A PROOF THEORETIC ANALYSIS OF INTRUDER THEORIES [*]

ALWEN TIU, RAJEEV GORÉ, AND JEREMY DAWSON

Logic and Computation Group, College of Engineering and Computer Science, The Australian National University
e-mail address: {Alwen.Tiu, Rajeev.Gore, Jeremy.Dawson}@rsise.anu.edu.au

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 problem, which amounts to solving certain equations in the underlying individual equational theories. We 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. To further demonstrate the utility of the sequent-based approach, we show that, for Dolev-Yao intruders, our sequent-based techniques can be used to solve the more difficult problem of solving *deducibility constraints*, where the sequents to be deduced may contain gaps (or variables) representing possible messages the intruder may produce. In particular, we show that there is a finite representation of all solutions to such a constraint problem.

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, 7, 11, 8]), 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. For example, a recent survey [13] 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 [13] 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 [11, 8, 1, 15, 19, 12]. 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* [17, 18, 6].

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

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 [23] 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 sequent calculus has not been more widely used in solving intruder deduction. Some early work by Millen and Shmatikov,

e.g., [20], appears to incorporate aspects of sequent calculus inference rules in their decision procedure for solving intruder deduction, but apart from this work, we are not aware of any systematic use of sequent calculus to solve the intruder deduction problem. It is important to note that we do not think that sequent calculus is a replacement for natural deduction as a *specification framework*; natural deduction is, naturally, a more intuitive framework to specify an intruder's ability. What we propose here is an alternative way to *structure proof search*, using known and widely used techniques from proof theory.

We are mainly concerned with 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 [11, 8], Abelian groups [11], and more generally, certain classes of monoidal theories [12]. We shall also present a solution to the more difficult problem of *deducibility constraint problems* (see Section 6), as a demonstration of feasibility of the sequent-based techniques, but only for a restricted model of the intruder.

A summary of the main results we obtain: 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. 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 [11, 8, 15, 14], 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*. We have not yet covered this more general problem for the intruder models with AC convergent theories, although, as we mentioned above, we do show a sequent-based solution to a restricted model of intruders (without AC theories). As future work, we plan to extend our approach to deal with active intruders under richer intruder models.

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 shows 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 shows that the sequent system in Section 2 can be extended straightforwardly to cover any combination of disjoint AC-convergent theories, and the same decidability results also hold for this extension. In Section 6 we show that the sequent-based techniques, in particular the normal form theorem, can be used to solve the more difficult problem of solving deducibility constraints for Dolev-Yao intruders, which do not involve any equational theories. The main results in Section 6, i.e., cut elimination and decision procedures for both intruder deduction and deducibility constraints, have been formally verified in Isabelle/HOL by the third author.

This paper is a revised and extended version of a conference paper [24]. More specifically, we have added detailed proofs of the results stated in the conference version and a new section on the sequent-based approach to solving deducibility constraint problems for Dolev-Yao intruders.

2. INTRUDER DEDUCTION UNDER AC-CONVERGENT THEORIES

We consider in the following the 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 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 constructor representing public key signature, blind is the blinding encryption function (as in [17, 18, 6]), $\langle \_, \_ \rangle$ is a pairing constructor, and $\{\_\}_\_$ is the Dolev-Yao symmetric encryption function. Note that the choice of the constructors here is not the most exhaustive one, in the sense that it does not cover all commonly used Dolev-Yao types of constructors (e.g., hash, asymmetric encryption, etc.); we select a subset which we think is representative enough. Adding those extra constructors to our model is straightforward, and the main results of this paper should extend to these additions as well. Note also that for clarity of presentation, in presenting the deduction rules corresponding to the encryption or signing operators, we do not attempt to abstract them further, e.g., by presenting a generic form of rules that could account for both encryption and signing (as they both have a similar structure).

In addition to constructors, we also assume a possibly empty equational theory E, whose signature is denoted with Σ_E. We require that $\Sigma_C \cap \Sigma_E = \emptyset$.[1] Function symbols (including constructors) are ranged over by f, g and h. The equational theory E may contain any number of associative-commutative function symbols, obeying the standard associative and commutative laws. However, for clarity of exposition, in this section, we shall restrict E to contain at most one associative-commutative symbol, which we denote with $\oplus$. Later in Section 5, we shall consider the more general case where the equational theory E can contain an arbitrary number of AC symbols. In any case, 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

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

where $f \in \Sigma_E$. The operational meaning of each constructor will be defined by their corresponding inference rules. Here we give an intuitive explanation for each constructor. Note that the language of messages as given above is untyped, but in the following explanation, it is helpful to draw analogy from practices in security protocol analysis to distinguish certain types of messages such as (public/private) keys, names, etc. The message $\mathsf{pub}(M)$ denotes

---

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

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 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 message M is *ground* if $V(M) = \emptyset$. In the following, we shall be mostly concerned with ground terms, so unless stated otherwise, we assume implicitly that messages are ground. The only exception is Proposition 3.6 and Proposition 3.7 and Section 6 where non-ground messages are also considered.

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.

Remark 2.1. Note that there is a choice on what function symbols one can regard as constructors and what one can put into the equational theory. At one extreme, we can consider all function symbols as part of the equational theory, e.g., by introducing one or more "destructor" functions for each constructor, and capture the intended meaning of each constructor via equations. For example, for symmetric encryption, one could introduce a decryption operator dec satisfying:

$$\mathsf{dec}(\{M\}_N, N) \approx M,$$

and for pairing, one could introduce the standard projection functions:

$$\pi_1(\langle M, N \rangle) \approx M \qquad \text{and} \qquad \pi_2(\langle M, N \rangle) \approx N.$$

However, incorporating all function symbols into the equational theory in this manner means that we lose the benefit of sequent calculus in analysing the structures of deduction, as equational theories are less constrained than inference rules as far as proof search is concerned. Ideally, one would want to push *all* function symbols into the inference system, but there appears to be no easy way to accomodate the associative-commutative symbols. The set of constructors that we can accomodate in the inference system is obviously larger than the one we consider here. Essentially, all equations that involve constructor-destructor pairs that obey simple equations, like the ones for pairing above, can be turned into appropriate introduction and elimination rules (in natural deduction) for the constructors. We leave as future work the exact characterisations of the equational theories that can be absorbed into inference rules.

Given an equational theory E, we denote with R_E the set of rewrite rules for E (modulo AC). We write $M \to_{R_E} N$ when M rewrites (modulo AC) to N using one application of a rewrite rule in R_E. The definition of rewriting modulo AC is standard and is omitted here (see, e.g., [4] for a definition). We recall one assumption about variables in rewrite rules that will be used explicitly in some proofs in the following section: if $s \to_{R_E} t$ is a rewrite rule, then the variables in t must occur in s. The reflexive-transitive closure of $\to_{R_E}$ is denoted with $\to^*_{R_E}$. We shall often remove the subscript R_E when no confusion arises. A term M is in *E-normal form* if $M \not\to_{R_E} N$ for any N. We write $M{\downarrow}_E$ to 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 $M = f(M_1, \ldots, M_k)$. 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 term M is a *proper subterm* of N if M is a subterm of N and $M \neq N$. Given a term $M = f(M_1, \ldots, M_k)$, where f is a constructor or a function symbol, the terms $M_1, \ldots, M_k$ are called the *immediate subterms* of M.

An E-alien subterm M of N is said to be an *E-factor* of N if there is another subterm F of N such that M is an immediate subterm of F and F is headed by a symbol $f \in \Sigma_E$. This notion of a factor of a term is generalised to sets of terms in the obvious way: a term M is an E-factor of Γ if it is an E-factor of a term in Γ.

Example 2.2. The term $M = d \oplus (\langle c, \langle a, b \rangle \rangle)$ has only one E-factor: $\langle c, \langle a, b \rangle \rangle$. Note that $\langle a, b \rangle$ is not an E-factor of M, since no subterm of M containing $\langle a, b \rangle$ as its immediate subterm is headed by a symbol from Σ_E. The subterm d is not an E-factor of M either, since it is not an E-alien term.

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 $M_1, \ldots, M_k$, where M_i occupies 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 are standard and can be found in the literature, e.g., [7, 11]. The blind signature rules are taken from the formulation given by Bernat and Comon-Lundh [6]. 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 *acut* 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 *acut* is very similar to *cut*, except that we have the proviso that A is an E-factor of the messages in the lower

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 they still obey the sub-formula property.

We need the rule *acut* because we do not have introduction rules for function symbols in Σ_E, in contrast to natural deduction. This rule is needed to "abstract" E-factors in a sequent (in the sense of the variable abstraction technique common in unification theory, see e.g., [22, 5]), 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 derivable without cut. Apart from the *acut* rule, the only other way to derive 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 *acut* rule:

$$\cfrac{\cfrac{\overline{a, b \vdash a}\ id \quad \overline{a, b \vdash b}\ id}{a, b \vdash \langle a, b \rangle}\ p_R \quad \overline{a, b, \langle a, b \rangle \vdash \langle a, b \rangle \oplus a}\ id}{a, b \vdash \langle a, b \rangle \oplus a}\ acut$$

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 $C[., .] = [.] \oplus [.]$.

Derivability 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 correspond to elimination rules. The straightforward translation from natural deduction to sequent calculus uses the cut rule.

Remark 2.3. Notice that the left rule for signing in the sequent calculus (sign_L) and the left rule for symmetric encryption (e_L) have different forms, although in the natural deduction system, their elimination rules are more or less the same. We could indeed use the following alternative left-rule for sign_L:

$$\cfrac{\Gamma, \mathsf{sign}(M, K) \vdash \mathsf{pub}(K) \quad \Gamma, \mathsf{sign}(M, K), M, \mathsf{pub}(K) \vdash N}{\Gamma, \mathsf{sign}(M, K), \vdash N}\ \mathsf{sign}'_L$$

It could be shown that sign_L and sign'_L are equivalent. We prefer the former since it has a 'nicer' form in that it satisfies the subformula property. Notice also that in sign_L, we need the proviso $K \equiv L$ because in the sequent rules, we do not quotient terms modulo AC.

In the following, given a derivation Π, we denote with $|\Pi|$ the *height* of Π, i.e., the length of the longest branch in Π.

Lemma 2.4 (Weakening). *Let Π be a derivation, in $\mathcal{S}$, of $\Gamma \vdash M$. If $\Gamma \subseteq \Gamma'$, then there exists an $\mathcal{S}$-derivation Π' of $\Gamma' \vdash M$ such that $|\Pi| = |\Pi'|$.*

Proof. By induction on $|\Pi|$.   □

Lemma 2.5. *If the judgment $\Gamma \vdash M$ is derivable in the natural deduction system $\mathcal{N}$ then $\Gamma\downarrow \vdash M\downarrow$ is derivable in the sequent system $\mathcal{S}$.*

Proof. Let Π be a natural deduction derivation of $\Gamma \vdash M$. We construct a sequent derivation Π' of $\Gamma\downarrow \vdash M\downarrow$ by induction on $|\Pi|$. The *id* rule translates to the *id* rule in sequent calculus; the introduction rules for constructors translate to the right-rules for the same constructors. If Π ends with the $\approx$-rule, then the premise and the conclusion of the rules translate to the same sequent, hence Π' is constructed by induction hypothesis. It remains to show the translations for the elimination rules and rules concerning $f \in \Sigma_E$.

- Suppose Π ends with f_I, for some $f \in \Sigma_E$:

$$\dfrac{\overset{\Pi_1}{\Gamma \vdash M_1} \quad \cdots \quad \overset{\Pi_k}{\Gamma \vdash M_k}}{\Gamma \vdash f(M_1, \ldots, M_k)} \; f_I$$

By induction hypothesis, we have sequent derivations Π_i' of $\Gamma{\downarrow} \vdash M_i{\downarrow}$, for each $i \in \{1, \ldots, k\}$. Lemma 2.4, applied to the Π_i', gives us another sequent derivation Π_i'' of $\Gamma{\downarrow}, M_1{\downarrow}, \ldots, M_{i-1}{\downarrow} \vdash M_i{\downarrow}$. We note that the sequent

$$\Gamma{\downarrow}, M_1{\downarrow}, \ldots, M_k{\downarrow} \vdash f(M_1, \ldots, M_k){\downarrow}$$

is derivable in the sequent system $\mathcal{S}$ by an application of the id-rule since $C[] = f(\ldots)$ is an E-context. The derivation Π' is then constructed by successive applications of the cut rule to this sequent with $\Pi_k'', \ldots, \Pi_1''$, where the i-th cut eliminates $M_i{\downarrow}$ from the conclusion by using the derivation Π_i'' of $\Gamma{\downarrow}, M_1{\downarrow}, \ldots, M_{i-1}{\downarrow} \vdash M_i{\downarrow}$.
- Suppose Π ends with p_E :

$$\dfrac{\overset{\Pi_1}{\Gamma \vdash \langle M, N \rangle}}{\Gamma \vdash M} \; p_E \qquad \dfrac{\dfrac{}{\Gamma{\downarrow}, \langle M{\downarrow}, N{\downarrow} \rangle, M{\downarrow}, N{\downarrow} \vdash M{\downarrow}} \; id}{\Gamma{\downarrow}, \langle M{\downarrow}, N{\downarrow} \rangle \vdash M{\downarrow}} \; p_L$$

Note that $\langle M, N \rangle{\downarrow} \equiv \langle M{\downarrow}, N{\downarrow} \rangle$ and that the sequent $\Gamma{\downarrow}, \langle M{\downarrow}, N{\downarrow} \rangle \vdash M{\downarrow}$ is derivable in the sequent calculus $\mathcal{S}$ (using an id rule followed by a p_L-rule), as shown above right. By the induction hypothesis, we have a sequent derivation Π_1' of $\Gamma{\downarrow} \vdash \langle M{\downarrow}, N{\downarrow} \rangle$, and so we can use the cut rule to get a sequent derivation of $\Gamma{\downarrow} \vdash M{\downarrow}$.
- Suppose Π ends with e_E :

$$\dfrac{\overset{\Pi_1}{\Gamma \vdash \{M\}_N} \quad \overset{\Pi_2}{\Gamma \vdash N}}{\Gamma \vdash M} \; e_E$$

By the induction hypothesis, we have a sequent derivation Π_1' of $\Gamma{\downarrow} \vdash \{M{\downarrow}\}_{N{\downarrow}}$ and a sequent derivation Π_2' of $\Gamma{\downarrow} \vdash N{\downarrow}$. By Lemma 2.4, we have a derivation Π_3 of $\Gamma{\downarrow}, \{M{\downarrow}\}_{N{\downarrow}} \vdash N{\downarrow}$, where $|\Pi_3| = |\Pi_2'|$. We construct a sequent derivation for the sequent

$$\Gamma{\downarrow}, \{M{\downarrow}\}_{N{\downarrow}}, N{\downarrow} \vdash M{\downarrow}$$

by an application of e_L, followed by two applications of id (read upwards). Then Π' is constructed by applying the cut rule to this sequent using Π_3 and Π_1'.
- Suppose Π ends with sign_E:

$$\dfrac{\overset{\Pi_1}{\Gamma \vdash \mathsf{sign}(M, K)} \quad \overset{\Pi_2}{\Gamma \vdash \mathsf{pub}(K)}}{\Gamma \vdash M} \; \mathsf{sign}_E$$

By induction hypothesis, we have a sequent derivation Π_1' and a sequent derivation Π_2' of, respectively,

$$\Gamma{\downarrow} \vdash \mathsf{sign}(M{\downarrow}, K{\downarrow}) \qquad \text{and} \qquad \Gamma{\downarrow} \vdash \mathsf{pub}(K{\downarrow}).$$

Let Π_2'' be a derivation of

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

obtained by an application of Lemma 2.4 to Π'_2. Let Π_3 be the derivation

$$\frac{\overline{\Gamma\downarrow, \mathsf{sign}(M\downarrow, K\downarrow), \mathsf{pub}(K\downarrow), M\downarrow \vdash M\downarrow} \;\; id}{\Gamma\downarrow, \mathsf{sign}(M\downarrow, K\downarrow), \mathsf{pub}(K\downarrow) \vdash M\downarrow} \;\; \mathsf{sign}_L$$

Then Π' is constructed by successive applications of cut with Π''_2 and cut with Π'_1 to Π_3.

- The cases where Π ends with blind_{E1} is analogous to the case with e_E.
- Suppose Π ends with blind_{E2}:

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma \vdash \mathsf{sign}(\mathsf{blind}(M, R), K) & \Gamma \vdash R \end{array}}{\Gamma \vdash \mathsf{sign}(M, K)} \;\; \mathsf{blind}_{E2}$$

By induction hypothesis, we have a derivation Π'_1 and a derivation Π'_2 of, respectively,

$$\Gamma\downarrow \vdash \mathsf{sign}(\mathsf{blind}(M\downarrow, R\downarrow), K\downarrow) \qquad \text{and} \qquad \Gamma\downarrow \vdash R\downarrow \;.$$

Let Π_3 be the derivation

$$\frac{\begin{array}{cc} \Pi''_2 & \\ \dots \vdash R\downarrow & \overline{\dots, \mathsf{sign}(M\downarrow, K\downarrow), R\downarrow \vdash \mathsf{sign}(M\downarrow, K\downarrow)} \;\; id \end{array}}{\Gamma\downarrow, \mathsf{sign}(\mathsf{blind}(M\downarrow, R\downarrow), K\downarrow) \vdash \mathsf{sign}(M\downarrow, K\downarrow)} \;\; \mathsf{blind}_{L2}$$

where Π''_2 is obtained from Π'_2 by weakening the sequent with

$$\mathsf{sign}(\mathsf{blind}(M\downarrow, R\downarrow), K\downarrow).$$

Then the derivation Π' is constructed by a cut between Π'_1 and Π_3. $\qquad\qquad \square$

For the case where the equational theory is empty, we conjecture that the translation from natural deduction derivations to sequent calculus derivations (with cuts) can be done in polynomial time, as there are no duplication of derivation trees needed in the translation. Note that in the translation, one needs to apply the weakening lemma to weaken certain derivations, but this can be done in linear time. Note also that in the translation of elimination rules, the cut rule is used to compose the inductively translated derivations with new derivations. But the latter are all derivations of bounded sizes (i.e., bounded by the size of the original sequent), hence they can also be constructed in linear time, and the overall complexity would still be bounded by polynomial time.

Lemma 2.6. *If $\Gamma \vdash M$, where $\Gamma \cup \{M\}$ is a set of terms in normal form, is derivable in the sequent system $\mathcal{S}$ then $\Gamma \vdash M$ is derivable in the natural deduction system $\mathcal{N}$.*

Proof. Let Π be a sequent derivation of $\Gamma \vdash M$. We construct a natural deduction derivation Π' of $\Gamma \vdash M$ by induction on Π.

- The right-introduction rules for $\mathcal{S}$ map to the same introduction rules in $\mathcal{N}$. When Π ends with such a rule, Π' in this case is constructed straightforwardly from the induction hypothesis using the introduction rules of $\mathcal{N}$.
- If Π ends with an *id* rule, i.e., $M \approx C[M_1, \dots, M_k]$, for some $M_1, \dots, M_k \in \Gamma$ and E-context $C[..]$, we construct a derivation Π_1 of $\Gamma \vdash C[M_1, \dots, M_k]$ by induction on the context $C[\dots]$. This is easily done using the f_I introduction rule in $\mathcal{N}$. The derivation Π' is then constructed from Π_1 by an application of the $\approx$-rule.

- Suppose $\Gamma = \Gamma' \cup \{\langle U, V \rangle\}$ and Π ends with p_L :

$$
\frac{\begin{array}{c} \Pi_1 \\ \Gamma', \langle U, V \rangle, U, V \vdash M \end{array}}{\Gamma', \langle U, V \rangle \vdash M} \; p_L
$$

By induction hypothesis, we have an $\mathcal{N}$-derivation Π_1' of $\Gamma', \langle U, V \rangle, U, V \vdash M$. We want an $\mathcal{N}$-derivation Π' of $\Gamma', \langle U, V \rangle \vdash M$ instead. The $\mathcal{N}$-derivation Π' is constructed inductively from Π_1' by copying the same rule applications in Π_1', except when Π_1' is either

$$
\frac{}{\Gamma, U, V \vdash U} \; id \quad \text{or} \quad \frac{}{\Gamma, U, V \vdash V} \; id
$$

in which case, Π' is

$$
\frac{\dfrac{}{\Gamma \vdash \langle U, V \rangle} \; id}{\Gamma \vdash U} \; p_E \quad \text{and} \quad \frac{\dfrac{}{\Gamma \vdash \langle U, V \rangle} \; id}{\Gamma \vdash V} \; p_E
$$

respectively, since $\langle U, V \rangle \in \Gamma$.

- Suppose $\Gamma = \Gamma' \cup \{\{U\}_V\}$ and Π ends with e_L :

$$
\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma \vdash V & \Gamma, U, V \vdash M \end{array}}{\Gamma', \{U\}_V \vdash M} \; e_L
$$

By induction hypothesis, we have an $\mathcal{N}$-derivation Π_1' of $\Gamma \vdash V$ and an $\mathcal{N}$-derivation Π_2' of $\Gamma, U, V \vdash M$. The $\mathcal{N}$-derivation Π' of $\Gamma \vdash M$ is then constructed inductively from Π_2' by applying the same rules as in Π_2', except when Π_2' is either

$$
\frac{}{\Gamma, U, V \vdash U} \; id \quad \text{or} \quad \frac{}{\Gamma, U, V \vdash V} \; id
$$

In the first case, Π' is

$$
\frac{\dfrac{}{\Gamma \vdash \{U\}_V} \; id \quad \begin{array}{c} \Pi_1' \\ \Gamma \vdash V \end{array}}{\Gamma \vdash U} \; e_E
$$

and in the second case Π' is simply Π_1'.

- Suppose $\Gamma = \Gamma' \cup \{\mathsf{sign}(N, K), \mathsf{pub}(L)\}$ and Π ends with sign_L:

$$
\frac{\begin{array}{c} \Pi_1 \\ \Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L), N \vdash M \end{array}}{\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L) \vdash M} \; \mathsf{sign}_L
$$

where $L \equiv K$ (hence $L \approx K$). By induction hypothesis, we have an $\mathcal{N}$-derivation Π_1' of

$$
\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L), N \vdash M.
$$

As in the previous case, the $\mathcal{N}$-derivation Π' of $\Gamma \vdash M$ is constructed by imitating the rules of Π_1', except for the following id case:

$$
\frac{}{\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L), N \vdash N} \; id
$$

which is replaced by

$$
\frac{\dfrac{}{\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L) \vdash \mathsf{sign}(N, K)} \; id \quad \dfrac{\dfrac{}{\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L) \vdash \mathsf{pub}(L)} \; id}{\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L) \vdash \mathsf{pub}(K)} \; \approx}{\Gamma', \mathsf{sign}(N, K), \mathsf{pub}(L) \vdash N} \; \mathsf{sign}_E
$$

- The case where Π ends with blind_{L1} is similar to the case with e_L.

- Suppose $\Gamma = \Gamma' \cup \{\mathsf{sign}(\mathsf{blind}(N, R), K)\}$ and Π ends with blind_{L2}:

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma \vdash R & \Gamma, \mathsf{sign}(N, K), R \vdash M \end{array}}{\Gamma', \mathsf{sign}(\mathsf{blind}(N, R), K) \vdash M} \ \mathsf{blind}_{L2}$$

Similarly to the previous case, we apply the induction hypothesis to both Π_1 and Π_2, obtaining Π_1' and Π_2'. The derivation Π' is constructed by imitating the rules of Π_2', but with the following *id* instances

$$\frac{}{\Gamma', \mathsf{sign}(N, K), R \vdash \mathsf{sign}(N, K)} \ id \qquad \frac{}{\Gamma', \mathsf{sign}(N, K), R \vdash R} \ id$$

replaced, respectively, by

$$\frac{\dfrac{}{\Gamma \vdash \mathsf{sign}(\mathsf{blind}(N, R), K)} \ id \quad \dfrac{\Pi_1'}{\Gamma \vdash R}}{\Gamma \vdash \mathsf{sign}(N, K)} \qquad \text{and} \quad \begin{array}{c} \Pi_1' \\ \Gamma \vdash R. \end{array}$$

- Suppose Π ends with *acut*:

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma \vdash A & \Gamma, A \vdash M \end{array}}{\Gamma \vdash M} \ acut$$

By induction hypothesis, we have an $\mathcal{N}$-derivation Π_1' of $\Gamma \vdash A$ and an $\mathcal{N}$-derivation Π_2' of $\Gamma, A \vdash M$. Again, as in the previous cases, we construct Π' inductively, on the height of Π_2', by imitating the rules in Π_2', except when Π_2' ends with an instance of *id* of the form

$$\frac{}{\Gamma, A \vdash A} \ id$$

in which case, Π' is Π_1'.

- Suppose Π ends with *cut*: this case is handled similarly to the previous case. $\qquad\square$

Proposition 2.7. *The judgment* $\Gamma \vdash M$ *is derivable in the natural deduction system* $\mathcal{N}$ *if and only if* $\Gamma{\downarrow} \vdash M{\downarrow}$ *is derivable in the sequent system* $\mathcal{S}$.

Proof. Immediate from Lemma 2.5 and Lemma 2.6. $\qquad\square$

3. Cut elimination for $\mathcal{S}$

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

Definition 3.1. 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* [22, 5].

3.1. **Variable abstraction.** 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 is so that we can reuse the results concerning variable abstraction for a more general case later in Section 5.

Definition 3.2. 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.

Example 3.3. 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 3.4. 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 $F_{E_i}(M) \equiv F_{E_i}(N)$.

Lemma 3.5. *Let E be a disjoint combination of AC theories $E_1, \ldots, E_n$. Let M be a quasi-E_i term. If $M \to_{R_E} N$ then N is also a quasi-E_i term and $F_{E_i}(M) \to_{R_E} F_{E_i}(N)$.*

Proof. By induction on the structure of M:
- If M is a name then the lemma holds vacuously.
- Suppose $M = f(u_1, \ldots, u_k)$, where $f \in \Sigma_{E_i}$. There are two cases to consider:
  - The redex is in u_j. This case follows straightforwardly from the induction hypothesis and the definition of F_{E_i}.
  - The redex is M. Then there must be a rewrite rule in R_E of the form

$$C[x_1, \ldots, x_n] \to C'[x_1, \ldots, x_n]$$

  where $C[..]$ and $C'[..]$ are E_i-context, such that

$$M \equiv (C[x_1, \ldots, x_l])\sigma \qquad \text{and} \qquad N \equiv (C'[x_1, \ldots, x_l])\sigma$$

  for some substitution σ. Note that since M is a quasi-E_i term, it follows that each $x_i\sigma$ is also a quasi-E_i term. Hence N must also be a quasi-E_i term. From the definition of F_{E_i}, we have the following equality (we abbreviate F_{E_i} as F):

$$\begin{aligned} F(M) \quad &\equiv F(C[x_1, \ldots, x_l]\sigma) \\ &= C[F(x_1\sigma), \ldots, F(x_l\sigma)] \\ &= C[x_1, \ldots, x_l]\sigma' \end{aligned}$$

where σ' is the substitution $\{F(x_1\sigma)/x_1, \ldots, F(x_l\sigma)/x_l\}$. Similarly, we can show that $F(N) \equiv C'[x_1, \ldots, x_l]\sigma'$. Therefore, we have $F(M) \to_{R_E} F(N)$.

- Suppose $M = g(u_1, \ldots, u_k)$ and $g \notin \Sigma_{E_i}$. Then M is an E_i-alien subterm of M, and since M is a quasi-E_i term, M must be in E-normal form. Therefore no reduction is possible, hence the lemma holds vacuously. □

Proposition 3.6. *Let E be a disjoint combination of $E_1, \ldots, E_n$. If M is a quasi-E_i term and $M \to^*_{R_E} N$, then N is a quasi-E_i term and $F_{E_i}(M) \to^*_{R_E} F_{E_i}(N)$.*

Proof. This follows directly from Lemma 3.5. □

Proposition 3.7. *Let E be a disjoint combination of $E_1, \ldots, E_n$. If M and N are quasi-E_i terms and $F_{E_i}(M) \to^*_{R_E} F_{E_i}(N)$, then $M \to^*_{R_E} N$.*

Proof. It is enough to show that this holds for the one-step rewrite $F_{E_i}(M) \to_{R_E} F_{E_i}(N)$. This can be done by induction on the structure of M. In particular, we need to show that a rewrite rule that applies to $F_{E_i}(M)$ also applies to M. Let $x_1, \ldots, x_k$ be the free variables in $F_{E_i}(M)$. Let $M_1, \ldots, M_k$ be normal E-terms such that $v_E(M_j) = x_j$ for each $j \in \{1, \ldots, k\}$, and

$$\sigma = \{M_1/x_1, \ldots, M_k/x_k\}.$$

Then we can show by induction on the structure of M and N, and using the fact that they are quasi-E_i terms, that

$$F_{E_i}(M)\sigma \equiv M \text{ and } F_{E_i}(N)\sigma \equiv N.$$

Note that for any rewrite rule in a rewrite system, by definition, we have that all the variables free in the right-hand side of the rule are also free in the left-hand side. Hence, the free variables of $F_{E_i}(N)$ are among the free variables in $F_{E_i}(M)$ since they are related by rewriting.

Now suppose there is a rewrite rule in R_E

$$C[y_1, \ldots, y_l] \to C'[y_1, \ldots, y_l]$$

where $C[..]$ and $C'[..]$ are E_i-contexts, such that $F_{E_i}(M) \equiv C[y_1, \ldots, y_l]\theta$ and $F_{E_i}(N) \equiv C'[y_1, \ldots, y_l]\theta$, for some substitution θ. Then we have

$$M \equiv F_{E_i}(M)\sigma \equiv (C[y_1, \ldots, y_l]\theta)\sigma \equiv C[y_1, \ldots, y_l](\theta \circ \sigma)$$

and

$$N \equiv F_{E_i}(N)\sigma \equiv (C'[y_1, \ldots, y_l]\theta)\sigma \equiv C'[y_1, \ldots, y_l](\theta \circ \sigma).$$

Hence we also have $M \to_{R_E} N$. □

3.2. **Cut elimination.** 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. Note that here the equational theory E contains at most one AC symbol.

Lemma 3.8. *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 $|\Pi| = |\Pi'|$.*

Proof. By induction on $|\Pi|$. □

Lemma 3.9. *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 $\Gamma, X, Y \vdash M$ has a cut-free derivation.*

Proof. Let Π be a cut-free derivation of $\Gamma, f(X, Y) \vdash M$. We construct a cut-free derivation Π' of $\Gamma, X, Y \vdash M$ by induction on $|f(X, Y)|$ with subinduction on $|\Pi|$. The only non-trivial cases are when Π ends with blind_{L2}, acting on $f(X, Y)$, and when Π ends with id and $f(X, Y)$ is used in the rule. We examine these cases in more detail below.

- Suppose Π ends with blind_{L2}, acting on $f(X, Y)$, i.e., $f = \mathsf{sign}$ and $X = \mathsf{blind}(N, R)$:

$$\dfrac{\overset{\Pi_1}{\Gamma, \mathsf{sign}(\mathsf{blind}(N, R), Y) \vdash R} \quad \overset{\Pi_2}{\Gamma, \mathsf{sign}(\mathsf{blind}(N, R), Y), \mathsf{sign}(N, Y), R \vdash M}}{\Gamma, \mathsf{sign}(\mathsf{blind}(N, R), Y) \vdash M} \; \mathsf{blind}_{L2}$$

Applying the inner induction hypothesis on derivation height to Π_1 and Π_2 we obtain two derivations Π_1' and Π_2' of

$$\overset{\Pi_1'}{\Gamma, \mathsf{blind}(N, R), Y \vdash R} \quad \text{and} \quad \overset{\Pi_2'}{\Gamma, \mathsf{blind}(N, R), Y, \mathsf{sign}(N, Y), R \vdash M}$$

Next we apply the outer induction hypothesis on the size of $f(X, Y)$ to decompose $\mathsf{sign}(N, Y)$ in the latter sequent to get a derivation Π_2'' of

$$\overset{\Pi_2''}{\Gamma, \mathsf{blind}(N, R), N, Y, R \vdash M}$$

The derivation Π' is constructed as follows:

$$\dfrac{\overset{\Pi_1'}{\Gamma, \mathsf{blind}(N, R), Y \vdash R} \quad \overset{\Pi_2''}{\Gamma, \mathsf{blind}(N, R), N, Y, R \vdash M}}{\Gamma, \mathsf{blind}(N, R), Y \vdash M} \; \mathsf{blind}_{L1}$$

- Suppose Π ends with id. The only non-trivial case is when $f(X, Y)$ is active in the rule, that is, we have

$$M \approx C[f(X, Y)^n, M_1, \ldots, M_k]$$

where $M_1, \ldots, M_k \in \Gamma$, $C[\ldots]$ is an E-context and $f(X, Y)$ fills n-holes in $C[\ldots]$. We distinguish several cases:

- There is an E-factor A of $M \cup \Gamma$ such that $f(X, Y) \equiv A$. Note that in this case A must be of the form $f(X', Y')$ for some $X' \equiv X$ and $Y' \equiv Y$. In this case, Π' is constructed as follows:

$$\dfrac{\overset{\Xi}{\Gamma, X, Y \vdash f(X', Y')} \quad \overset{id}{\Gamma, X, Y, f(X', Y') \vdash M}}{\Gamma, X, Y \vdash M} \; acut$$

where Ξ is a derivation formed using id and the right rules for the constructor f.

- Suppose that there is no E-factor A of $M \cup \Gamma$ such that $A \equiv f(X, Y)$. Note that since M is in normal form, we have

$$C[f(X, Y)^n, M_1, \ldots, M_k] \to^* M$$

and both $C[f(X, Y)^n, M_1, \ldots, M_k]$ and M are quasi-E terms.
Let $x = v(f(X, Y))$. It follows from Proposition 3.6 that

$$F_E(C[f(X, Y)^n, M_1, \ldots, M_k]) = C[x^n, F_E(M_1), \ldots, F_E(M_k)] \to^* F_E(M).$$

Since no factors of M and $M_1, \ldots, M_k$ are equivalent to $f(X, Y)$, x obviously does not appear in any of $F_E(M)$, $F_E(M_1), \ldots, F_E(M_k)$. Now let a be a name that does not

occur in Γ, X, Y or M. Since rewriting is invariant under variable/name substitution, by substituting a for x in the above sequence of rewrites, we have

$$F_E(C[a^n, M_1, \ldots, M_k]) = C[a^n, F_E(M_1), \ldots, F_E(M_k)] \to^* F_E(M).$$

Now by Proposition 3.7, we have

$$C[a^n, M_1, \ldots, M_k] \to^* M.$$

By substituting X for a in this sequence, we have

$$C[X^n, M_1, \ldots, M_k] \longrightarrow^*_{\mathcal{R}} M.$$

Thus, in this case, Π' is constructed by an application of id. $\qquad\square$

Lemma 3.10. *Let $X_1, \ldots, X_k$ be terms in normal form 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 $\Gamma, X_1, \ldots, X_k \vdash M$.*

Proof. By induction on $|\Pi|$. The cases where Π ends with id, or rules in which $f(X_1, \ldots, X_k)\!\downarrow$ is not principal, are trivial. The other cases, where Π ends with a rule applied to the term $f(X_1, \ldots, X_k)\!\downarrow$, are given in the following.

• Suppose Π ends with p_L on $f(X_1, \ldots, X_k)\!\downarrow$. This means that $f(X_1, \ldots, X_k)\!\downarrow$ is a pair $\langle U, V \rangle$ for some U and V, and Π is

$$\frac{\overset{\displaystyle \Xi}{\Gamma, \langle U, V \rangle, U, V \vdash M}}{\Gamma, \langle U, V \rangle \vdash M} \; p_L$$

We have that

$$f(X_1, \ldots, X_k) \to^* \langle U, V \rangle.$$

Let $x = F_E(\langle U, V \rangle)$. By Proposition 3.6, we have

$$f(F_E(X_1,), \ldots, F_E(X_k)) \to^* x.$$

Obviously, x has to occur in $F_E(X_i)$ for some X_i. Without loss of generality, assume that $i = 1$. This means that there exists an E-alien subterm A of X_1 such that $A = \langle U', V' \rangle$ and $U \equiv U'$ and $V \equiv V'$. There are two cases to consider.

− A is a factor of X_1. Then Π' is the derivation:

$$\frac{\overline{\Gamma, X_1, \ldots, X_k \vdash \langle U', V' \rangle} \; id \quad \overset{\displaystyle \Pi_1}{\Gamma, X_1, \ldots, X_k, \langle U', V' \rangle \vdash M}}{\Gamma, X_1, \ldots, X_k \vdash M} \; acut$$

The instance of id above is valid since $\langle U', V' \rangle \equiv \langle U, V \rangle \approx f(X_1, \ldots, X_k)$. The derivation Π_1 is obtained by weakening Π with $X_1, \ldots, X_k$ and applying Lemma 3.8 to replace $\langle U, V \rangle$ with its equivalent $\langle U', V' \rangle$.

− A is not a factor of X_1. This can only mean that either $X_1 = A$ or that every occurrence of A in X_1 is as immediate subterm of another E-alien subterm. The latter would mean that A would not be abstracted by F_{E_i} at all, contradicting the assumption that it is. So it must be the case that $X_1 = A$. Then Π' is the derivation

$$\frac{\overset{\displaystyle \Xi'}{\Gamma, \langle U', V' \rangle, U', V', X_2, \ldots, X_k \vdash M}}{\Gamma, \langle U', V' \rangle, X_2, \ldots, X_k \vdash M} \; p_L$$

where Ξ' is obtained by weakening Ξ with $X_2, \ldots, X_k$, and then applying Lemma 3.8 to replace U and V with their equivalent U' and V'.

The cases where $f(X_1, \ldots, X_k)\!\downarrow$ is headed with some other constructor are proved analogously.

- Suppose Π ends with *acut* which abstracts an E-factor of $f(X_1, \ldots, X_k)\!\downarrow$:

$$\frac{\overset{\Pi_1}{\Gamma' \vdash A} \quad \overset{\Pi_2}{\Gamma', A \vdash M}}{\Gamma, f(X_1, \ldots, X_k)\!\downarrow \,\vdash M} \; acut$$

where A is an E-factor of $f(X_1, \ldots, X_k)\!\downarrow$ and $\Gamma' = \Gamma \cup \{f(X_1, \ldots, X_k)\!\downarrow\}$. In this case, we have that

$$f(X_1, \ldots, X_k)\!\downarrow \, = C[g(\ldots, A, \ldots)]$$

for some context $C[]$ and some $g \in \Sigma_E$. By Proposition 3.6, we have

$$f(F_E(X_1,), \ldots, F_E(X_k)) \to^* F_E(C[g(\ldots, A, \ldots)]).$$

We have a couple of cases to analyse, depending on whether that particular occurrence of A is abstracted by F_E or not (i.e., if $g(\ldots, A, \ldots)$ is nested inside another E-alien subterm). In both cases, it can be shown that there exist $A' \equiv A$ and some X_i such that either $A' = X_i$ or A' is an E-factor of X_i. For the latter case, Π' is constructed as follows:

$$\frac{\overset{\Pi'_1}{\Gamma'' \vdash A'} \quad \overset{\Pi'_2}{\Gamma'', A' \vdash M}}{\Gamma, X_1, \ldots, X_k \vdash M} \; acut$$

where $\Gamma'' = \Gamma \cup \{X_1, \ldots, X_k\}$ and Π'_1 and Π'_2 are obtained by applying the induction hypothesis on Π_1 and Π_2, followed by applications of Lemma 3.8 to replace A with its equivalent A'. If $X_1 = A'$ then Π' is obtained by weakening Π_2 with $X_2, \ldots, X_k$, followed by an application of Lemma 3.8 to replace A with A'. $\qquad \square$

Lemma 3.11. *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 $\Gamma, M_1, \ldots, M_k \vdash M$.*

Proof. By induction on the size of $C[\ldots]$, Lemma 3.8 and Lemma 3.10. $\qquad \square$

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 rules for $\{M\}_K$, on both the left and 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 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 3.12. *The cut rule is admissible for $\mathcal{S}$.*

Proof. We give a set of transformation rules for derivations ending with cuts and show that given any derivation, there is a sequence of reductions that applies to this derivation, and terminates with a cut free derivation with the same end sequent. This is proved by induction on the height of the *left premise derivation* immediately above the cut rule. This measure is called the *cut rank*. As usual in cut elimination, we proceed by eliminating the topmost instances of cut with the highest rank. So in the following, we suppose a given derivation

Π ending with a cut rule, which is the only cut in Π, and then show how to transform this to a cut free derivation Π'.

The cut reduction is driven by the left premise derivation of the cut. We distinguish several cases, based on the last rule of the left premise derivation.

(1) Suppose the left premise of Π ends with either p_R, e_R, sign_R or blind_R, thus Π is

$$
\cfrac{\cfrac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ \Gamma \vdash M & \Gamma \vdash N\end{array}}{\Gamma \vdash f(M,N)}\ \rho \qquad \cfrac{\Pi_3}{\Gamma, f(M,N) \vdash R}}{\Gamma \vdash R}\ cut
$$

where f is a constructor and ρ is its right introduction rule. By Lemma 3.9, we have a cut free derivation Π'_3 of $\Gamma, M, N \vdash R$. By applying Lemma 2.4 to Π_2, we also have a cut-free derivation Π'_2 of $\Gamma, M \vdash N$ such that $|\Pi_2| = |\Pi'_2|$. The above cut is then reduced to

$$
\cfrac{\cfrac{\Pi_1}{\Gamma \vdash M} \qquad \cfrac{\cfrac{\begin{array}{cc}\Pi'_2 & \Pi'_3 \\ \Gamma, M \vdash N & \Gamma, M, N \vdash R\end{array}}{\Gamma, M \vdash R}\ cut}{}}{\Gamma \vdash R}\ cut \ .
$$

These two cuts can then be eliminated by induction hypothesis since their left premises are of smaller height than the left premise of Π.

(2) Suppose the left premise of the cut ends with a left rule acting on Γ. We show here the case where the left-rule has only one premise; generalisation to the other case (with two premises) is straightforward. Therefore Π is of the form:

$$
\cfrac{\cfrac{\cfrac{\Pi_1}{\Gamma' \vdash M}}{\Gamma \vdash M}\ \rho \qquad \cfrac{\Pi_2}{\Gamma, M \vdash R}}{\Gamma \vdash R}\ cut
$$

By inspection of the inference rules in Figure 2, it is clear that in the rule ρ above, we have $\Gamma \subseteq \Gamma'$. We can therefore weaken Π_2 to a derivation Π'_2 of $\Gamma', M \vdash R$ with $|\Pi_2| = |\Pi'_2|$. The cut is then reduced as follows.

$$
\cfrac{\cfrac{\cfrac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ \Gamma' \vdash M & \Gamma', M \vdash R\end{array}}{\Gamma' \vdash R}\ cut}{\Gamma \vdash R}\ \rho}{}
$$

The cut rule above ρ can be eliminated by induction hypothesis, the height of the left premise of the cut is smaller than that of the left premise of the original cut.

(3) Suppose the left premise of the cut ends with $acut$, but using an E-factor of the right hand side of the sequent, i.e., Π is

$$
\cfrac{\cfrac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ \Gamma \vdash A & \Gamma, A \vdash C[A]\end{array}}{\Gamma \vdash C[A]}\ acut \qquad \cfrac{\Pi_3}{\Gamma, C[A] \vdash R}}{\Gamma \vdash R}\ cut
$$

Then this derivation reduces to:

$$\cfrac{\Pi_1 \quad \cfrac{\cfrac{\Pi_2}{\Gamma, A \vdash C[A]} \quad \cfrac{\Pi_3'}{\Gamma, A, C[A] \vdash R}}{\Gamma, A \vdash R} \; cut}{\Gamma \vdash R} \; cut$$

The derivation Π_3' is obtained by weakening Π_3 with A (Lemma 2.4). Both cuts can be removed by induction hypothesis (the upper cut followed by the lower cut).

(4) Suppose the left premise of the cut ends with the *id*-rule:

$$\cfrac{\cfrac{}{\Gamma \vdash M} \; id \quad \cfrac{\Pi_1}{\Gamma, M \vdash R}}{\Gamma \vdash R} \; cut$$

where $M = C[M_1, \ldots, M_k]\!\downarrow$ and $M_1, \ldots, M_k \in \Gamma$. In this case, we apply Lemma 3.11 to Π_1, hence we get a cut free derivation Π' of $\Gamma \vdash R$. $\square$

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 to be decidable for several AC theories, e.g., exclusive-or, abelian groups and their extensions with a homomorphism axiom [11, 8, 15, 14, 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 4.1. 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 3.6 and Proposition 3.7, 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 "sub-formula" 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 structure of cut-free derivations. Recall that the rules $p_L, e_L, \mathsf{sign}_L, \mathsf{blind}_{L1}, \mathsf{blind}_{L2}$ and *acut* are called left rules (the other rules are right rules). Central to the decidability results in this section is the notion of a normal derivation, given in the following definition.

Definition 4.2. 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).

Lemma 4.3. *Let Π be a cut-free derivation of $\Gamma \vdash M$. Then there is a cut-free derivation of the same sequent such that all the right rules appear above left rules.*

Proof. We permute any offending right rules up over any left rules. This is done by induction on the number of occurrences of the offending rules. We first show the case where Π has at most one offending right rule. In this case, we show, by induction on the height of Π, that any offending right-introduction rule can be permuted up in the derivation tree until it is above any left-introduction rule. We show here a non-trivial case involving *acut*; the others are treated analogously. Suppose Π is as shown below at left where ρ denotes a right introduction rule for the constructor f and A is an E-factor of $\Gamma \cup \{M\}$. By the weakening lemma (Lemma 2.4), we have a derivation Π'_3 of $\Gamma, A \vdash N$ with $|\Pi'_3| = |\Pi_3|$. The original derivation Π is then transformed into the derivation shown below at right:

$$
\cfrac{\cfrac{\cfrac{\Pi_1}{\Gamma \vdash A} \quad \cfrac{\Pi_2}{\Gamma, A \vdash M}}{\Gamma \vdash M} \; acut \quad \cfrac{\Pi_3}{\Gamma \vdash N}}{\Gamma \vdash f(M, N)} \; \rho
\qquad
\cfrac{\cfrac{\Pi_1}{\Gamma \vdash A} \quad \cfrac{\cfrac{\Pi_2}{\Gamma, A \vdash M} \quad \cfrac{\Pi'_3}{\Gamma, A \vdash N}}{\Gamma, A \vdash f(M, N)} \; \rho}{\Gamma \vdash f(M, N)} \; acut
$$

The rule ρ in the right premise can then be further permuted up (i.e., if Π_2 or Π'_3 ends with a left rule) by induction hypothesis.

The derivation Π' is then constructed by repeatedly applying the above transformation to the topmost offending rules until all of them appear above left-introduction rules. □

Proposition 4.4. *If $\Gamma \vdash M$ is derivable then it has a normal derivation.*

Proof. Let Π be a cut-free derivation of $\Gamma \vdash M$. By Lemma 4.3, we can assume without loss of generality that all the right rules in Π appear above the left rules. We construct a normal derivation Π' of the same sequent by induction on the number of offending left rules in Π.

We first consider the case where Π has at most one offending left rule. Let Ξ be a subtree of Π where the offending rule occurs, i.e., Ξ ends with a branching left rule, whose left premise derivation ends with a left rule. We show by induction on the height of the left premise derivation of the last rule in Ξ that Ξ can be transformed into a normal derivation. There are two cases to consider: one in which the left premise derivation ends with a branching left rule and the other where it ends with a non-branching left rule. We consider the former case here, the latter can be dealt with analogously. So suppose Ξ is of the form:

$$
\cfrac{\cfrac{\cfrac{\Pi_1}{\Gamma_1 \vdash N_2} \quad \cfrac{\Pi_2}{\Gamma_2 \vdash N_1}}{\Gamma_1 \vdash N_1} \; L_2 \quad \cfrac{\Pi_3}{\Gamma_3 \vdash M'}}{\Gamma_1 \vdash M'} \; L_1
$$

where L_1 is a left rule, and Π_1, Π_2 and Π_3 are normal derivations, $\Gamma_2 \supseteq \Gamma_1$ and $\Gamma_3 \supseteq \Gamma_1$. We first weaken Π_3 into a derivation Π'_3 of $\Gamma_4 \vdash M'$, where $\Gamma_4 = \Gamma_2 \cup \Gamma_3$. Such a weakening can be easily shown to not affect the shape of the derivations (i.e., it does not introduce or

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

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

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

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

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

$$\frac{\Gamma, A \vdash M}{\Gamma \vdash M} \; ls, \text{where } A \text{ is an } E\text{-factor of } \Gamma \cup \{M\} \text{ and } \Gamma \Vdash_{\mathcal{R}} A.$$

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

remove any rules in Π_3). Ξ is then transformed into

$$\frac{\Pi_1 \qquad \dfrac{\Pi_2 \qquad \Pi_3'}{\dfrac{\Gamma_2 \vdash N_1 \quad \Gamma_4 \vdash M'}{\Gamma_2 \vdash M'} \; L_1}}{\dfrac{\Gamma_1 \vdash N_2}{\Gamma_1 \vdash M'} } \; L_2$$

By inspection of the rules in Figure 2, it can be shown that this transformation is valid for any pair of left rules (L_1, L_2). Note that this transformation may introduce at most two offending left rules, i.e., if Π_1 and/or Π_2 end with left rules. But notice that the left premise derivations of both L_1 and L_2 in this case have smaller height than the left premise derivation of L_1 in Ξ. By induction hypothesis, the right premise derivation of L_2 can be transformed into a normal derivation, say Π_4, resulting in

$$\frac{\Pi_1 \qquad\qquad \Pi_4}{\dfrac{\Gamma_1 \vdash N_2 \quad \Gamma_2 \vdash M'}{\Gamma_1 \vdash M'}} \; L_2$$

By another application of the induction hypothesis, this derivation can be transformed into a normal derivation.

The general case where Π has more than one offending rules can be dealt with by transforming the topmost occurrences of the left rule, one by one, following the above transformation. $\qquad\square$

In a normal derivation, the left branch of a branching left rule is derivable using only right rules and id. This means that we can represent a normal derivation as a sequence (reading the derivation 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 derivable 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 4.5. *A sequent* $\Gamma \vdash M$ *is derivable in* $\mathcal{S}$ *if and only if it is derivable in* $\mathcal{L}$.

Proof. This follows immediately from cut elimination for $\mathcal{S}$ and the normal form for $\mathcal{S}$ (Proposition 4.4). $\qquad\square$

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 $st(\Gamma)$. We write $pst(\Gamma)$ for the set of proper subterms of Γ, and write $St(\Gamma)$ for the *saturated set* of Γ, where

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

The set $sst(\Gamma)$ is needed so that the saturated set is closed under the unblinding operation, i.e., the bottom-up application of the blind_2-rule. 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 the 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 cardinality of $St(\Gamma \cup \{M\})$. We denote with $\#(\Sigma)$ the cardinality of the set Σ.

Definition 4.6. 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 4.7. *Let* Π *be an* $\mathcal{L}$-*derivation of* $\Gamma \vdash M$. *Then for every sequent* $\Gamma' \vdash M'$ *occurring in* Π, *we have* $\Gamma' \cup \{M'\} \subseteq St(\Gamma \cup \{M\})$.

Proof. By induction on $|\Pi|$. It is enough to show that for each rule ρ in $\mathcal{L}$ other than r

$$\frac{\Gamma' \vdash M'}{\Gamma \vdash M} \; \rho$$

we have that $St(\Gamma \cup \{M\}) = St(\Gamma' \cup \{M'\})$.

The non-trivial case is the rule blind_2:

$$\frac{\Gamma_1, \mathsf{sign}(\mathsf{blind}(N, R), K), \mathsf{sign}(N, K), R \vdash M}{\Gamma_1, \mathsf{sign}(\mathsf{blind}(N, R), K) \vdash M} \; \mathsf{blind}_2$$

where $\Gamma = \Gamma_1 \cup \{\mathsf{sign}(\mathsf{blind}(N, R), K)\}$. The premise of the rule has a term $\mathsf{sign}(N, K)$ which may not occur in the conclusion. However, the proper subterms of $\mathsf{sign}(N, K)$ are included

in the proper subterms of $\mathsf{sign}(\mathsf{blind}(N,R),K)$, hence both the premise and the conclusion have the same set of proper subterms. Notice that $\mathsf{sign}(N,K) \in sst(\Gamma)$, since both N and K are in $pst(\Gamma)$. Therefore in this case we also have that $St(\Gamma \cup \{M\}) = St(\Gamma' \cup \{M'\})$. □

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

Lemma 4.8. *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 $\#(St(\Gamma \cup \{M\}))$.*

Proof. We first note that any derivation of $\Gamma \vdash M$ can be turned into one in which every sequent in the derivation occurs exactly once on a branch. Our rules preserve their principal formula when read upwards from conclusion to premise, hence the left hand sides of the sequents as we go up a branch accumulate more and more formulae. That is, they form an increasing chain. At worst, each such rule adds only one formula from $St(\Gamma \cup \{M\})$. Thus, by Lemma 4.7, the number of different sequents on a branch is bounded by the cardinality of $St(\Gamma \cup \{M\})$. □

Another useful observation is that the left-rules of $\mathcal{L}$ are *invertible*; at any point in a bottom-up proof search, we do not lose derivability 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.

We now show that the decision problem $\Gamma \Vdash M$ is polynomially reducible to the elementary deduction problem. This proof will make use of the linear proof system $\mathcal{L}$. Since the side conditions in some rules in $\mathcal{L}$ depend on $\Vdash_{\mathcal{R}}$, we first need to prove this reducibility result for $\Vdash_{\mathcal{R}}$. This is straightforward since the right introduction rules do not modify messages in the left hand side of the sequent, hence, if m is the number of distinct subterms of M, checking this deducibility relation amounts to checking at most m instances of $\Vdash_E$ on subterms of M.

Lemma 4.9. *The decidability of the relation $\Vdash_{\mathcal{R}}$ is polynomially reducible to the decidability of elementary deduction $\Vdash_E$.*

Proof. Recall that the relation $\Gamma \Vdash_{\mathcal{R}} M$ holds if we can derive $\Gamma \vdash M$ using only right-rules and *id*. Here is a simple proof search procedure for $\Gamma \vdash M$, using only right-rules:

(1) If $\Gamma \vdash M$ is elementarily deducible, then we are done.
(2) Otherwise, apply a right-introduction rule (backwards) to $\Gamma \vdash M$ and repeat step 1 for each obtained premise, and so on. If no such rules are applicable, then $\Gamma \vdash M$ is not derivable.

There are at most n iterations where n is the number of distinct subterms of M. Note that the check for elementary deducibility in step 1 is done on problems of size less or equal to $\#(St(\Gamma \cup M))$. □

Before we proceed with proving the main decidability result (Theorem 4.10 below), let us first define the notion of a *principal term* in a left-rule in the proof system $\mathcal{L}$ (we refer to Figure 3 in the following definition):

- $\langle M, N \rangle$ is the principal term of lp
- $\{M\}_K$ is the principal term of le
- $\mathsf{sign}(M,K)$ is the principal term of sign
- $\mathsf{blind}(M,K)$ is the principal term of blind_1
- $\mathsf{sign}(\mathsf{blind}(M,R),K)$ is the principal term of blind_2

- A is the principal term of ls.

Given a sequent $\Gamma \vdash M$ and a pair of principal-term and a left-rule (N, ρ), we say that the pair (N, ρ) is *applicable* to the sequent if

- ρ is ls, N is a factor of $\Gamma \cup \{M\}$, and there is an instance of ρ with $\Gamma, N \vdash M$ as its premise;
- ρ is not ls, $N \in \Gamma$, and there is an instance of ρ with $\Gamma \vdash M$ as its conclusion.

Let us assume that the complexity of $\Vdash_E$ is $O(f(n))$. Given a sequent $\Gamma \vdash M$ and a pair of principal-term and a left-rule (N, ρ), we note the following two facts:

F1: the complexity of checking whether (N, ρ) is applicable to $\Gamma \vdash M$ is $O(n^l f(n))$ for some constant l;

F2: if (N, ρ) is applicable to $\Gamma \vdash M$, then there is a unique sequent $\Gamma' \vdash M$ such that the sequent below is a valid instance of ρ:

$$\frac{\Gamma' \vdash M}{\Gamma \vdash M} \ \rho$$

Note that for (F1) to hold, we need to assume a DAG representation of sequents with maximal sharing of subterms. The complexity of checking whether a rule is applicable or not then consists of

- pointer comparisons;
- pattern matching a subgraph with a rule;
- checking equality modulo associativity and commutativity (for the rule sign);
- and checking $\Vdash_\mathcal{R}$.

The first three can be done in polynomial time; and the last one is polynomially reducible to $\Vdash_E$ (Lemma 4.9).

Theorem 4.10. *The decidability of the relation $\Vdash_\mathcal{L}$ is polynomially reducible to the decidability of elementary deduction $\Vdash_E$.*

Proof. Let n be the size of $St(\Gamma \cup \{M\})$. Notice that the left-rules in Figure 3 are invertible (they accumulate terms, reading the rules bottom-up), so one does not lose derivability by applying any of the rules in proof search. Thus by blindly applying the left-rules, we eventually reach a point where the right-rule (r) is applicable, hence the original sequent is derivable, or we reach a "fix point" where we encounter all previous sequents. For the latter, we show that there is a polynomial bound to the number of rule applications we need to try before concluding that the original sequent is not provable.

Let $M_1, \ldots, M_n$ be an enumeration of the set $St(\Gamma \cup \{M\})$. Suppose $\Gamma \vdash M$ is provable in $\mathcal{L}$. Then there is a shortest derivation in Γ where each sequent appears exactly once in the (linear) derivation. This also means that there exists a sequence of principal-term-and-rule pairs

$$(M_{i_1}, \rho_1), \ldots, (M_{i_q}, \rho_q)$$

that are applicable, successively, to $\Gamma \vdash M$. Note that $q \leq n$ by Lemma 4.8.

A simple proof search strategy for $\Gamma \vdash M$ is therefore to repeatedly try all possible applicable pairs (M', ρ') for each possible $M' \in St(\Gamma \cup \{M\})$ and each left-rule ρ'. More precisely: Let $j := 0$ and initialise $\Delta := \Gamma$

(1) $j := j + 1$.
(2) If $\Delta \Vdash_\mathcal{R} M$ then we are done.
(3) Otherwise, for $k = 1$ to n do

for every left-rule ρ do

if (M_k, ρ) is applicable to $\Delta \vdash M$, then let $\Gamma_1 \vdash M$ be the unique premise of ρ determined by (M_k, ρ) via **F2** and let $\Delta := \Gamma_1$.

(4) If $j \leq n$ then go to step 1.

If the original sequent is derivable, then at each iteration j, the algorithm (i.e., step 3) will find the correct pair (M_{i_j}, ρ_j). (Strictly speaking, the algorithm finds the j-th pair of a shortest derivation, and not necessarily the one given above, since there can be more than one derivation of a given length.) Note that the algorithm does not construct the shortest derivation, but at each j iteration, it will guess correctly the j-th pair of such a derivation if one exists. If no derivation is found after n (outer) iterations, then the original sequent is not derivable, since the length of any shortest derivation is bound by n by Lemma 4.8. By Lemma 4.9, step 2 takes $O(n^a f(n))$ for some constant a. By (**F1**) above, each iteration in step 3 takes $O(n^b f(n))$ for some constant b. Since there are at most $6n$ distinct principal-term-and-rule pairs, this means step 3 takes $O(6n^{b+1} f(n))$. Therefore the whole procedure takes $O(n^{c+1} f(n))$ where c is the greater of a and $b+1$. Hence the complexity of $\Vdash_{\mathcal{L}}$ is polynomially reducible to $\Vdash_E$. $\qquad\square$

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

5. COMBINING DISJOINT CONVERGENT THEORIES

We now consider a slightly more general intruder deduction problem than the previous sections: we shall allow any AC convergent theory which is obtained from a union of pairwise disjoint convergent AC theories. That is, the AC theory E in this case can be a disjoint combination of AC convergent theories $E_1, \ldots, E_n$, where 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. The notions of subterms, factors, alien terms, etc., carry over to this more general setting, but we shall be mostly concerned with the constituent theories E_i's, so we shall be speaking of E_i-alien terms, E_i-factors, etc.

The sequent system $\mathcal{S}$ needs to be modified slightly to accomodate this combination of theories. Throughout this section, we shall consider a sequent system $\mathcal{D}$, whose rules are those of $\mathcal{S}$, but with id replaced by the rule id_{E_i} below left and with the rule $acut$ below right:

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

where N is an E_i-factor of $\Gamma \cup \{M\}$. Notice that the sequent system $\mathcal{S}$ is then just a special case of $\mathcal{D}$ where E contains only a single AC operator. Note that in the proviso of the id_{E_i} rule, we require that $M \approx_E C[M_1, \ldots, M_k]$. However, as a consequence Proposition 3.6 and Proposition 3.7, we have

$$\begin{array}{rll} M \approx_E C[M_1, \ldots, M_k] & \text{iff} & C[F_E(M_1), \ldots, F_E(M_k)] \approx_E F_E(M) \\ & \text{iff} & C[F_E(M_1), \ldots, F_E(M_k)] \approx_{E_i} F_E(M). \end{array}$$

That is, in applying the id_{E_i} rule, one can abstract all the E_i-alien subterms from the sequent and check for equality in the theory E_i, rather than E.

A straightforward adaptation of the proof of Proposition 2.7 gives an analog of it for $\mathcal{D}$.

Proposition 5.1. *The judgment $\Gamma \vdash M$ is derivable in the natural deduction system $\mathcal{N}$, under theory E, if and only if $\Gamma{\downarrow}\vdash M{\downarrow}$ is derivable 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 crucial part of the proof in this case relies on the variable abstraction technique (Proposition 3.6 and Proposition 3.7), which applies to disjoint combination of theories. We can then prove the analog of the decomposition lemmas (Lemma 3.9 and Lemma 3.10), given below.

Lemma 5.2. *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 $\Gamma, X, Y \vdash M$.*

Proof. This is proved analogously to Lemma 3.9. $\qquad\qquad\square$

Lemma 5.3. *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 $f \in \Sigma_{E_i}$. Then there exists a cut-free derivation Π' of $\Gamma, X_1, \ldots, X_k \vdash M$.

Proof. By induction on $|\Pi|$. As in the proof of Lemma 3.10, we do case analyses on the last rule of Π. The cases involving constructors are the same as in the proof of Lemma 3.10. The non-trivial cases are when Π ends with either *id* or *acut*.

- Suppose Π ends with id_{E_j}: That is, we have

$$C[f(X_1, \ldots, X_k){\downarrow}^n, M_1, \ldots, M_l] \approx M$$

  for some E_j-context $C[\ldots]$. If $i = j$ then $f \in \Sigma_{E_j}$ and the sequent $\Gamma, X_1, \ldots, X_k \vdash M$ is provable by an application of id_{E_j} using the E_j-context $C[f(\ldots)^n, \ldots]$.

  Otherwise, we have that $i \neq j$. Let $R = f(X_1, \ldots, X_k){\downarrow}$. There are two subcases to consider:

  − R is an E_j-alien term. Suppose $v(R) = x$. Then by Proposition 3.6 we have

$$F_{E_j}(C[R^n, M_1, \ldots, M_l]) = C[x^n, F_{E_j}(M_1), \ldots, F_{E_j}(M_l)] \to^* F_{E_j}(M).$$

  If x does not occur in $F_{E_j}(M)$ then, using the same line of arguments as in the proof of Lemma 3.9, it can be shown that

$$C[X_1, M_1, \ldots, M_l] \approx M,$$

  hence Π' in this case is a simple application of id_{E_j}.

  Otherwise, if x does occur in $F_{E_j}(M)$, then it can be shown that there exists $R' \equiv R$ such that either $R' = M$ or R' is an E_j-factor of M. For the former case, Π' is simply an application of the id_{E_i} rule, since $f(X_1, \ldots, X_k) \approx M$. For the latter case, we can apply the *acut* rule to abstract R' from M:

$$\dfrac{\dfrac{f(X_1, \ldots, X_k) \approx R'}{\Gamma, X_1, \ldots, X_k \vdash R'}\ id_{E_i} \quad \dfrac{C[R'^n, M_1, \ldots, M_l] \approx M}{\Gamma, R', X_1, \ldots, X_k \vdash M}\ id_{E_j}}{\Gamma, X_1, \ldots, X_k \vdash M}\ acut$$

  − R is not an E_j-alien term, i.e., R is headed by some $g \in E_j$. This means that R is an E_i-alien term. Since $f(X_1, \ldots, X_k) \to^* R$, again using variable abstraction, it can be shown that there exists $R' \equiv R$ such that either $R' \equiv X_p$ or R' is an E_i-factor of X_p. In either case, it is easy to construct a derivation of $\Gamma, X_1, \ldots, X_k \vdash M$.

- Suppose Π ends with *acut*

$$\dfrac{\overset{\displaystyle \Pi_1}{\Gamma, f(X_1,\ldots,X_k){\downarrow}\vdash A} \quad \overset{\displaystyle \Pi_2}{\Gamma, f(X_1,\ldots,X_k){\downarrow}, A \vdash M}}{\Gamma, f(X_1,\ldots,X_k){\downarrow}\vdash M} \ acut$$

where A is an E_j-factor of $f(X_1,\ldots,X_k){\downarrow}$. Note that A in this case must be headed by a function symbol not in Σ_{E_j}.

If $i = j$ then we have

$$f(X_1,\ldots,X_k){\downarrow} = C[g(\ldots A \ldots)]$$

for some context $C[\ldots]$ and some $g \in \Sigma_{E_i}$. Again, using variable abstraction, it can be shown that there exists $A' \equiv A$ and some X_p such that either $A' = X_p$ or A' is an E_i-factor of X_p. For the former case, the derivation Π' is obtained by applying the induction hypothesis to Π_2. For the latter case, the derivation Π' is constructed as follows

$$\dfrac{\overset{\displaystyle \Pi'_1}{\Gamma, X_1,\ldots,X_k \vdash A'} \quad \overset{\displaystyle \Pi'_2}{\Gamma, X_1,\ldots,X_k, A' \vdash M}}{\Gamma, X_1,\ldots,X_k \vdash M} \ acut$$

where Π'_1 and Π'_2 are obtained from the induction hypothesis, followed by applications of Lemma 3.8.

If $i \neq j$, then $g \notin \Sigma_{E_i}$ and therefore $g(\ldots A \ldots)$ is an E_i-alien term. In this case, there must exist $B \equiv g(\ldots A \ldots)$ such that B is a subterm of some X_p. In other words, A is an E_j-factor of X_p. So Π' in this case is constructed as in the derivation figure above. $\qquad\Box$

We state the theorem below and omit the proof since it is a straightforward adaptation of the cut elimination proof for $\mathcal{S}$.

Theorem 5.4. *The cut rule is admissible for $\mathcal{D}$.*

Proof. Analogous to the proof of Theorem 3.12, making use of Lemmas 5.2 and 5.3. $\qquad\Box$

The decidability result for $\mathcal{S}$ also holds for $\mathcal{D}$. Its proof is basically the same as the decidability result for $\mathcal{S}$. That is, we first show that derivations in $\mathcal{D}$ admits the same normal form as in $\mathcal{S}$. It then remains to design a linear proof system for $\mathcal{D}$. This is the same as $\mathcal{L}$, except that the side condition of ls is modified slightly:

$$\dfrac{\Gamma, N \vdash M}{\Gamma \vdash M} \ ls$$

where N is an E_i-factor of $\Gamma \cup \{M\}$ and and $\Gamma \Vdash_{\mathcal{R}} N$. We denote with $\mathcal{LD}$ the linear proof system obtained from $\mathcal{L}$ by changing the ls rule to the above one. Then the following proposition is straightforward.

Proposition 5.5. *Every sequent $\Gamma \vdash M$ is derivable in $\mathcal{D}$ if and only if it is derivable 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. Note that here we only talk about the maximal complexity of the elementary deduction in the *constituent theories*, and not the elementary deduction in the combined theory E, which may be higher.

Theorem 5.6. *The decidability of the relation $\Vdash_{\mathcal{LD}}$ is polynomially reducible to the decidability of elementary deductions $\Vdash_{E_1}, \ldots, \Vdash_{E_n}$.*

6. Deducibility constraints for Dolev-Yao intruders

We now consider a constraint problem that arises from analysis of security protocols for a bounded number of sessions. This typically assumes an active intruder which can synthesize messages from a set of known messages, intercepted during runs of protocols, to affect the running of the protocols. Since there could be infinitely many such messages, these need to be represented symbolically as variables. As have been shown in a number of previous works [20, 7, 10], the problem of finding an attack on a protocol for a bounded number of sessions (typically, violation of secrecy or authentication properties) can be mapped into the problem of solving *deducibility constraints*. The latter are essentially a list of sequents, possibly with occurrences of variables, and finding attacks to a protocol then correspond to finding substitutions to the variables such that the instances of the sequents under those substitutions are derivable in the inference system modeling the intruder's abilities. We shall not delve into the specifics of the mapping from protocol analysis into deducibility constraints; the interested reader can consult the existing literature on the subject, e.g., [20, 10]. In this section, we report on our preliminary study on how sequent calculus can be applied to solve the deducibility constraint problem in a limited setting, where the intruder model does not assume any equational theories. For future work, we intend to study the more general deducibility constraint problems involving AC convergent theories.

We note that the main results in this section have been formally verified in the Isabelle/HOL proof assistant. The proof scripts are available via the web (given in the introduction).

We shall be concerned only with Dolev-Yao intruders in this section, i.e., we restrict to the constructors $\langle .,. \rangle$ and $\{.\}_.$, and an empty equational theory. For this class of intruders, the deducibility constraint problem has been shown decidable in several existing works [7, 20, 21, 10]. In particular, our constraint reduction rules bear some similarity with the reduction rules in [20]. We shall, however, prove a stronger result, which is that every deducibility constraint system is satisfiable if and only if it can be transformed into a certain solved form, in which its solvability is immediate. A procedure for this transformation has been given recently in [10] using a natural deduction formulation of the intruder model. Our aim here is to illustrate how the sequent calculus can be used to solve the deducibility constraint problem.

Note that since we restrict to Dolev-Yao intruders, the rule *acut* becomes redundant, since there could be no E-factors in messages composed using constructors alone. Therefore in this case, the sequent system $\mathcal{S}$ can be simplified to the one given in Figure 4.

Definition 6.1. A *deducibility constraint* is an expression of the form $\Sigma \Vdash^? M$ (called a *proper deducibility constraint*) or $\Sigma \Vdash^?_R M$ (called a *right-deducibility constraint*), where Σ is a set of messages and M is a message. Σ here is called the left side of the constraint and M its right side. We write $\Sigma \Vdash^?_{(R)} M$ to denote a constraint generally without referring to its specific form.

Intuitively, the constraint $\Sigma \Vdash^? M$ denotes the problem of finding a derivable instance of the sequent $\Sigma \vdash M$, while the constraint $\Sigma \Vdash^?_R M$ denotes the problem of finding an

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

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

Figure 4: Sequent system for Dolev-Yao intruders

instance of the sequent $\Sigma \vdash M$ that is derivable using only the identity and the right-rules. The separation of constraints into these two kinds is motivated by the structure of normal derivations, which separates proof search into general deducibility and right-deducibility. Indeed, our decision procedure for solving constraints exploits the structure of normal derivations.

If C is a list of constraints, then $V(C)$ denotes the set of variables occuring in C. A *substitution* is a mapping from variables to terms. It is extended to a mapping from terms to terms in the usual way. We denote with $dom(\theta)$ the *domain* of the substitution θ, and $ran(\theta)$ denotes its range. We denote with ϵ the substitution with empty domain, i.e., the identity map on variables. A substitution θ is a *ground substitution* if $\theta(x)$ is a ground message for every $x \in dom(\theta)$. Application of a substitution θ to a message M is written in a postfix notation, i.e., $M\theta$. This notation generalises to sets of terms, sequents, constraints, etc., in the obvious way, e.g., $\Gamma\theta$ denotes the set of messages obtained from applying the substitution θ to each member of the set. Composition of substitutions is written $\theta \circ \rho$ and is defined as $M(\theta \circ \rho) = (M\theta)\rho$.

Definition 6.2. A ground substitution θ is a *solution to a list of deducibility constraints* C if
- for every $\Sigma \Vdash^? M \in C$, we have $\Sigma\theta \Vdash M\theta$, and
- for every $\Sigma \Vdash^?_R M \in C$, we have $\Sigma\theta \Vdash_R M\theta$.

We say that C is *satisfiable* if there is a solution for C.

Given a list of constraints C and an index i, we write C^i to denote the prefix of C of length $(i-1)$. So, if C is, for example,

$$(\Sigma_1 \Vdash^? M_1); (\Sigma_2 \Vdash^? M_2); (\Sigma_3 \Vdash^? M_3)$$

then C^1 is the empty list; C^2 is the singleton list $(\Sigma_1 \Vdash^? M_1)$. Obviously, if θ is a solution for C then it is also a solution for any of its prefixes.

In the following, given Σ_1 and Σ_2, we write $\Sigma_1 \Vdash \Sigma_2$ if $\Sigma_1 \Vdash M$ for every $M \in \Sigma_2$.

Definition 6.3. A *deducibility constraint system* C is a list of deducibility constraints

$$\Sigma_1 \Vdash^?_{(R)} M_1; \cdots ; \Sigma_n \Vdash^?_{(R)} M_n$$

such that:
(1) For $i < j$ if Σ_j^{dv} is obtained from Σ_j by deleting messages which contain a variable not in any message in Σ_i, then for all solutions θ to C^j, $\Sigma_j^{dv}\theta \Vdash \Sigma_i\theta$.

(2) For every variable $x \in V(C)$, there exists $\Sigma_i \Vdash^?_{(R)} M_i$ such that $x \in V(M_i)$, $x \notin V(\Sigma_i)$, and for every $j < i$, $x \notin V(\Sigma_j \Vdash^?_{(R)} M_j)$. The index i in this case is called the *order of* x and will be denoted by $Ord(x)$.

Remark 6.4. A commonly used definition of deducibility constraint systems (in the natural-deduction-based approach) imposes a condition that the lefthand sides of the constraints (the Σ_i's) are ordered by set inclusion (see e.g., [21, 10]). This condition captures the fact that the knowledge of the intruder increases with time as it accumulates more messages. Our definition of a deducibility constraint system is slightly different in this respect. We capture this monotonicity condition via the deduction relation itself. This is somewhat more complicated than the natural deduction counterpart, but it is essentially imposed by our choice of the reduction rules on constraints: a natural choice of the reduction rules is one which mimics closely the inference rules of the proof system, hence we allow decomposition of messages on both the lefthand sides and the righthand sides of constraints, in contrast to the natural-deduction-based approach where decomposition of messages happens only on the righthand sides. Note that in Condition 1 in Definition 6.3, if the lefthand sides of the constraints are totally ordered by set inclusion, then $\Sigma_j^{dv} \supseteq \Sigma_i$, hence trivially, $\Sigma_j^{dv}\theta \Vdash \Sigma_i\theta$. Therefore, our definition of deducibility constraint system subsumes that used in the natural-deduction-based approaches.

Definition 6.5. A deducibility constraint system C is in *solved form* if every element in C is of the form $\Sigma \Vdash^?_R x$ for some Σ and variable x.

For simplicity, we shall assume that in a deducibility constraint system C

$$\Sigma_1 \Vdash^?_{(R)} M_1; \cdots ; \Sigma_n \Vdash^?_{(R)} M_n$$

there is a name, say a, that is in every Σ_i. As a consequence, if C is in solved form, then it is trivially solvable: simply instantiate every variable in $V(C)$ to a. This assumption is harmless as far as reasoning about protocols is concerned, since in this setting, the intruder is usually assumed to have access to infinitely many "environment" names. Some work in the literature, e.g., [7], chooses to make this explicit by adding a special inference rule for deriving environment names.

The goal of this section is to show that every deducibility constraint system can be transformed into a deducibility constraint system in solved form, preserving the set of solutions.

Definition 6.6. The family of relations $\overset{\theta}{\leadsto}$, where θ is a substitution, relate lists of constraints and are defined below. If θ is the identity substitution we write $\leadsto$ instead of $\overset{\theta}{\leadsto}$.

C1: $C_1; \Sigma \Vdash^?_R M; C_2 \overset{\theta}{\leadsto} C_1\theta; C_2\theta$, if M is not a variable and there exists $N \in \Sigma$ such that $\theta = mgu(M, N)$.

C2: $C_1; \Sigma \Vdash^?_R f(M, N); C_2 \leadsto C_1; \Sigma \Vdash^?_R M; \Sigma \Vdash^?_R N; C_2$, where f is either $\langle .,. \rangle$ or $\{.\}.$.

C3: $C_1; \Sigma \Vdash^? M; C_2 \leadsto C_1; \Sigma \Vdash^?_R M; C_2$.

C4: $C_1; (\Sigma, \langle M, N \rangle \Vdash^? U); C_2 \leadsto C_1; (\Sigma, M, N \Vdash^? U); C_2$, where $\langle M, N \rangle \notin \Sigma$.

C5: $C_1; (\Sigma, \{M\}_N \Vdash^? U); C_2 \leadsto C_1; (\Sigma, \{M\}_N \Vdash^?_R N); (\Sigma, M, N \Vdash^? U); C_2$, where $\{M\}_N \notin \Sigma$.

Notice that in **C4** and **C5**, when M and N are already in Σ, then these steps are essentially a weakening step, as they remove a pair or an encrypted message from the lefthand side of a constraint. Notice also that the reduction is defined on lists of constraints,

not just constraint systems. But as we shall see later, the reduction does preserve the property of being a deducibility constraint system. This preservation will be used in proving the completeness of the reduction rules for deducibility constraint systems.

Lemma 6.7 (Soundness)**.** *Let C be a list of constraints and suppose $C \overset{\theta}{\rightsquigarrow} C'$. If C' is solvable then C is also solvable. Moreover, if σ is a solution for C' then $\theta \circ \sigma$ is a solution for C.*

Proof. The reduction rules **C1** to **C3** are obviously sound (**C1** relies on the properties of mgu). For **C4** and **C5**, we need to apply the weakening lemma (Lemma 2.4). □

An immediate consequence of Lemma 6.7 is that, if C rewrites to a solved form, then C is satisfiable, and a solution for C can be computed by composing the substitutions associated with the reduction.

Lemma 6.8. *If $C_1; \Sigma \Vdash^? M; C_2$ is reducible, and $\Sigma \subseteq \Sigma'$ then $C_1; \Sigma' \Vdash^? M; C_2$ is reducible.*

Lemma 6.9. *If C is a deducibility constraint system and $C \overset{\theta}{\rightsquigarrow} C'$ then C' is also a deducibility constraint system.*

Proof. Condition 1 of Definition 6.3 requires that, for constraints $\Sigma_i \Vdash^?_{(R)} X_i$ and $\Sigma_j \Vdash^?_{(R)} X_j$, for all solutions σ of C^j, $\Sigma_j^{dv} \sigma \Vdash \Sigma_i \sigma$, where Σ_j^{dv} is Σ_j, modified by deleting messages containing variables which are not in Σ_i.

We first note that this property is preserved by a substitution which arises in the reduction rule **C1**. Suppose $C \overset{\theta}{\rightsquigarrow} C'$ by rule **C1**, and let σ be a solution for C'. Then, by Lemma 6.7, $\theta \circ \sigma$ is a solution for C, hence also a solution for C^j. So we have $\Sigma_j^{dv}(\theta \circ \sigma) \Vdash \Sigma_i(\theta \circ \sigma)$, and we require $(\Sigma_j \theta)^{dv} \sigma \Vdash (\Sigma_i \theta) \sigma$, where $(\Sigma_j \theta)^{dv}$ is obtained by removing from $\Sigma_j \theta$ messages containing variables which are not in $\Sigma_i \theta$. But if $M\theta$ is such a message, then M must contain variables which are not in Σ_i, and so M has been removed in constructing Σ_j^{dv} from Σ_j. Therefore $\Sigma_j^{dv} \theta \subseteq (\Sigma_j \theta)^{dv}$ and so $\Sigma_j^{dv}(\theta \circ \sigma) \Vdash \Sigma_i(\theta \circ \sigma)$ implies $(\Sigma_j \theta)^{dv} \circ \sigma \Vdash (\Sigma_i \theta) \sigma$.

Reduction rules **C2** and **C3** do not change the left-hand side of a constraint, so the only issue they raise is that **C2** produces two constraints from one — this gives an additional case of constraints $\Sigma_i \Vdash^?_{(R)} X_i$ and $\Sigma_j \Vdash^?_{(R)} X_j$. However here, $\Sigma_i = \Sigma_j$ which satisfies this requirement.

Reduction rule **C4**: Consider the requirement that $\Sigma_j^{dv} \sigma \Vdash \Sigma_i \sigma$. If Σ_i is changed to Σ_i' by an application of rule **C4**, then we have $\Sigma_i \sigma \Vdash \Sigma_i' \sigma$ and so $\Sigma_j^{dv} \sigma \Vdash \Sigma_i' \sigma$. (It is also necessary to observe that Σ_i' contains the same variables as does Σ_i, and so Σ_j^{dv}, defined relative to Σ_i', is the same as Σ_j^{dv}, defined relative to Σ_i). If Σ_j is changed to Σ_j' by an application of rule **C4**, then we have $\Sigma_j' \sigma \Vdash \Sigma_j \sigma$. Further, note that when, say, $\Sigma_j = \Omega, \langle M, N \rangle$, and $\Sigma_j' = \Omega, M, N$, if either M or N is deleted in forming $\Sigma_j'^{dv}$, then $\langle M, N \rangle$ is deleted in forming Σ_j^{dv}. Thus we get $\Sigma_j'^{dv} \sigma \Vdash \Sigma_j^{dv} \sigma$ and so $\Sigma_j'^{dv} \sigma \Vdash \Sigma_i \sigma$.

Reduction rule **C5**: In part, the argument is similar to that for **C4**. If Σ_i is subject to an application of rule **C5**, say $\Sigma_i = \Omega, \{M\}_N$ then the first new constraint resulting is $\Omega, \{M\}_N \Vdash^?_R N$, which has the same left-hand side. The second new constraint resulting is $\Omega, MN \Vdash^?_R X_i$, and we have that if σ is a solution of C' (and so $(\Omega, \{M\}_N)\sigma \Vdash N\sigma$) then we get $(\Omega, \{M\}_N)\sigma \Vdash (\Omega, MN)\sigma$, and so $\Sigma_i^{dv} \sigma \Vdash (\Omega, MN)\sigma$, as required.

If Σ_j is subject to an application of rule **C5**, then the argument is similar to that for rule **C4**.

Finally if we consider the two constraints resulting from rule **C5**, it is easy to check that the condition holds.

Condition 2 of Definition 6.3 is that any variable appears on the right-hand side of a constraint before it appears on the left-hand side of any constraint (equivalently, any variable which in the left-hand side of any constraint appears in an earlier constraint).

We first show that this property is preserved by any substitution. Consider a constraint system $\Sigma_1 \Vdash^?_{(R)} X_1; \cdots ; \Sigma_n \Vdash^?_{(R)} X_n$ and a substitution θ. Let x be in $\Sigma_k \theta$. Then for some y in Σ_k, x is in $y\theta$. Now as y must be in some earlier X_j $(j < k)$, x is in $X_j\theta$, as required. Reduction **C1** consists of a substitution, then deleting a constraint $\Sigma \Vdash^?_R M$ for which $M \in \Sigma$. Clearly deleting such a constraint also preserves condition 2 of Definition 6.3.

It is straightforward to check that condition 2 is preserved by reductions **C2** to **C5**. $\square$

Given a term M, we denote by $|M|$ the size of the term M. Given a set of terms Σ, define $|\Sigma| = \sum_{M \in \Sigma} |M|$.

Definition 6.10. Let Σ be a set of messages. We define a measure on deducibility constraints, denoted by $|\cdot|$ as follows:

$$|\Sigma \Vdash^?_R M| = (0, |M|) \qquad |\Sigma \Vdash^? M| = (1, |\Sigma|)$$

Deducibility constraints are ordered by lexicographical ordering on their measures.

The measure of a deducibility constraint system C, denoted by $|C|$, is

$$|C| = (\#V(C), S)$$

where S is the multiset of measures of the deducibility constraints in C. There is a well-founded ordering on constraints systems, i.e., one which is obtained by lexicographical ordering on $|C|$, where the first component is ordered according to $\leq$ on natural numbers, and the second component is ordered according to multiset ordering (parameterised on the ordering on deducibility constraints).

Lemma 6.11 (Termination of constraints reduction). *For every constraint system C, there is no infinite reduction sequence starting from C.*

Proof. It is enough to show that each instance of the rewrite rules **C1** to **C5** reduces the measure on constraint systems. That is, we show that whenever $C \overset{\theta}{\rightsquigarrow} C'$ then $|C'| < |C|$. For **C1**, by the properties of mgu, the number of variables in C' is smaller than or equal to the number of variables in C, but the number of deducibility constraints in C' is smaller than C, so $|C'| < |C|$. All other cases are straightforward from Definition 6.6 and Definition 6.10. $\square$

In the following, a rewrite sequence such as

$$C_1 \overset{\theta_1}{\rightsquigarrow} C_2 \overset{\theta_2}{\rightsquigarrow} \cdots \overset{\theta_{n-1}}{\rightsquigarrow} C_n$$

shall be abbreviated as $C_1 \overset{\theta}{\Longrightarrow} C_n$ where $\theta = \theta_1 \circ \cdots \circ \theta_{n-1}$. Given two substitutions θ and σ, and a set of variables V, we write

$$\theta =_V \sigma$$

when θ and σ coincide on V.

Lemma 6.12 (Completeness). *Let C be a constraint system and let θ be a solution for C. Then there exists a rewrite sequence $C \overset{\sigma}{\Longrightarrow} C'$ such that C' is in solved form, $\theta =_{V(C)} \sigma \circ \gamma$, and γ is a solution for C'.*

Proof. We prove this by induction on $|C|$. If C is in solved form (this includes the case where C is empty), then let $C' = C$ and let $\gamma = \theta$ and σ be the identity substitution. Otherwise, since θ is a solution for C, for every $\Sigma \Vdash^?_{(R)} M \in C$, we have $\Sigma\theta \Vdash_{(R)} M\theta$. Without loss of generality, we assume that all derivations are in normal form. We construct a rewriting sequence on C by examining the last rule of a selected constraint in C.

By definition, elements of C can be listed as

$$\Sigma_1 \Vdash^?_{(R)} M_1; \cdots ; \Sigma_n \Vdash^?_{(R)} M_n$$

Let i be the maximal index such that C^i is in solved form. We shall select the constraint $\Sigma_i \Vdash^?_{(R)} M_i$ as a candidate for reduction.

We now proceed to showing that it is always possible to apply a rewrite rule to the selected constraint such that $C \overset{\rho}{\leadsto} D$, for some constraint system D, and such that $\theta = \rho \circ \beta$, and β is a solution of D. There are several possible rewritings on the selected constraint, depending on the last rule of the normal derivation of the selected constraint:

(1) Suppose the selected constraint is a right-deducibility constraint, and suppose that there is a normal derivation of $\Sigma_i\theta \vdash M_i\theta$ ending with an *id*. That is, $M_i\theta = N\theta$ for some $N \in \Sigma_i$. Let $\rho = mgu(M_i, N)$. Then rewrite C using **C1**:

$$C = C^i; (\Sigma_i \Vdash^?_R M_i); C_1 \overset{\rho}{\leadsto} C^i\rho; C_1\rho = D$$

Obviously, $\theta = \rho \circ \beta$ for some β, and β is a solution to D.

(2) Suppose the selected constraint is $\Sigma_i \Vdash^?_R f(M, N)$, where f is either $\langle.,.\rangle$ or $\{.\}.$, and the normal derivation of $\Sigma_i\theta \vdash f(M\theta, N\theta)$ ends with a right-introduction rule. The latter means that $\Sigma_i\theta \Vdash_R M\theta$ and $\Sigma_i\theta \Vdash_R N\theta$. Then rewrite C using **C2**:

$$C = C^i; (\Sigma_i \Vdash^?_R f(M, N)); C_1 \leadsto C^i; (\Sigma \Vdash^?_R M); (\Sigma \Vdash^?_R N); C_1 = D.$$

Obviously, θ is also a solution to D, so in this case, $\rho = \epsilon$ and $\beta = \theta$.

(3) Suppose the selected constraint is $\Sigma_i \Vdash^? M_i$ but the normal derivation of $\Sigma_i\theta \vdash M_i\theta$ ends with a right-rule. The latter means that $\Sigma_i\theta \Vdash_R M_i\theta$. Then rewrite C using **C3**:

$$C = C^i; (\Sigma_i \Vdash^? M_i); C_1 \leadsto C^i; (\Sigma_i \Vdash^?_R M_i); C_1 = D.$$

Obviously, θ is also a solution to D, so $\rho = \epsilon$ and $\beta = \theta$.

(4) Suppose the selected constraint is a proper deducibility constraint and suppose there exists $M \in \Sigma_i$, i.e., $\Sigma_i = \Sigma'_i \cup \{M\}$, such that M is not a variable, and there is a normal derivation of $\Sigma'_i\theta, M\theta \vdash M_i\theta$ ending with a left rule applied to $M\theta$. Since M is not a variable, it must be either a pair $\langle N_1, N_2 \rangle$ or an encrypted term $\{N_1\}_{N_2}$.

- If $M = \langle N_1, N_2 \rangle$, then, by normal derivability of $\Sigma'_i\theta, M\theta \vdash M_i\theta$, we have that

$$\Sigma'_i\theta, M\theta, N_1\theta, N_2\theta \Vdash M_i\theta.$$

Note that by Lemma 3.9, we also have

$$\Sigma'_i\theta, N_1\theta, N_2\theta \Vdash M_i\theta.$$

In this case, apply the rewrite rule **C4**:

$$C = C^i; (\Sigma'_i, M \Vdash^? M_i); C_1 \leadsto C^i; (\Sigma'_i, N_1, N_2 \Vdash^? M_i); C_1 = D.$$

Then θ is obviously a solution for D. As in the previous case, let $\rho = \epsilon$ and $\beta = \theta$.

- If $M = \{N_1\}_{N_2}$ then we have

$$\Sigma'_i\theta, M\theta \Vdash_R N_2\theta \quad \text{and} \quad \Sigma'_i\theta, M\theta, N_1\theta, N_2\theta \Vdash M_i\theta.$$

  By Lemma 3.9, we also have

$$\Sigma'_i\theta, N_1\theta, N_2\theta \Vdash M_i\theta.$$

  In this case, apply the rewrite rule **C5**:

$$C = C^i; (\Sigma'_i, M \Vdash^? M_i); C_1 \rightsquigarrow C^i; (\Sigma'_i, M \Vdash^?_R N_2); (\Sigma'_i, N_1, N_2 \Vdash^? M_i) = D.$$

  It is clear that θ is also a solution to D, so let $\rho = \epsilon$ and $\beta = \theta$.

  Note that in both cases, Lemma 3.9 does not need to be applied if $M\theta \in \Sigma'_i\theta$, since in this case we have

$$(\Sigma'_i \cup \{N_1, N_2\})\theta = (\Sigma'_i \cup \{M, N_1, N_2\})\theta.$$

(5) Suppose the selected constraint is

$$\Sigma'_i, x_1, \ldots, x_n \Vdash^? M_i$$

where Σ'_i contains only non-variable terms. Note that since C^i is in solved form, and since C is a deducibility constraint system, it must be the case that each x_k appears in the righthand side of a constraint in C^i.[2] Obviously, any two distinct variables x_k and x_l cannot be the same righthand side, therefore, without loss of generality, we assume that $Ord(x_k) < Ord(x_l)$ whenever $k < l$. Notice that by well-formedness of C, $Ord(x_l) < i$ for every $l \in \{1, \ldots, n\}$.

Suppose that there is a normal derivation Π of the sequent

$$\Sigma'_i\theta, x_1\theta, \ldots, x_n\theta \vdash M_i\theta \tag{6.1}$$

which ends with a left rule applied to one of $x_k\theta$. We first show that the following sequent is derivable

$$\Sigma'_i\theta \vdash M_i\theta. \tag{6.2}$$

To derive the above sequent, we first note the following facts:

(a) Since C^i is in solved form, we have for each $k \in \{1, \ldots, n\}$, $(\Sigma_{o(k)} \Vdash^?_R x_k) \in C^i$, where $o(k)$ is the order of x_k, hence

$$\Sigma_{o(k)}\theta \Vdash_R x_k\theta. \tag{6.3}$$

(b) Let $\Sigma^k_i = \Sigma'_i \cup \{x_1, \ldots, x_{k-1}\}$ for $k \le n$. Since C is a deducibility constraint system, by Definition 6.3(1), there exists $\Omega_k \subseteq \Sigma^k_i$ such that $V(\Omega_k) \subseteq V(\Sigma_{o(k)})$ and

$$\Omega_k\theta \Vdash \Sigma_{o(k)}\theta$$

by definition, hence by weakening (Lemma 2.4), $\Sigma^k_i\theta \Vdash \Sigma_{o(k)}\theta$. Then by several applications of cut (using Sequent (6.3) above), we get

$$\Sigma^k_i\theta \Vdash x_k\theta \tag{6.4}$$

for any $k \le n$.

---

[2]More precisely, since C is a deducibility constraint system, it must be the case that each x_k appears in the righthand side of a constraint in C^i, and since C^i is in solved form, each x_k is the righthand side of a constraint in C^i.

Applying cuts successively using instances of Sequent (6.4) and Sequent (6.1), we obtain Sequent (6.2) as required.

Then consider a normal derivation of Sequent (6.2). The arguments of the previous cases show that the constraint $\Sigma'_i \Vdash^? M_i$ would admit a reduction. It follows trivially (similarly to Lemma 6.8) that the enlarged sequent $\Sigma'_i, x_1, \ldots, x_n \Vdash^? M_i$ would admit a reduction.

Since rewriting reduces the size of the constraint system, by induction hypothesis $D \stackrel{\rho'}{\Longrightarrow} C'$ such that C' is in solved form, $\beta =_{V(D)} \rho' \circ \gamma'$ and γ' is a solution for C'. Now let $\sigma = \rho \circ \rho'$ and let $\gamma = \gamma'$. Then we indeed have $C \stackrel{\sigma}{\Longrightarrow} C'$, $\theta =_{V(C)} \sigma \circ \gamma$ and γ is a solution for C'. $\square$

Theorem 6.13 (Decidability of deducibility constraints). *Given a deducibility constraint system C, it is decidable whether or not the constraint is satisfiable.*

Proof. This is a consequence of Lemma 6.11, Lemma 6.7, Lemma 6.12 and the fact that the rewrite system $\rightsquigarrow$ is finitely branching. $\square$

To conclude this section, we shall comment briefly on the main differences between our approach and that of Comon-Lundh, et. al., [10]. Apart from the difference in the way we impose the monotonicity condition (see Remark 6.4), the main difference is of course in the reduction rules.[3] In their work, no explicit decomposition is applied to the left-hand side of a constraint. Instead, they allow unification of arbitrary subterms in a constraint. Our reduction rules, on the other hand, have a direct correspondence with the inference rules of the proof system itself. This could perhaps be beneficial when dealing with theories for which the subformula property does not hold, e.g., when it involves blind signatures, where exhaustive unification tests on subterms may not be sufficient to get completeness.

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. In particular, this reduction is obtained in a purely proof theoretical way, using standard techniques such as cut elimination and permutation of inference rules. We show that sequent-based techniques can also be used to solve the deducibility constraint problems, for Dolev-Yao intruders.

There are several existing works in the literature that deal with intruder deduction. Our work is more closely related to, e.g., [11, 14, 19], in that we do not have explicit destructors (projection, decryption, unblinding), than, say, [1, 12]. 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 [9, 3, 16], as part of their solution to a more difficult problem of deducibility constraints which assumes active intruders. In particular, Delaune, et. al., [16] obtain results similar to what we have here concerning combination of AC

---

[3]They also consider a slightly richer intruder model, containing asymmetric encryption and signing. But it is easy to extend our work to accomodate these additional operators.

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 do 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 [19]. Another interesting challenge is to see how sequent calculus can be used to study the more difficult problem of solving intruder deduction constraints under richer intruder models, e.g., like those studied in [11, 8, 15]. An immediate avenue for future work is to prove the same results as in Section 6, in particular, the transformation to solved forms, but for the intruder model with blind signatures.

It may be of proof theoretic interest to study the exact complexity of the cut elimination procedure and the translation from natural deduction to sequent calculus, although these results are not needed in establishing the complexity results for the intruder deduction problem. We leave the complete study of the complexity results for these derivation transformations to future work.

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 T. Nipkow. *Term rewriting and all that*. Cambridge University Press, New York, NY, USA, 1998.

[5] 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.

[6] V. Bernat and H. Comon-Lundh. Normal proofs in intruder theories. In *ASIAN 2006*, volume 4435 of *LNCS*, pages 151–166. Springer, 2007.

[7] 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.

[8] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with xor. In *LICS*, pages 261–270, 2003.

[9] 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.

[10] H. Comon-Lundh, V. Cortier, and E. Zalinescu. Deciding security properties for cryptographic protocols: application to key cycles. *ACM Trans. Comput. Log.*, 11(2), 2010.

[11] 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.

[12] 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.

[13] 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.

[14] S. Delaune. Easy intruder deduction problems with homomorphisms. *Inf. Process. Lett.*, 97(6):213–218, 2006.

[15] 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.

[16] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis for monoidal equational theories. *Inf. Comput.*, 206(2-4):312–351, 2008.

[17] 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.

[18] 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.

[19] 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.

[20] J. K. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *ACM Conference on Computer and Communications Security*, pages 166–175, 2001.

[21] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is np-complete. In *CSFW*, pages 174–190. IEEE Computer Society, 2001.

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

[23] A. Tiu. A trace based bisimulation for the spi calculus: An extended abstract. In *APLAS*, volume 4807 of *LNCS*, pages 367–382. Springer, 2007.

[24] A. Tiu and R. Goré. A proof theoretic analysis of intruder theories. In R. Treinen, editor, *RTA*, volume 5595 of *Lecture Notes in Computer Science*, pages 103–117. Springer, 2009.