Yao Model Extended with an Equational Theory

The most widely used deduction relation representing the deduction abilities of an intruder is often referred to as the Dolev-Yao model [8]. In addition, we give to the intruder the power to use equational reasoning modulo a set E of equational axioms. The resulting set of deduction rules for symmetric encryption is given in Figure 1. It is not difficult to design a similar deduction system for asymmetric encryption and to extend our results to this inference system.

Axiom (A) $\dfrac{u \in T}{T \vdash_{\mathsf{E}} u}$ Compose (C) $\dfrac{T \vdash_{\mathsf{E}} u_1 \ \ldots \ T \vdash_{\mathsf{E}} u_n}{T \vdash_{\mathsf{E}} f(u_1, \ldots, u_n)}$ with $f \in \mathcal{F}$

Unpairing (UL) $\dfrac{T \vdash_{\mathsf{E}} \langle u, v\rangle}{T \vdash_{\mathsf{E}} u}$ Decryption (D) $\dfrac{T \vdash_{\mathsf{E}} \{u\}_v \quad T \vdash_{\mathsf{E}} v}{T \vdash_{\mathsf{E}} u}$

Unpairing (UR) $\dfrac{T \vdash_{\mathsf{E}} \langle u, v\rangle}{T \vdash_{\mathsf{E}} v}$ Equality (Eq) $\dfrac{T \vdash_{\mathsf{E}} u \quad u =_{\mathsf{E}} v}{T \vdash_{\mathsf{E}} v}$

Fig. 1. Dolev-Yao Model Extended with an Equational Theory

The intended meaning of a *sequent* $T \vdash_{\mathsf{E}} u$ is that the intruder is able to deduce the term $u \in \mathcal{T}(\mathcal{F})$ from the finite set of terms $T \subseteq \mathcal{T}(\mathcal{F})$. As in the standard Dolev-Yao model, the intruder knows any term that he has previously observed (A), he can compose new terms (C) from known terms, he can also decompose pairs (UL, UR) and decrypt ciphertexts, providing that he can deduce the decryption key (D). Finally, we relax the *perfect cryptography assumption* through the rule (Eq) allowing the intruder to exploit the algebraic properties of cryptographic primitives.

Definition 1 *(E-proof) An E-proof P of $T \vdash_{\mathsf{E}} u$ is a tree such that:*

- *every leaf of P is labeled with an expression of the form "$v \in T$",*
- *for every node labeled with a sequent $T \vdash_{\mathsf{E}} v$ having n sons labeled with $T \vdash_{\mathsf{E}} s_1, \ldots, T \vdash_{\mathsf{E}} s_n$, there is an instance of an inference rule with conclusion $T \vdash_{\mathsf{E}} v$ and hypotheses $T \vdash_{\mathsf{E}} s_1, \ldots, T \vdash_{\mathsf{E}} s_n$. We say that P ends with this instance if the node is the root of P,*
- *the root is labeled with $T \vdash_{\mathsf{E}} u$.*

Assume that the equational theory E is fixed. The problem whether an intruder can gain certain information s from a set of knowledge T, *i.e.* whether there is an E-proof of $T \vdash_{\mathsf{E}} s$, is called the *intruder deduction problem* (ID).

INPUT: a finite set of terms T, a term s (the secret).
OUTPUT: Does there exist an E-proof of $T \vdash_{\mathsf{E}} s$?

In this paper, we focus on the theories ACh, ACUNh, AGh, *i.e.* the homomorphism axiom (h), $h(x \oplus y) = h(x) \oplus h(y)$, in combination with:

(1) Associativity, Commutativity (AC): $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, $x \oplus y = y \oplus x$.
(2) Exclusive or (ACUN): (AC), Unit (U): $x \oplus 0 = x$, Nilpotence (N): $x \oplus x = 0$.
(3) Abelian groups (AG): (AC), Unit (U): $x \oplus 0 = x$, Inverse (Inv): $x \oplus I(x) = 0$.

3 PTIME Decision Procedures

The proof system given in Figure 1 is not appropriate for automated proof search: the rule (Eq) allows equational reasoning at any moment of a proof. To define a more effective model, we represent the equational theory by an AC-convergent rewrite system. In the case of ACh, we have just to orient from left to right (h). For ACUNh, we orient from left to right the equations (U), (N) and (h) and we add $h(0) \to 0$. For AGh, this can be achieved by orienting from left to right (U), (Inv) and (h) and by adding the rules in Figure 2.

$$I(x \oplus y) \to I(x) \oplus I(y) \qquad \begin{array}{ll} h(0) \to 0 & I(I(x)) \to x \\ I(0) \to 0 & h(I(x)) \to I(h(x)) \end{array}$$

Fig. 2. Rewriting Rules

Now, we omit the rule (Eq) and consider a variant of the deduction model which works on normal forms. After each step, the term obtained is reduced to its normal form. This new deduction system on *sequents* $T \vdash u$ consists in:

(1) the deduction rules $(\mathsf{A}, \mathsf{UL}, \mathsf{UR}, \mathsf{D})$ (where $\vdash_{\mathsf{E}}$ is replaced by $\vdash$),
(2) a restricted form of the rule (C), denoted by (C^-), where $\vdash_{\mathsf{E}}$ is replaced by $\vdash$ and the side condition is slightly more restrictive: $f \in \mathcal{F} \smallsetminus sig(\mathsf{E})$,

(3) and lastly, a rule scheme, denoted $(\mathsf{M_E})$:

$$\frac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]} \text{ with } C \text{ an } \mathsf{E}\text{-context}$$

Example 2 *If we consider the* ACUNh *theory, the inference below is an instance of the rule* $(\mathsf{M_E})$ *with* $C = x_1 \oplus h(x_1) \oplus h^2(x_1) \oplus h(x_2)$.

$$\frac{T \vdash a \oplus h(a) \qquad T \vdash b}{T \vdash a \oplus h^3(a) \oplus h(b)}$$

Equivalence modulo AC is easy to decide, so we omit the equality rule for AC and just work with equivalence classes modulo AC. The notion of *proof* in this inference system is similar to the notion of E-proof previously defined. The only difference is that nodes are labeled with sequents of the form "$T \vdash v$".

Since the equational theories studied in this paper do not interfere with the standard function symbols, *i.e.* $sig(\mathsf{E}) \cap \{\{\_\}_\_; \langle\_,\_\rangle\} = \emptyset$, we have:

Theorem 3 *Let T be a set of terms and u a term (in normal form). We have:*
$T \vdash u$ is derivable $\Leftrightarrow$ $T \vdash_{\mathsf{E}} u$ is derivable

PROOF. Given a proof of $T \vdash u$, we can easily find an E-proof of $T \vdash_{\mathsf{E}} u$ by inserting (Eq) steps. Conversely, given an E-proof of $T \vdash_{\mathsf{E}} u$, we can transform it by changing all $\vdash_{\mathsf{E}}$ into $\vdash$, normalizing all terms to the right of $\vdash$ and dropping all applications of (Eq). Note that an instance of (C) in the E-proof has to be seen (in the proof of $T \vdash u$) either as an instance of $(\mathsf{M_E})$ or of (C^-), depending on whether $f \in sig(\mathsf{E})$ or not. □

To show that (ID) is decidable in PTIME, we use the notion of *locality* introduced by McAllester [12]. As in [10], we need to establish:

(1) a locality result (Section 4) for the inference system $\vdash$: checking the existence of a proof of $T \vdash u$ amounts to checking the existence of a local proof involving only a polynomial number of terms,
(2) a one-step-deducibility result (Section 5) to ensure that we can test in PTIME whether a term is deducible in one-step from a set of terms by using an instance of one of the inference rules. The only critical rule is $(\mathsf{M_E})$.

The existence of a local proof of $T \vdash u$ can be checked in polynomial time by saturation of T with terms deducible in one-step. Thanks to locality, the number of iteration to obtain a saturated set is bounded by the number of terms that can be involved in a local proof. This yields a PTIME algorithm.

In the remainder, we study locality and provide algorithms for one-step deducibility of $(\mathsf{M_E})$ in our three cases. For ACh, (ID) is NP-complete as mentioned in [10] without proof. Anyway, a reduction from BIN PACKING entails that solving linear Diophantine equations over $\mathbb{N}$ is strongly NP-complete. Then, it is easy to see that (ID) is NP-complete as well. Hence, there is no hope of improving the complexity result of [10] in this case.

Theorem 4 (Main Result) (ID) *is PTIME-complete for* ACUNh *and* AGh*.*

The PTIME-hardness is due to the Dolev-Yao part of the model and can be proved by a reduction from HORNSAT.

4 Locality

A term t is *headed* with f if t is of the form $f(u)$ for some term u. A term t is *standard* if it is not headed with any $f \in sig(\mathsf{E})$.

Definition 5 *P is a* decomposition proof *of $T \vdash u$ if P ends either with an instance of a decomposition rule (i.e.* (A, UL, UR, D)*), or with an instance of* $(\mathsf{M_E})$ *where u is a standard term.*
The size *of a proof P, denoted by $|P|$, is the number of nodes in P. A proof P of $T \vdash u$ is minimal if there is no proof P' of $T \vdash u$ such that $|P'| < |P|$.*

Definition 6 *Let t be a term, $t = C[t_1, \ldots, t_n]$ for some standard terms $t_1, \ldots, t_n$ and an E-context C. The set $Fact_{\mathsf{E}}(t)$ of* factors *of t is defined by $Fact_{\mathsf{E}}(t) = \{t_1, \ldots, t_n\}$. The set $St_{\mathsf{E}}(t)$ of* subterms *of t is the smallest set s.t.:*

- *$t \in St_{\mathsf{E}}(t)$,*
- *if $f(t_1, \ldots, t_n) \in St_{\mathsf{E}}(t)$ is standard then $t_1, \ldots t_n \in St_{\mathsf{E}}(t)$,*
- *if $s \in St_{\mathsf{E}}(t)$ is not standard then $Fact_{\mathsf{E}}(s) \subseteq St_{\mathsf{E}}(t)$.*

For example, let $t_1 = h^2(a) \oplus b \oplus c$ and $t_2 = h(\langle a, b\rangle) \oplus c$. We have $St_{\mathsf{E}}(t_1) = \{t_1, a, b, c\}$ and $St_{\mathsf{E}}(t_2) = \{t_2, \langle a, b\rangle, a, b, c\}$. These notations are extended as expected to sets of terms.

Lemma 7 *Let T be a set of terms and u a term (in normal forms) such that $0 \in T$. A minimal proof P of $T \vdash u$ only contains terms in $St_{\mathsf{E}}(T \cup \{u\})$.*

PROOF. This is similar to proofs in [6]. By induction on P, we prove that:

(1) P only contains terms in $St_{\mathsf{E}}(T \cup \{u\})$,
(2) if P is a decomposition proof, then P contains only terms in $St_{\mathsf{E}}(T)$.

We consider all possible cases for the last inference rule of P and we conclude by applying the induction hypothesis (1) or (2). The most interesting case is when the last inference is $(\mathsf{M_E})$. We have the following derivation:

$$\frac{P_1\left\{\ \dfrac{\cdots}{T \vdash u_1}\right. \qquad \cdots \qquad P_n\left\{\ \dfrac{\cdots}{T \vdash u_n}\right.}{T \vdash C[u_1,\ldots,u_n]}\ (\mathsf{M_E})$$

By (1), each P_i only contains terms in $St_{\mathsf{E}}(T \cup \{u_i\})$. Moreover, if u_i is not a standard term, P_i is necessarily a decomposition proof (by minimality of P, we could otherwise merge the last rule with $(\mathsf{M_E})$) and we can apply (2). Now, we have to deal with the u_i that are standard. Either $u_i \in St_{\mathsf{E}}(u)$, or u_i is canceled out by another term. In the second case, since P is minimal, u_i must be canceled out by some term u_j with $j \neq i$ that is not standard (otherwise the same term would appear twice in the premises, which contradicts the minimality of P). Hence $u_i \in St_{\mathsf{E}}(T)$. Therefore P only contains terms in $St_{\mathsf{E}}(T \cup \{u\})$. Moreover, if we assume that u is a standard term, we have $u \in St_{\mathsf{E}}(u_i)$ for some u_i that is not standard. Hence $u_i \in St_{\mathsf{E}}(T)$ and P only contains terms in $St_{\mathsf{E}}(T)$. □

5 One-Step Deducibility

We now investigate the complexity of one-step deducibility for the rule $(\mathsf{M_E})$. Our method is inspired by the technique used in [13] to solve unification problems in monoidal theories and has also been successfully used to solve one-step deducibility for a simple scheme rule (see [5,10] for instance). The algorithm described below reduces one-step deducibility into the solvability of a system of linear equations over $\mathbb{N}[\mathrm{X}]$, $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]$ or $\mathbb{Z}[\mathrm{X}]$ (depending on E).

Input: a finite set $T = \{t_1, \ldots t_n\}$ of terms and a term s (in normal forms).

Output: Let $\mathcal{B} = \{b \mid b \in \mathit{Fact}_{\mathsf{E}}(T \cup \{s\})\}$ and $m = |\mathcal{B}|$. The output is a matrix A of size $n \times m$, a vector b of size m, over $\mathbb{N}[\mathrm{X}]$ (resp. $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]$, $\mathbb{Z}[\mathrm{X}]$) such that s is one-step deducible by $(\mathsf{M_E})$ with $\mathsf{E} = \mathsf{ACh}$ (resp. ACUNh, AGh) if and only if there exists $Y \in \mathbb{N}[\mathrm{X}]^n$ (resp. $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]^n$, $\mathbb{Z}[\mathrm{X}]^n$) such that $A \cdot Y = b$.

Algorithm: Let $\mathcal{T}_{\mathcal{B}} = \{t \in \mathcal{T}(\mathcal{F}) \mid \mathit{Fact}_{\mathsf{E}}(t) \subseteq \mathcal{B}\}$. We write $\mathcal{B} = \{b_1, \ldots, b_m\}$. Let $\psi : \mathcal{T}_{\mathcal{B}} \to \mathbb{N}[\mathrm{X}]^m$ (resp. $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]^m$, $\mathbb{Z}[\mathrm{X}]^m$) be defined as follows:

- if $x = b_i$ then $\psi(x) = (0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is at the i^{th} position,
- if x is headed with h, then $x = h^k(u)$ and $\psi(x) = \psi(u) \cdot X^k$,
- if x is headed with $\oplus$, then $x = u_1 \oplus \cdots \oplus u_l$ and $\psi(x) = \sum_{1 \leq i \leq l} \psi(u_i)$,
- if x is headed with I (AGh case) , then $x = I(u)$ and $\psi(x) = -\psi(u)$.

The algorithm returns $A = (\psi(t_1), \ldots, \psi(t_n))$ and $b = \psi(s)$.

Lemma 8 *The algorithm described above is such that $A \cdot Y = b$ has a solution over $\mathbb{N}[\mathrm{X}]$ (resp. $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]$, $\mathbb{Z}[\mathrm{X}]$) if and only if there exists an E-context C such that $C[t_1, \ldots, t_n] =_{\mathsf{E}} s$ with $\mathsf{E} = \mathsf{ACh}$ (resp. ACUNh, AGh), i.e. s is one-step deducible from $t_1, \ldots, t_n$ by $(\mathsf{M}_{\mathsf{E}})$.*

PROOF. The function ψ, described above, associates to every term $t \in \mathcal{T}_{\mathcal{B}}$, an element $\psi(t)$ of $\mathbb{N}[\mathrm{X}]^m$ (resp. $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]^m$, $\mathbb{Z}[\mathrm{X}]^m$), and is such that: for any two terms t, t', we have $\psi(t) = \psi(t')$ if and only if $t =_{\mathsf{E}} t'$. In the same way, we define $\phi : \mathcal{C} \to \mathbb{N}[\mathrm{X}]^n$ (resp. $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]^n$, $\mathbb{Z}[\mathrm{X}]^n$) where $\mathcal{C} = \{C \mid C \text{ is an } \mathsf{E}\text{-context with } n \text{ variables}\}$. Note that ϕ is surjective and that we have: $\psi(C[t_1, \ldots, t_n]) = (\psi(t_1), \ldots, \psi(t_n)) \cdot \phi(C)$. It follows that:

$$\begin{aligned} \exists Y \text{ s.t. } A \cdot Y = b &\Leftrightarrow \exists Y \text{ s.t. } (\psi(t_1), \ldots, \psi(t_n)) \cdot Y = \psi(s) \\ &\Leftrightarrow \exists Y \text{ s.t. } (\psi(t_1), \ldots, \psi(t_n)) \cdot \phi(C) = \psi(s) \\ &\Leftrightarrow \exists C \text{ s.t. } \psi(C[t_1, \ldots, t_n]) = \psi(s) \\ &\Leftrightarrow \exists C \text{ s.t. } C[t_1, \ldots, t_n] =_{\mathsf{E}} s \end{aligned}$$

□

Example 9 *Let $T = \{a_1 \oplus h(a_1) \oplus h^2(a_1), a_2 \oplus h^2(a_1), h(a_2) \oplus h^2(a_1)\}$ and $s = a_1 \oplus h^2(a_1)$ with a_1, a_2 standard terms. We obtain:*

$$A = \begin{pmatrix} 1 + X + X^2 & X^2 & X^2 \\ 0 & 1 & X \end{pmatrix} \qquad b = \begin{pmatrix} 1 + X^2 \\ 0 \end{pmatrix}$$

The equation $A \cdot Y = b$ has a solution over $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]$: $Y = (1 + X, X, 1)$ is a solution. Hence, s is one-step deducible with $(\mathsf{M}_{\mathsf{E}})$ by using the E-context $x_1 \oplus h(x_1) \oplus h(x_2) \oplus x_3$ where x_i is used to denote the i^{th} term of T.

Different ways of measuring the size of a term t are conceivable. As in [10], we can consider the case where the size of t is defined as the number of positions in t. In [4], the size of t is defined by $|t|_d + \|t\|$ where $|t|_d$ is the number of nodes needed to represent the factors of t ($Fact_{\mathsf{E}}(t)$) as a tree with maximal sharing (DAG representation) and $\|t\|$ is the number of bits needed to represent the coefficients (*i.e.* polynomials) of the factors occurring in t. Anyway, the complexity results described below does not depend on it.

- over $\mathbb{N}[\mathrm{X}]$: it is easy to see that each component of a solution of $A \cdot Y = b$ has a degree smaller than the degree of b. The question of whether there exists Y such that $A \cdot Y = b$ can be reduced to solving a system of linear equations over $\mathbb{N}$. We obtain an NP decision procedure. The problem of solving linear Diophantine equations being strongly NP-complete, there is no hope to obtain a better theoretical complexity result.
- over $\mathbb{Z}/2\mathbb{Z}[\mathrm{X}]$: solvability of linear equations is known to be in PTIME [9].
- over $\mathbb{Z}[\mathrm{X}]$: a result (theorem 6.5 in [2]) shows that if a solution of $A \cdot Y = b$ exists, then it has such a solution the degrees of whose components is

polynomially bounded by both the degrees and the size of the coefficients that appear in A and b. The computable character of this bound reduces the problem to solving a large (but polynomial) system of linear equations over $\mathbb{Z}$. We obtain a PTIME decision procedure for the solvability of linear equations in $\mathbb{Z}[X]$ through a PTIME decision procedure over $\mathbb{Z}$ [14].

6 Conclusion

In this paper, PTIME algorithms allowing us to solve (ID) in ACUNh, AGh are proposed. The high complexity in [10] is essentially due to the fact that the authors treat $\oplus$ and h separately. Hence, it may be necessary (in their inference system) to build large intermediate terms which partially cancel out when combining them by $\oplus$. To establish their locality lemma, they have to consider a large set of terms. In this paper, the locality part is easy to prove thanks to the rule scheme $(\mathsf{M_E})$. The most complicated part is to establish one-step deducibility, but well-know algebraic results allow us to conclude.

We think that the technique is general enough to deal with some other monoidal theories [13] provided that algebraic techniques exist to solve equations over the corresponding semiring. For instance, considering several commuting homomorphisms symbols would return to work on polynomials with several indeterminates (one per homomorphism symbol). The case where the encryption distributes over the AC symbol, studied in [11], seems to be more complicated and can not be handled straightforwardly with this method.

Acknowledgment: I thank an anonymous referee for pointing out the NP-hardness proof of (ID) for (ACh). I am also particularly grateful to H. Comon-Lundh for his assistance, C. Picaronny for enriching discussions that contributed to this work and R. Treinen for his reading of a preliminary version of this paper. This work has been partly supported by the RNTL project PROUVÉ 03V360 and the ACI-SI Rossignol.

References

[1] M. Abadi and V. Cortier. Deciding knowledge in security protocols under (many more) equational theories. In *Proc. 18th IEEE Computer Security Foundations Workshop (CSFW'05)*, pages 62–76, Aix-en-Provence (France), 2005. IEEE Comp. Soc. Press.

[2] M. Aschenbrenner. Ideal membership in polynomial rings over the integers. *Journal of the American Mathematical Society*, 17:407–441, 2004.

[3] J. Benaloh. *Verifiable Secret Ballot Elections.* PhD thesis, Yale University, 1987.

[4] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with Diffie-Hellman exponentiation and product in exponents. In *Proc. 23rd Conf. Foundations of Software Technology and Theoretical Computer Science (FST&TCS'03)*, volume 2914 of *LNCS*, pages 124–135, Mumbai (India), 2003. Springer.

[5] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. In *Proc. of 18th Annual IEEE Symp. Logic in Computer Science (LICS'03)*, pages 261–270, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.

[6] H. Comon-Lundh and R. Treinen. Easy intruder deductions. In *Verification: Theory & Practice, Essays Dedicated to Zohar Manna on the Occasion of His 64th Birthday*, volume 2772 of *LNCS*, pages 225–242. Springer, 2003.

[7] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 2005. To appear.

[8] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[9] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Fast parallel computation of Hermite and Smith forms of polynomial matrices. *SIAM Journal of Algebraic and Discrete Methods*, 8(4):683–690, 1987.

[10] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In *Proc. 16th Int. Conf. Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *LNCS*, pages 308–322, Nara (Japan), 2005. Springer.

[11] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of exclusive-or with distributive encryption. Research Report LSV-05-19, Laboratoire Spécification et Vérification, ENS Cachan, France, 2005.

[12] D. A. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, 40(2):284–303, 1993.

[13] W. Nutt. Unification in monoidal theories. In *Proc. 10th Int. Conf. Automated Deduction, (CADE'90)*, volume 449 of *LNCS*, pages 618–632, Kaiserslautern (Germany), 1990. Springer.

[14] A. Schrijver. *Theory of Linear and Integer Programming.* Wiley, 1986.

[15] M. Tatebayashi, N. Matsuzaki, and D. B. Newman. Key distribution protocol for digital mobile communication systems. In *Proc. 9th Annual International Cryptology Conference (CRYPTO'89)*, volume 435 of *LNCS*, pages 324–333, Santa Barbara (California, USA), 1989. Springer.