A Proof Theoretic Analysis of Intruder Theories

Alwen Tiu and Rajeev Goré

Logic and Computation Group
College of Computer Science and Engineering
The Australian National University

Abstract. We consider the problem of intruder deduction in security protocol analysis: that is, deciding whether a given message M can be deduced from a set of messages Γ under the theory of blind signatures and arbitrary convergent equational theories modulo associativity and commutativity (AC) of certain binary operators. The traditional formulations of intruder deduction are usually given in natural-deduction-like systems and proving decidability requires significant effort in showing that the rules are "local" in some sense. By using the well-known translation between natural deduction and sequent calculus, we recast the intruder deduction problem as proof search in sequent calculus, in which locality is immediate. Using standard proof theoretic methods, such as permutability of rules and cut elimination, we show that the intruder deduction problem can be reduced, in polynomial time, to the elementary deduction problems, which amounts to solving certain equations in the underlying individual equational theories. We further show that this result extends to combinations of disjoint AC-convergent theories whereby the decidability of intruder deduction under the combined theory reduces to the decidability of elementary deduction in each constituent theory. Although various researchers have reported similar results for individual cases, our work shows that these results can be obtained using a systematic and uniform methodology based on the sequent calculus.

Keywords: AC convergent theories, sequent calculus, intruder deduction, security protocols.

1 Introduction

One of the fundamental aspects of the analysis of security protocols is the model of the intruder that seeks to compromise the protocols. In many situations, such a model can be described in terms of a deduction system which gives a formal account of the ability of the intruder to analyse and synthesize messages. As shown in many previous works (see, e.g., [2, 6, 9, 7]), finding attacks on protocols can often be framed as the problem of deciding whether a certain formal expression is derivable in the deduction system which models the intruder capability. The latter is sometimes called the *intruder deduction problem*, or the (ground) reachability problem. A basic deductive account of the intruder's capability is based on the so-called Dolev-Yao model, which assumes perfect encryption. While this

model has been applied fruitfully to many situations, a stronger model of intruders is needed to discover certain types of attacks. A recent survey [11] shows that attacks on several protocols used in real-world communication networks can be found by exploiting algebraic properties of encryption functions.

The types of attacks mentioned in [11] have motivated many recent works in studying models of intruders in which the algebraic properties of the operators used in the protocols are taken into account [9, 7, 1, 13, 17, 10]. In most of these, the intruder's capability is usually given as a natural-deduction-like deductive system. As is common in natural deduction, each constructor has a rule for introducing the constructor and one for eliminating the constructor. The elimination rule typically decomposes a term, reading the rule top-down: *e.g.*, a typical elimination rule for a pair $\langle M, N\rangle$ of terms is:

$$\frac{\Gamma \vdash \langle M, N\rangle}{\Gamma \vdash M}$$

Here, Γ denotes a set of terms, which represents the terms accumulated by the intruder over the course of its interaction with participants in a protocol. While a natural deduction formulation of deductive systems may seem "natural" and may reflect the meaning of the (logical) operators, it does not immediately give us a proof search strategy. Proof search means that we have to apply the rules bottom up, and as the above elimination rule demonstrates, this requires us to come up with a term N which might seem arbitrary. For a more complicated example, consider the following elimination rule for *blind signatures* [15, 16, 5].

$$\frac{\Gamma \vdash \mathsf{sign}(\mathsf{blind}(M, R), K) \quad \Gamma \vdash R}{\Gamma \vdash \mathsf{sign}(M, K)}$$

The basis for this rule is that the "unblinding" operation commutes with signature. Devising a proof search strategy in a natural deduction system containing this type of rule does not seem trivial. In most of the works mentioned above, in order to show the decidability results for the natural deduction system, one needs to prove that the system satisfies a notion of *locality*, i.e., in searching for a proof for $\Gamma \vdash M$, one needs only to consider expressions which are made of subterms from Γ and M. In addition, one has to also deal with the complication that arises from the use of the algebraic properties of certain operators.

In this work, we recast the intruder deduction problem as proof search in sequent calculus. A sequent calculus formulation of Dolev-Yao intruders was previously used by the first author in a formulation of open bisimulation for the spi-calculus [19] to prove certain results related to open bisimulation. The current work takes this idea further to include richer theories. Part of our motivation is to apply standard techniques, which have been well developed in the field of logic and proof theory, to the intruder deduction problem. In proof theory, sequent calculus is commonly considered a better calculus for studying proof search and decidability of logical systems, in comparison to natural deduction. This is partly due to the so-called "subformula" property (that is, the premise of every inference rule is made up of subterms of the conclusion of the

rule), which in most cases entails the decidability of the deductive system. It is therefore rather curious that none of the existing works on intruder deduction so far uses sequent calculus to structure proof search. We consider the ground intruder deduction problem (i.e., there are no variables in terms) under the class of *AC-convergent theories*. These are equational theories that can be turned into convergent rewrite systems, modulo associativity and commutativity of certain binary operators. Many important theories for intruder deduction fall into this category, e.g., theories for exclusive-or [9, 7], Abelian groups [9], and more generally, certain classes of monoidal theories [10].

We show two main results. Firstly, we show that the decidability of intruder deduction under AC-convergent theories can be reduced, in polynomial time, to *elementary intruder deduction problems*, which involve only the equational theories under consideration. Secondly, we show that the intruder deduction problem for a combination of disjoint theories $E_1, \ldots, E_n$ can be reduced, in polynomial time, to the elementary deduction problem *for each theory* E_i. This means that if the elementary deduction problem is decidable for each E_i, then the intruder deduction problem under the combined theory is also decidable. We note that these decidability results are not really new, although there are slight differences and improvements over the existing works (see Section 7). Our contribution is more of a methodological nature. We arrive at these results using rather standard proof theoretical techniques, e.g., *cut-elimination* and permutability of inference rules, in a uniform and systematic way. In particular, we obtain locality of proof systems for intruder deduction, which is one of the main ingredients to decidability results in [9, 7, 13, 12], for a wide range of theories that cover those studied in these works. Note that these works deal with a more difficult problem of deducibility constraints, which models *active intruders*, whereas we currently deal only with passive intruders. As future work, we plan to extend our approach to deal with active intruders.

The remainder of the paper is organised as follows. Section 2 presents two systems for intruder theories, one in natural deduction and the other in sequent calculus, and show that the two systems are equivalent. In Section 3, the sequent system is shown to enjoy cut-elimination. In Section 4, we show that cut-free sequent derivations can be transformed into a certain normal form. Using this result, we obtain another "linear" sequent system, from which the polynomial reducibility result follows. Section 5 discusses several example theories which can be found in the literature. Section 6 shows that the sequent system in Section 2 can be extended to cover any combination of disjoint AC-convergent theories, and the same decidability results also hold for this extension. Detailed proofs can be found in an extended version of the paper. [1]

2 Intruder deduction under AC convergent theories

We consider the following problem of formalising, given a set of messages Γ and a message M, whether M can be synthesized from the messages in Γ. We shall

[1] Available from http://arxiv.org/abs/0804.0273.

write this judgment as $\Gamma \vdash M$. This is sometimes called the 'ground reachability' problem or the 'intruder deduction' problem in the literature.

Messages are formed from names, variables and function symbols. We shall assume the following sets: a countably infinite set N of names ranged over by a, b, c, d, m and n; a countably infinite set V of variables ranged over by x, y and z; and a finite set $\Sigma_C = \{\mathsf{pub}, \mathsf{sign}, \mathsf{blind}, \langle .,. \rangle, \{.\}_.\}$ of symbols representing the *constructors*. Thus pub is a public key constructor, sign is a public key encryption function, blind is the blinding encryption function (as in [15, 16, 5]), $\langle .,. \rangle$ is a pairing constructor, and $\{.\}_.$ is the Dolev-Yao symmetric encryption function. Additionally, we also assume a possibly empty equational theory E, whose signature is denoted with Σ_E. We require that $\Sigma_C \cap \Sigma_E = \emptyset$.[2] Function symbols (including constructors) are ranged over by f, g and h. The equational theory E may contain at most one associative-commutative function symbol, which we denote with $\oplus$, obeying the standard associative and commutative laws. We restrict ourselves to equational theories which can be represented by terminating and confluent rewrite systems, modulo the associativity and commutativity of $\oplus$. We consider the set of messages generated by the following grammar

$$M, N := a \mid x \mid \mathsf{pub}(M) \mid \mathsf{sign}(M, N) \mid \mathsf{blind}(M, N) \\ \mid \langle M, N \rangle \mid \{M\}_N \mid f(M_1, \ldots, M_k).$$

The message $\mathsf{pub}(M)$ denotes the public key generated from a private key M; $\mathsf{sign}(M, N)$ denotes a message M signed with a private key N; $\mathsf{blind}(M, N)$ denotes a message M encrypted with N using a special blinding encryption; $\langle M, N \rangle$ denotes a pair of messages; and $\{M\}_N$ denotes a message M encrypted with a key N using a Dolev-Yao symmetric encryption. The blinding encryption has a special property that it commutes with the sign operation, i.e., one can "unblind" a signed blinded message $\mathsf{sign}(\mathsf{blind}(M, r), k)$ using the blinding key r to obtain $\mathsf{sign}(M, k)$. This aspect of the blinding encryption is reflected in its elimination rules, as we shall see later. We denote with $V(M)$ the set of variables occurring in M. A term M is *ground* if $V(M) = \emptyset$. We shall be mostly concerned with ground terms, so unless stated otherwise, we assume implicitly that terms are ground (the only exception is Proposition 2 and Proposition 3).

We shall use several notions of equality so we distinguish them using the following notation: we shall write $M = N$ to denote syntactic equality, $M \equiv N$ to denote equality modulo associativity and commutativity (AC) of $\oplus$, and $M \approx_T N$ to denote equality modulo a given equational theory T. We shall sometimes omit the subscript in $\approx_T$ if it can be inferred from context.

Given an equational theory E, we denote with R_E the set of rewrite rules for E (modulo AC). We write $M \rightarrow_{R_E} N$ when M rewrites to N using one application of a rewrite rule in R_E. The definition of rewriting modulo AC is standard and is omitted here. The reflexive-transitive closure of $\rightarrow_{R_E}$ is denoted with $\rightarrow^*_{R_E}$. We shall often remove the subscript R_E when no confusion arises. A term M is in *E-normal form* if $M \not\rightarrow_{R_E} N$ for any N. We write $M{\downarrow_E}$ to

[2] This restriction means that intruder theory such as homomorphic encryption is excluded. Nevertheless, it still covers a wide range of intruder theories.

denote the normal form of M with respect to the rewrite system R_E, modulo commutativity and associativity of $\oplus$. Again, the index E is often omitted when it is clear which equational theory we refer to. This notation extends straightforwardly to sets, e.g., $\Gamma\downarrow$ denotes the set obtained by normalising all the elements of Γ. A term M is said to be *headed by* a symbol f if $M = f(M_1, \ldots, M_k)$. M is *guarded* if it is either a name, a variable, or a term headed by a constructor. A term M is an *E-alien term* if M is headed by a symbol $f \notin \Sigma_E$. It is a *pure E-term* if it contains only symbols from Σ_E, names and variables.

A *context* is a term with holes. We denote with $C^k[]$ a context with k-hole(s). When the number k is not important or can be inferred from context, we shall write $C[\ldots]$ instead. Viewing a context $C^k[]$ as a tree, each hole in the context occupies a unique position among the leaves of the tree. We say that a hole occurrence is the i-th hole of the context $C^k[]$ if it is the i-th hole encountered in an inorder traversal of the tree representing $C^k[]$. An E-context is a context formed using only the function symbols in Σ_E. We write $C[M_1, \ldots, M_k]$ to denote the term resulting from replacing the holes in the k-hole context $C^k[]$ with $M_1, \ldots, M_k$, with M_i occuping the i-th hole in $C^k[]$.

Natural deduction and sequent systems The standard formulation of the judgment $\Gamma \vdash M$ is usually given in terms of a natural-deduction style inference system, as shown in Figure 1. We shall refer to this proof system as $\mathcal{N}$ and write $\Gamma \Vdash_{\mathcal{N}} M$ if $\Gamma \vdash M$ is derivable in $\mathcal{N}$. The deduction rules for Dolev-Yao encryption is standard and can be found in the literature, e.g., [6, 9]. The blind signature rules are taken from the formulation given by Bernat and Comon-Lundh [5]. Note that the rule sign_E assumes implicitly that signing a message hides its contents. An alternative rule without this assumption would be

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

The results of the paper also hold, with minor modifications, if we adopt this rule.

A sequent $\Gamma \vdash M$ is in *normal form* if M and all the terms in Γ are in normal form. Unless stated otherwise, in the following we assume that sequents are in normal form. The sequent system for intruder deduction, under the equational theory E, is given in Figure 2. We refer to this sequent system as $\mathcal{S}$ and write $\Gamma \Vdash_{\mathcal{S}} M$ to denote the fact that the sequent $\Gamma \vdash M$ is derivable in $\mathcal{S}$.

Unlike natural deduction rules, sequent rules also allow introduction of terms on the left hand side of the sequent. The rules p_L, e_L, sign_L, blind_{L1}, blind_{L2}, and gs are called *left introduction rules* (or simply *left rules*), and the rules $p_R, e_R, \mathsf{sign}_R, \mathsf{blind}_R$ are called *right introduction rules* (or simply, *right rules*). Notice that the rule gs is very similar to *cut*, except that we have the proviso that A is a subterm of a term in the lower sequent. This is sometimes called *analytic cut* in the proof theory literature. Analytic cuts are not problematic as far as proof search is concerned, since it still obeys the sub-formula property.

We need the rule gs because we do not have introduction rules for function symbols in Σ_E, in contrast to natural deduction. This rule is needed to "abstract"

$$\frac{M \in \Gamma}{\Gamma \vdash M}\ id \qquad \frac{\Gamma \vdash \{M\}_K \quad \Gamma \vdash K}{\Gamma \vdash M}\ e_E \qquad \frac{\Gamma \vdash M \quad \Gamma \vdash K}{\Gamma \vdash \{M\}_K}\ e_I$$

$$\frac{\Gamma \vdash \langle M, N\rangle}{\Gamma \vdash M}\ p_E \qquad \frac{\Gamma \vdash \langle M, N\rangle}{\Gamma \vdash N}\ p_E \qquad \frac{\Gamma \vdash M \quad \Gamma \vdash N}{\Gamma \vdash \langle M, N\rangle}\ p_I$$

$$\frac{\Gamma \vdash \mathsf{sign}(M, K) \quad \Gamma \vdash \mathsf{pub}(K)}{\Gamma \vdash M}\ \mathsf{sign}_E \qquad \frac{\Gamma \vdash M \quad \Gamma \vdash K}{\Gamma \vdash \mathsf{sign}(M, K)}\ \mathsf{sign}_I$$

$$\frac{\Gamma \vdash \mathsf{blind}(M, K) \quad \Gamma \vdash K}{\Gamma \vdash M}\ \mathsf{blind}_{E1} \qquad \frac{\Gamma \vdash M \quad \Gamma \vdash K}{\Gamma \vdash \mathsf{blind}(M, K)}\ \mathsf{blind}_I$$

$$\frac{\Gamma \vdash \mathsf{sign}(\mathsf{blind}(M, R), K) \quad \Gamma \vdash R}{\Gamma \vdash \mathsf{sign}(M, K)}\ \mathsf{blind}_{E2}$$

$$\frac{\Gamma \vdash M_1 \quad \cdots \quad \Gamma \vdash M_n}{\Gamma \vdash f(M_1, \ldots, M_n)}\ f_I, \text{ where } f \in \Sigma_E \qquad \frac{\Gamma \vdash N}{\Gamma \vdash M}\ \approx, \text{ where } M \approx_E N$$

Fig. 1. System $\mathcal{N}$: a natural deduction system for intruder deduction

E-alien subterms in a sequent (in the sense of the variable abstraction technique common in unification theory, see e.g., [18, 4]), which is needed to prove that the cut rule is redundant. For example, let E be a theory containing only the associativity and the commutativity axioms for $\oplus$. Then the sequent $a, b \vdash \langle a, b\rangle \oplus a$ should be provable without cut. Apart from the gs rule, the only other way to prove this is by using the id rule. However, id is not applicable, since no E-context $C[...]$ can obey $C[a, b] \approx \langle a, b\rangle \oplus a$ because E-contexts can contain only symbols from Σ_E and thus cannot contain $\langle ., .\rangle$. Therefore we need to "abstract" the term $\langle a, b\rangle$ in the right hand side, via the gs rule:

$$\dfrac{\dfrac{\dfrac{}{a, b \vdash a}\ id \quad \dfrac{}{a, b \vdash b}\ id}{a, b \vdash \langle a, b\rangle}\ p_R \quad \dfrac{}{a, b, \langle a, b\rangle \vdash \langle a, b\rangle \oplus a}\ id}{a, b \vdash \langle a, b\rangle \oplus a}\ gs$$

The third id rule instance (from the left) is valid because we have $C[\langle a, b\rangle, a] \equiv \langle a, b\rangle \oplus a$, where $C[., .] = [.] \oplus [.]$.

Provability in the natural deduction system and in the sequent system are related via the standard translation, i.e., right rules in sequent calculus correspond to introduction rules in natural deduction and left rules corresponds to elimination rules. The straightforward translation from natural deduction to sequent calculus uses the cut rule.

Proposition 1. *The judgment $\Gamma \vdash M$ is provable in the natural deduction system $\mathcal{N}$ if and only if $\Gamma\downarrow \vdash M\downarrow$ is provable in the sequent system $\mathcal{S}$.*

3 Cut elimination for $\mathcal{S}$

We now show that the cut rule is redundant for $\mathcal{S}$.

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

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

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

$$\frac{\Gamma, \mathsf{sign}(M, K), \mathsf{pub}(L), M \vdash N}{\Gamma, \mathsf{sign}(M, K), \mathsf{pub}(L) \vdash N}\ \mathsf{sign}_L, K \equiv L \qquad \frac{\Gamma \vdash M \quad \Gamma \vdash K}{\Gamma \vdash \mathsf{sign}(M, K)}\ \mathsf{sign}_R$$

$$\frac{\Gamma, \mathsf{blind}(M, K) \vdash K \quad \Gamma, \mathsf{blind}(M, K), M, K \vdash N}{\Gamma, \mathsf{blind}(M, K) \vdash N}\ \mathsf{blind}_{L1} \qquad \frac{\Gamma \vdash M \quad \Gamma \vdash K}{\Gamma \vdash \mathsf{blind}(M, K)}\ \mathsf{blind}_R$$

$$\frac{\Gamma, \mathsf{sign}(\mathsf{blind}(M, R), K) \vdash R \quad \Gamma, \mathsf{sign}(\mathsf{blind}(M, R), K), \mathsf{sign}(M, K), R \vdash N}{\Gamma, \mathsf{sign}(\mathsf{blind}(M, R), K) \vdash N}\ \mathsf{blind}_{L2}$$

$$\frac{\Gamma \vdash A \quad \Gamma, A \vdash M}{\Gamma \vdash M}\ gs, A \text{ is a guarded subterm of } \Gamma \cup \{M\}$$

Fig. 2. System $\mathcal{S}$: a sequent system for intruder deduction.

Definition 1. *An inference rule R in a proof system $\mathcal{D}$ is* admissible for $\mathcal{D}$ *if for every sequent $\Gamma \vdash M$ derivable in $\mathcal{D}$, there is a derivation of the same sequent in $\mathcal{D}$ without instances of R.*

The *cut-elimination* theorem for $\mathcal{S}$ states that the cut rule is admissible for $\mathcal{S}$. Before we proceed with the main cut elimination proof, we first prove a basic property of equational theories and rewrite systems, which is concerned with a technique called *variable abstraction* [18, 4].

Given derivation Π, the *height* of the derivation, denoted by $|\Pi|$, is the length of a longest branch in Π. Given a normal term M, the *size* $|M|$ of M is the number of function symbols, names and variables appearing in M.

In the following, we consider slightly more general equational theories than in the previous section: each AC theory E can be a theory obtained from a disjoint combination of AC theories $E_1, \ldots, E_k$, where each E_i has at most one AC operator $\oplus_i$. This allows us to reuse the results for a more general case later.

Definition 2. *Let E be a disjoint combination of AC convergent theories E_1, $\ldots$, E_n. A term M is a* quasi-E_i term *if every E_i-alien subterm of M is in E-normal form.*

For example, let $E = \{h(x, x) \approx x\}$. Then $h(\langle a, b\rangle, c)$ is a quasi E-term, whereas $h(\langle a, b\rangle, \langle h(a, a), b\rangle)$ is not, since its E-alien subterm $\langle h(a, a), b\rangle$ is not in its E-normal form $\langle a, b\rangle$. Obviously, any E normal term is a quasi E_i term.

In the following, given an equational theory E, we assume the existence of a function v_E, which assigns a variable from V to each ground term such that

$v_E(M) = v_E(N)$ if and only if $M \approx_E N$. In other words, v_E assigns a unique variable to each equivalence class of ground terms induced by $\approx_E$.

Definition 3. *Let E be an equational theory obtained by disjoint combination of AC theories $E_1, \ldots, E_n$. The E_i* abstraction function *F_{E_i} is a function mapping ground terms to pure E_i terms, defined recursively as follows:*

$$F_{E_i}(u) = \begin{cases} u, & \text{if } u \text{ is a name,} \\ f(F_{E_i}(u_1), \ldots, F_{E_i}(u_k)), & \text{if } u = f(u_1, \ldots, u_k) \text{ and } f \in \Sigma_{E_i}, \\ v_E(u), & \text{otherwise.} \end{cases}$$

It can be easily shown that the function F_{E_i} preserves the equivalence relation $\equiv$. That is, if $M \equiv N$ then $F_{E_i}(M) \equiv F_{E_i}(N)$.

Proposition 2. *Let E be a disjoint combination of $E_1, \ldots, E_n$. If M is a quasi E_i term and $M \rightarrow^*_{R_E} N$, then N is a quasi E_i term and $F_{E_i}(M) \rightarrow^*_{R_E} F_{E_i}(N)$.*

Proposition 3. *Let E be a disjoint combination of $E_1, \ldots, E_n$. If M and N are quasi E_i terms and $F_{E_i}(M) \rightarrow^*_{R_E} F_{E_i}(N)$, then $M \rightarrow^*_{R_E} N$.*

We now show some important proof transformations needed to prove cut elimination, i.e., in an inductive argument to reduce the size of cut terms. In the following, when we write that a sequent $\Gamma \vdash M$ is derivable, we mean that it is derivable in the proof system $\mathcal{S}$, with a fixed AC theory E.

Lemma 1. *Let Π be a derivation of $M_1, \ldots, M_k \vdash N$. Then for any $M'_1, \ldots, M'_k$ and N' such that $M_i \equiv M'_i$ and $N \equiv N'$, there is a derivation Π' of $M'_1, \ldots, M'_k \vdash N'$ such that $|\Pi| = |\Pi'|$.*

Lemma 2. *Let X and Y be terms in normal form and let f be a binary constructor. If $\Gamma, f(X,Y) \vdash M$ is cut-free derivable, then so is $\Gamma, X, Y \vdash M$.*

The more interesting case in the proof of Lemma 2 is when $\Gamma, f(X,Y) \vdash M$ is proved by an application of the *id* rule where $f(X,Y)$ is active. That is, we have $C[f(X,Y), M_1, \ldots, M_k] \approx_E M$, where $M_1, \ldots, M_k \in \Gamma$, for some E-context $C[..]$. Since M is in normal form, we have

$$C[f(X,Y), M_1, \ldots, M_k] \rightarrow^* M. \tag{1}$$

There are two cases to consider in the construction of a proof for $\Gamma, X, Y \vdash M$. If $f(X,Y)$ occurs as a subterm of M or Γ, then we simply apply the *gs* rule (bottom up) to abstract the term $f(X,Y)$ and then apply the *id* rule. Otherwise, we use the variable abstraction techniques (Proposition 2 and Proposition 3) to abstract $f(X,Y)$ from the rewrite steps (1) above, and then replace its abstraction with X to obtain: $C[X, M_1, \ldots, M_k] \rightarrow^* M$. That is, the *id* rule is applicable to the sequent $\Gamma, X, Y \vdash M$, with X taking the role of $f(X,Y)$.

Lemma 3. *Let $X_1, \ldots, X_k$ be normal terms and let Π be a cut-free derivation of $\Gamma, f(X_1, \ldots, X_k)\downarrow \vdash M$, where $f \in \Sigma_E$. Then there exists a cut-free derivation Π' of $\Gamma, X_1, \ldots, X_k \vdash M$.*

Lemma 4. *Let $M_1, \ldots, M_k$ be terms in normal form and let $C[\ldots]$ be a k-hole E-context. If $\Gamma, C[M_1, \ldots, M_k]\downarrow \vdash M$ is cut-free derivable, then so is $\Gamma, M_1, \ldots, M_k \vdash M$.*

One peculiar aspect of the sequent system $\mathcal{S}$ is that in the introduction rules for encryption functions (including blind signatures), there is no switch of polarities for the encryption key. For example, in the introduction rule for $\{M\}_K$, both on the left and on the right, the key K appears on the right hand side of a premise of the rule. This means that there is no exchange of information between the left and the right hand side of sequents, unlike, say, typical implication rules in logic. This gives rise to an easy cut elimination proof, where we need only to measure the complexity of the left premise of a cut in determining the cut rank.

Theorem 1. *The cut rule is admissible for $\mathcal{S}$.*

4 Normal derivations and decidability

We now turn to the question of the decidability of the deduction problem $\Gamma \vdash M$. This problem is known already for several AC theories, e.g., exclusive-or, abelian groups and their extensions with a homomorphism axiom [9, 7, 13, 12, 1]. What we would like to show here is how the decidability result can be reduced to a more elementary decision problem, defined as follows.

Definition 4. *Given an equational theory E, the* elementary deduction problem *for E, written $\Gamma \Vdash_E M$, is the problem of deciding whether the id rule is applicable to the sequent $\Gamma \vdash M$ (by checking whether there exists an E-context $C[\ldots]$ and terms $M_1, \ldots, M_k \in \Gamma$ such that $C[M_1, \ldots, M_k] \approx_E M$).*

Note that as a consequence of Proposition 2 and Proposition 3, in checking elementary deducibility, it is enough to consider the pure E equational problem where all E-alien subterms are abstracted, i.e., we have

$$C[M_1, \ldots, M_k] \approx_E M \qquad \text{iff} \qquad C[F_E(M_1), \ldots, F_E(M_k)] \approx_E F_E(M).$$

Our notion of elementary deduction corresponds roughly to the notion of "recipe" in [1], but we note that the notion of a recipe is a stronger one, since it bounds the size of the equational context.

The cut free sequent system does not strictly speaking enjoy the "subformula" property, i.e., in blind_{L2}, the premise sequent has a term which is not a subterm of any term in the lower sequent. However, it is easy to see that, reading the rules bottom up, we only ever introduce terms which are smaller than the terms in the lower sequent. Thus a naive proof search strategy which non-deterministically tries all applicable rules and avoids repeated sequents will eventually terminate. This procedure is of course rather expensive. We show that we can obtain a better complexity result by analysing the structures of cut-free derivations. Recall that the rules $p_L, e_L, \mathsf{sign}_L, \mathsf{blind}_{L1}, \mathsf{blind}_{L2}$ and gs are called left rules (the other rules are right rules).

$$\frac{\Gamma \Vdash_{\mathcal{R}} M}{\Gamma \vdash M}\ r \qquad \frac{\Gamma, \{M\}_K, M, K \vdash N}{\Gamma, \{M\}_K \vdash N}\ le,\ \text{where } \Gamma, \{M\}_K \Vdash_{\mathcal{R}} K$$

$$\frac{\Gamma, \langle M, N\rangle, M, N \vdash T}{\Gamma, \langle M, N\rangle \vdash T}\ lp \qquad \frac{\Gamma, \mathsf{sign}(M, K), \mathsf{pub}(L), M \vdash N}{\Gamma, \mathsf{sign}(M, K), \mathsf{pub}(L) \vdash N}\ \mathsf{sign}, K \equiv L$$

$$\frac{\Gamma, \mathsf{blind}(M, K), M, K \vdash N}{\Gamma, \mathsf{blind}(M, K) \vdash N}\ \mathsf{blind}_1,\ \text{where } \Gamma, \mathsf{blind}(M, K) \Vdash_{\mathcal{R}} K$$

$$\frac{\Gamma, \mathsf{sign}(\mathsf{blind}(M, R), K), \mathsf{sign}(M, K), R \vdash N}{\Gamma, \mathsf{sign}(\mathsf{blind}(M, R), K) \vdash N}\ \mathsf{blind}_2,$$

where $\Gamma, \mathsf{sign}(\mathsf{blind}(M, R), K) \Vdash_{\mathcal{R}} R$.

$$\frac{\Gamma, A \vdash M}{\Gamma \vdash M}\ ls, \text{where } A \text{ is a guarded subterm of } \Gamma \cup \{M\} \text{ and } \Gamma \Vdash_{\mathcal{R}} A.$$

Fig. 3. System $\mathcal{L}$: a linear proof system for intruder deduction.

Definition 5. *A cut-free derivation Π is said to be a* normal derivation *if it satisfies the following conditions:*

1. *no left rule appears above a right rule;*
2. *no left rule appears immediately above the left-premise of a branching left rule (i.e., all left rules except p_L and sign_L).*

Proposition 4. *If $\Gamma \vdash M$ is derivable then it has a normal derivation.*

In a normal derivation, the left branch of a branching left rule is provable using only right rules and *id*. This means that we can represent a normal derivation as a sequence (reading the proof bottom-up) of sequents, each of which is obtained from the previous one by adding terms composed of subterms of the previous sequent, with the proviso that certain subterms can be constructed using right-rules. Let us denote with $\Gamma \Vdash_{\mathcal{R}} M$ the fact that the sequent $\Gamma \vdash M$ is provable using only the right rules and *id*. This suggests a more compact deduction system for intruder deduction, called system $\mathcal{L}$, given in Figure 3.

Proposition 5. *Every sequent $\Gamma \vdash M$ is provable in $\mathcal{S}$ if and only if it is provable in $\mathcal{L}$.*

We now show that the decidability of the deduction problem $\Gamma \Vdash_{\mathcal{S}} M$ can be reduced to decidability of elementary deduction problems. We consider a representation of terms as directed acyclic graphs (DAG), with maximum sharing of subterms. Such a representation is quite standard and can be found in, e.g., [1], so we will not go into the details here.

In the following, we denote with $st(\Gamma)$ the set of subterms of the terms in Γ. In the DAG representation of Γ, the number of distinct nodes in the DAG representing distinct subterms of Γ co-incides with the cardinality of $st(\Gamma)$. A

term M is a *proper subterm* of N if M is a subterm of N and $M \neq N$. We denote with $pst(\Gamma)$ the set of proper subterms of Γ, and we define

$$sst(\Gamma) = \{\mathsf{sign}(M, N) \mid M, N \in pst(\Gamma)\}.$$

The *saturated set* of Γ, written $St(\Gamma)$, is the set

$$St(\Gamma) = \Gamma \cup pst(\Gamma) \cup sst(\Gamma).$$

The cardinality of $St(\Gamma)$ is at most quadratic in the size of $st(\Gamma)$. If Γ is represented as a DAG, one can compute the DAG representation of $St(\Gamma)$ in polynomial time, with only a quadratic increase of the size of the graph. Given a DAG representation of $St(\Gamma \cup \{M\})$, we can represent a sequent $\Gamma \vdash M$ by associating each node in the DAG with a tag which indicates whether or not the term represented by the subgraph rooted at that node appears in Γ or M. Therefore, in the following complexity results for deducibility problem $\Gamma \Vdash_S M$ (for some proof system S), we assume that the input consists of the DAG representation of the saturated set $St(\Gamma \cup \{M\})$, together with approriate tags in the nodes. Since each tag takes only a fixed amount of space (e.g., a two-bit data structure should suffice), we shall state the complexity result w.r.t. the size of $St(\Gamma \cup \{M\})$.

Definition 6. *Let $\Gamma \Vdash_{\mathcal{D}} M$ be a deduction problem, where $\mathcal{D}$ is some proof system, and let n be the size of $St(\Gamma \cup \{M\})$. Let E be the equational theory associated with $\mathcal{D}$. Suppose that the elementary deduction problem in E has complexity $O(f(m))$, where m is the size of the input. Then the problem $\Gamma \Vdash_{\mathcal{D}} M$ is said to be* polynomially reducible *to the elementary deduction problem $\Vdash_E$ if it has complexity $O(n^k \times f(n))$ for some constant k.*

A key lemma in proving the decidability result is the following invariant property of linear proofs.

Lemma 5. *Let Π be an $\mathcal{L}$-derivation of $\Gamma \vdash M$. Then for every sequent $\Gamma' \vdash M'$ occurring in Π, we have $\Gamma' \cup \{M'\} \subseteq St(\Gamma \cup \{M\})$.*

The existence of linear size proofs then follows from the above lemma.

Lemma 6. *If there is an $\mathcal{L}$-derivation of $\Gamma \vdash M$ then there is an $\mathcal{L}$-derivation of the same sequent whose length is at most $|St(\Gamma \cup \{M\})|$.*

Another useful observation is that the left-rules of $\mathcal{L}$ are *invertible*; at any point in proof search, we do not lose provability by applying any left rule. Polynomial reducibility of $\Vdash_{\mathcal{L}}$ to $\Vdash_E$ can then be proved by a deterministic proof search strategy which systematically tries all applicable rules.

Theorem 2. *The decidability of the relation $\Vdash_{\mathcal{L}}$ is polynomially reducible to the decidability of elementary deduction $\Vdash_E$.*

Note that in the case where the theory E is empty, we obtain a PTIME decision procedure for intruder deduction with blind signatures.

5 Some example theories

We now consider several concrete AC convergent theories that are often used in reasoning about security protocols. Decidability of intruder deduction under these theories has been extensively studied [9, 7, 1, 13, 17, 10]. These results can be broadly categorized into those with explicit pairing and encryption constructors, e.g., [9, 17], and those where the constructors are part of the equational theories, e.g., [1, 10]. For the latter, one needs explicit decryption operators with, e.g., an equation like $dec(\{M\}_N, N) \approx M$. Decidability results for these deduction problems are often obtained by separating elementary deducibility from the general deduction problem. This is obtained by studying some form of normal derivations in a natural deduction setting. Such a reduction, as has been shown in the previous section, applies to our calculus in a more systematic fashion.

Exclusive-or. The signature of this theory consists of a binary operator $\oplus$ and a constant 0. The theory is given by the axioms of associativity and commutativity of $\oplus$ together with the axiom $x \oplus x \approx 0$ and $x \oplus 0 \approx x$. This theory can be turned into an AC convergent rewrite system with the following rewrite rules:

$$x \oplus x \to 0 \qquad \text{and} \qquad x \oplus 0 \to x.$$

Checking $\Gamma \Vdash_E M$ can be done in PTIME, as shown in, e.g., [7].

Abelian groups. The exclusive-or theory is an instance of Abelian groups, where the inverse of an element is the element itself. The more general case of Abelian groups includes an inverse operator, denoted with I here. The equality theory for Abelian groups is given by the axioms of associativity and commutativity, plus the theory $\{x \oplus 0 \approx 0, x \oplus I(x) \approx 0\}$. The equality theory of Abelian groups can be turned into a rewrite system modulo AC by orienting the above equalities from left to right, in addition to the following rewrite rules:

$$I(x \oplus y) \to I(x) \oplus I(y) \qquad I(I(x)) \to x \qquad I(0) \to 0.$$

One can also obtain an AC convergent rewrite system for an extension of Abelian groups with a homomorphism axiom involving a unary operator h: $h(x \oplus y) = h(x) \oplus h(y)$. In this case, the rewrite rules above need to be extended with

$$h(x \oplus y) \to h(x) \oplus h(y) \qquad h(0) \to 0 \qquad h(I(x)) \to I(h(x)).$$

Decidability of elementary deduction under Abelian groups (with homomorphism) can be reduced to solving a system of linear equations over some semirings (see [12] for details).

6 Combining disjoint convergent theories

We now consider the intruder deduction problem under a convergent AC theory E, which is obtained from the union of pairwise disjoint convergent AC theories

$E_1, \ldots, E_n$. Each theory E_i may contain an associative-commutative binary operator, which we denote with $\oplus_i$. We show that the intruder deduction problem under E can be reduced to the elementary deduction problem of each E_i.

Given a term $M = f(M_1, \ldots, M_k)$, where f is a function symbol (i.e., a constructor, an equational symbol or $\oplus$), the terms $M_1, \ldots, M_k$ are called the *immediate subterms* of M. Given a term M and a subterm occurrence N in M, we say that N is a *cross-theory subterm* of M if N is headed with a symbol $f \in \Sigma_{E_i}$ and it is an immediate subterm of a subterm in M which is headed by a symbol $g \in \Sigma_{E_j}$, where $i \neq j$. We shall also refer to N as an E_{ij}*-subterm* of M when we need to be explicit about the equational theories involved.

Throughout this section, we consider a sequent system $\mathcal{D}$, whose rules are those of $\mathcal{S}$, but with *id* replaced by the rule below left and with the addition of the rule below right where N is a cross-theory subterm of some term in $\Gamma \cup \{M\}$:

$$\frac{\begin{array}{c} M \approx_E C[M_1, \ldots, M_k] \\ C[\,] \text{ an } E_i\text{-context, and } M_1, \ldots, M_k \in \Gamma \end{array}}{\Gamma \vdash M}\ id_{E_i} \qquad \frac{\Gamma \vdash N \quad \Gamma, N \vdash M}{\Gamma \vdash M}\ cs$$

The analog of Proposition 1 holds for $\mathcal{D}$. Its proof is a straightforward adaptation of the proof of Proposition 1.

Proposition 6. *The judgment $\Gamma \vdash M$ is provable in the natural deduction system $\mathcal{N}$, under theory E, if and only if $\Gamma\downarrow \vdash M\downarrow$ is provable in the sequent system $\mathcal{D}$.*

Cut elimination also holds for $\mathcal{D}$. Its proof is basically the same as the proof for $\mathcal{S}$, since the "logical structures" (i.e., those concerning constructors) are the same. The only difference is in the treatment of abstracted terms (the rules *gs* and *cs*). In $\mathcal{D}$ we allow abstraction of arbitrary cross-theory subterms, in addition to guarded subterm abstraction. The crucial part of the proof in this case relies on the variable abstraction technique (Proposition 2 and Proposition 3), which applies to both guarded subterm and cross-theory subterm abstraction.

Theorem 3. *The cut rule is admissible for $\mathcal{D}$.*

The decidability result for $\mathcal{S}$ also holds for $\mathcal{D}$. This can be proved with straightforward modifications of the similar proof for $\mathcal{S}$, since the extra rule *cs* has the same structure as *gs* in $\mathcal{S}$. It is easy to see that the same normal forms for $\mathcal{S}$ also holds for $\mathcal{D}$, with *cs* considered as a left-rule. It then remains to design a linear proof system for $\mathcal{D}$. We first define the notion of right-deducibility: The relation $\Gamma \Vdash_{\mathcal{RD}} M$ holds if and only if the sequent $\Gamma \vdash M$ is derivable in $\mathcal{D}$ using only the right rules. We next define a linear system for $\mathcal{D}$, called $\mathcal{LD}$, which consists of the rules of $\mathcal{L}$ defined in the previous section, but with the proviso $\Gamma \Vdash_{\mathcal{R}} M$ changed to $\Gamma \Vdash_{\mathcal{RD}} M$, and with the additional rule:

$$\frac{\Gamma, R \vdash M}{\Gamma \vdash M}\ lcs$$

where R is a cross-theory subterm of some term in $\Gamma \cup \{M\}$ and $\Gamma \Vdash_{\mathcal{RD}} R$.

Proposition 7. *A sequent $\Gamma \vdash M$ is provable in $\mathcal{D}$ if and only if it is provable in $\mathcal{LD}$.*

The notion of polynomial reducibility is slightly changed. Suppose each elementary deduction problem in E_i is bounded by $O(f(m))$. Let m be the size of $St(\Gamma \cup \{M\})$. Then the deduction problem $\Gamma \Vdash_{\mathcal{D}} M$ is polynomially reducible to $\Vdash_{E_1}, \ldots, \Vdash_{E_n}$ if it has complexity $O(m^k f(m))$, for some constant k.

Theorem 4. *The decidability of the relation $\Vdash_{\mathcal{LD}}$ is polynomially reducible to the decidability of elementary deductions $\Vdash_{E_1}, \ldots, \Vdash_{E_n}$.*

7 Conclusion and related work

We have shown that decidability of the intruder deduction problem, under a range of equational theories, can be reduced to the simpler problem of elementary deduction, which amounts to solving equations in the underlying equational theories. This reduction is obtained in a purely proof theoretical way, using standard techniques such as cut elimination and permutation of inference rules.

There are several existing works in the literature that deal with intruder deduction. Our work is more closely related to, e.g., [9, 12, 17], in that we do not have explicit destructors (projection, decryption, unblinding), than, say, [1, 10]. In the latter work, these destructors are considered part of the equational theory, so in this sense our work slightly extends theirs to allow combinations of explicit and implicit destructors. A drawback for the approach with explicit destructors is that one needs to consider these destructors together with other algebraic properties in proving decidability, although recent work in combining decidable theories [3] allows one to deal with them modularly. Combination of intruder theories has been considered in [8, 3, 14], as part of their solution to a more difficult problem of deducibility constraints which assumes active intruders. In particular, Delaune, et. al., [14] obtain results similar to what we have here concerning combination of AC theories. One difference between these works and ours is in how this combination is derived. Their approach is more algorithmic whereas our result is obtained through analysis of proof systems.

It remains to be seen whether sequent calculus, and its associated proof techniques, can prove useful for richer theories. For certain deduction problems, i.e., those in which the constructors interact with the equational theory, there does not seem to be general results like the ones we obtain for theories with no interaction with the constructors. One natural problem where this interaction occurs is the theory with homomorphic encryption, e.g., like the one considered in [17]. Another interesting challenge is to see how sequent calculus can be used to study the more difficult problem of solving intruder deduction constraints, e.g., like those studied in [9, 7, 13].

Acknowledgement We thank the anonymous referees of earlier drafts of this paper for their careful reading and helpful comments. This work has been supported by the Australian Research Council (ARC) Discovery Project DP0880549.

References

1. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theor. Comput. Sci.*, 367(1-2):2–32, 2006.
2. R. M. Amadio and D. Lugiez. On the reachability problem in cryptographic protocols. In C. Palamidessi, editor, *CONCUR*, volume 1877 of *LNCS*, pages 380–394. Springer, 2000.
3. M. Arnaud, V. Cortier, and S. Delaune. Combining algorithms for deciding knowledge in security protocols. In B. Konev and F. Wolter, editors, *FroCos*, volume 4720 of *LNCS*, pages 103–117. Springer, 2007.
4. F. Baader and K. U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. *J. Sym. Comp.*, 21(2):211–243, 1996.
5. V. Bernat and H. Comon-Lundh. Normal proofs in intruder theories. In *ASIAN 2006*, volume 4435 of *LNCS*, pages 151–166. Springer, 2007.
6. M. Boreale. Symbolic trace analysis of cryptographic protocols. In F. Orejas, P. G. Spirakis, and J. van Leeuwen, editors, *ICALP*, volume 2076 of *LNCS*, pages 667–681. Springer, 2001.
7. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with xor. In *LICS*, pages 261–270, 2003.
8. Y. Chevalier and M. Rusinowitch. Combining intruder theories. In L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, editors, *ICALP*, volume 3580 of *LNCS*, pages 639–651. Springer, 2005.
9. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *LICS*, pages 271–280. IEEE Computer Society, 2003.
10. V. Cortier and S. Delaune. Deciding knowledge in security protocols for monoidal equational theories. In N. Dershowitz and A. Voronkov, editors, *LPAR*, volume 4790 of *LNCS*, pages 196–210. Springer, 2007.
11. V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
12. S. Delaune. Easy intruder deduction problems with homomorphisms. *Inf. Process. Lett.*, 97(6):213–218, 2006.
13. S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, *ICALP (2)*, volume 4052 of *LNCS*, pages 132–143. Springer, 2006.
14. S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis for monoidal equational theories. *Inf. Comput.*, 206(2-4):312–351, 2008.
15. A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In *ASIACRYPT 1992*, volume 718 of *LNCS*, pages 244–251. Springer, 1993.
16. S. Kremer and M. Ryan. Analysis of an electronic voting protocol in the applied pi calculus. In *ESOP*, volume 3444 of *LNCS*, pages 186–200. Springer, 2005.
17. P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of abelian groups with distributive encryption. *Inf. Comput.*, 205(4):581–623, 2007.
18. M. Schmidt-Schauß. Unification in a combination of arbitrary disjoint equational theories. *J. Symb. Comput.*, 8(1/2):51–99, 1989.
19. A. Tiu. A trace based bisimulation for the spi calculus: An extended abstract. In *APLAS*, volume 4807 of *LNCS*, pages 367–382. Springer, 2007.