Reduction of the Intruder Deduction Problem into Equational Elementary Deduction for Electronic Purse Protocols with Blind Signatures*

Daniele Nantes Sobrinho[1]** and Mauricio Ayala-Rincón[1,2]***

Grupo de Teoria da Computação
Departamentos de [1]Matemática e [2]Ciência da Computação
Universidade de Brasília
daniele.nantes@gmail.com, ayala@unb.br

Abstract. The intruder deduction problem for an electronic purse protocol with blind signatures is considered. The algebraic properties of the protocol are modeled by an equational theory implemented as a convergent rewriting system which involves rules for addition, multiplication and exponentiation. The whole deductive power of the intruder is modeled as a sequent calculus that, modulo this rewriting system, deals with blind signatures. It is proved that the associative-commutative (AC) equality of the algebraic theory can be decided in polynomial time, provided a strategy to avoid distributivity law between the AC operators is adopted. Moreover, it is also shown that the intruder deduction problem can be reduced in polynomial time to the elementary deduction problem for this equational theory.

1 Introduction

Cryptographic protocols are programs designed to ensure secure communication over computer networks. A cryptographic protocol involves some cryptographic algorithm, but generally the goal of the protocol is something beyond a simple secrecy. The parties participating of the protocol might want share parts of their secrets to compute a value, jointly generate a random sequence, convince one another of their identity, our simultaneously sign a contract. The objective of using cryptography in a protocol is to prevent or detect eavesdropping and cheating.

By formalizing protocols, one can examine ways in which dishonest parties can subvert them and then develop protocols that are immune to that subversion. These protocols use cryptographic primitives such as public and symmetric encryption, functions that are based on mathematical notions, such as modular

* Work supported by the District Federal Research Foundation - FAP-DF 8-004/2007.
** Author supported by the Brazilian Research Council CNPq.
*** Corresponding author partially supported by the Brazilian Research Council CNPq.

exponentiation and multiplication, and algorithmically hard problems such as the difficulty of calculating discrete logarithms in a finite field.

One of the main challenges in cryptography is to formally verify the security of the cryptographic models taking into account the algebraic properties of the cryptographic primitives. Cryptographic protocols may themselves make use of algebraic properties, which makes it impossible to describe protocols in models that do not handle algebraic properties. A list of algebraic properties used in cryptographic protocols is surveyed in [7]; for instance, the associativity is necessary in Needham-Schoreder-Lowe Modified Protocol, exclusive-or is used in Bull's protocol [5]. Another interesting equational theory, which is the focus of this work is the theory composed by the properties of Abelian groups and modular exponentiation, this is the case of Schnorr's, the Multi-Authority Secret Ballot Election and the Electronic Purse Protocols (EPP) [6, 8].

For studying the EPP, the representation of an execution of the protocol requires the addition of several algebraic properties, which makes its modeling a very complex problem. In order to build the equational theory, one has to consider the Abelian group properties of multiplication and addition and also the properties of modular exponentiation. Unfortunately, a theory having both multiplication and exponentiation properties, together with the distributivity laws, yields undecidability of unification, as was shown by Kapur *et alii* in [9]. In order to obtain decidability of the unification problem, it was necessary to restrict the axioms used in the execution of the protocol. Therefore, to avoid the distributivity axiom, exponentials are not multiplied to each other and an additional homomorphism axiom is included into the equational theory. These changes allows the study of the *intruder deduction problem* for this protocol, which is known to be polynomially decidable [6].

In this work, the EPP is improved allowing blind signatures. Blind signatures are useful to authenticate documents and authorize transactions without knowing their contents as is done, for example, by the election authorities in electronic voting protocols.

In [12] deductive techniques for dealing with a protocol with blind signatures in which mutually disjoint equational theories containing a unique AC operator each are considered. In that paper the intruder capability of deduction is modeled inside a sequent calculus modulo a rewriting system that models the algebraic deductive power following the approach in [3]. The intruder deduction problem can be reduced in polynomial time to the elementary deduction problem (EDP). The restriction on the AC operators to belong to mutually disjoint theories is essential to guarantee polynomiality.

In this work the techniques in [12] are combined with the ones in [6] in order to model an EPP with blind signatures and it is proved, adapting the techniques in these works, that the intruder deduction problem can be also polynomially reduced to the EDP. Instead combining several disjoint equational theories as in [12], the algebraic power is modeled by a unique equational theory, which has more than one AC operator. This is achieved presenting a polynomial algorithm that decides AC equality of the operators used to model the protocol.

Detailed proofs are included in an extended version of this paper available at `http://ayala.mat.unb.br/publications.html`.

Section 2 presents the necessary notions about the considered protocol as well as how it is modeled: firstly, the protocol is described in detail; afterwards, the equational theory and the associated convergent rewriting system are presented; finally, the cut-free sequent calculus that models the intruder deduction is introduced. Before concluding, Section 3 introduces the notion of *normal derivations* that is useful to present a *linear* inference system for the intruder. This system is necessary to prove polynomial reduction to the EDP.

2 Modeling Intruder Deduction for the Electronic Purse Protocol with Blind Signatures

It is assumed basic knowledge on cryptography and rewriting (e.g, [2, 4, 11]). In the following, an important security problem in presence of a passive eavesdropper will be considered, the so-called *intruder deduction problem*: given a finite set of messages Γ and a message M, is it possible for the intruder to retrieve M from Γ by using his deduction capabilities?

2.1 Syntax

The signature adopted consists of a set of function symbols, composed by the union of the set

$$\Sigma_C = \{\mathsf{pub}(\_), \mathsf{sign}(\_\,,\_), \mathsf{blind}(\_\,,\_), \{\_\}_\_, <\_\,,\_>\}$$

representing the *constructors*, whose interpretations are:

- $\mathsf{pub}(M)$ gives the public key generated from a private key M;
- $\mathsf{blind}(M, N)$ gives M encrypted with N using blinding encryption;
- $\mathsf{sign}(M, N)$ gives M signed with a private key N;
- $\{M\}_N$ gives M encrypted with the key N using Dolev-Yao symmetric encryption and;
- $\langle M, N\rangle$ constructs a pair of terms from M and N.

In addition, the signature includes the set of symbols Σ_{EP} associated with the equational theory EP. It is also required that $\Sigma_{\mathsf{EP}} \cap \Sigma_C = \emptyset$.

The equational theory EP contains three different AC symbols, which will be denoted by $\{+, \bullet, \star\}$, obeying the standard Abelian group laws and also some axioms for exponentiation. The signature of EP contains three constant symbols for the neutral elements, $e_\circ$, three for the inverse functions, $J_\circ(\_)$, associated with each of the AC symbols: $\circ \in \{+, \bullet, \star\}$. In addition, EP contains two symbols for exponentiation $h(\_)$ and $\mathsf{exp}(\_\,,\_)$ whose rules will be presented in the Subsection 2.2. Messages are built over countably infinite sets of names N and variables V. As notational convention names will range over the first and variables over the last letters of the Roman alphabet.

Then the grammar of the set of *terms* or messages is given as

$$\begin{aligned} M, N \;:=\; & a \mid x \mid \mathsf{pub}(M) \mid \mathsf{sign}(M,N) \mid \mathsf{blind}(M,N) \mid \{M\}_N \mid \langle M, N\rangle \mid \\ & M + N \mid M \bullet N \mid M \star N \mid e_+ \mid e_\bullet \mid e_\star \mid J_+(M) \mid J_\bullet(M) \mid J_\star(M) \mid \\ & \mathsf{exp}(M,N) \mid h(M) \end{aligned}$$

As in [12], some definitions related to terms are necessary, for instance, a term M is said to be an EP-*alien term* if M is headed by a symbol $f \notin \Sigma_{\mathsf{EP}}$.M is *guarded* if it is either a name, a variable, or a term headed by a constructor. It is a *pure* EP-*term* if it contains only symbols from Σ_{EP}, names and variables.

A *context* is a term with holes. $C^k[\,]$ denotes a context with k-hole(s). An EP-*context* is a context formed using only function symbols in Σ_{EP}.

2.2 The Electronic Purse Protocol: the equational theory EP

This protocol, as presented in [6], allows the transaction between an electronic purse and a server. It aims to guarantee a good level of security, using asymmetric cryptography and with a small cost. It involves three agents: the electronic purse EP, a server S and a trusted autority A, which is involved in case of claims of either party only and consequently is not considered here.

Let b and r denote two public positive integers. The public key of EP is $b^s \bmod r$, where s is its private key. Initially, there is a phase during which the server authenticates itself, that is not considered here, since it does not make use of algebraic properties. After this phase, the electronic purse EP authenticates itself with the server S and performs the transaction:

Step 1. EP computes the message $M = \{S, N_S, N_{EP}, M_t\}_{K_A(P)}$ (which is used in case of conflict only);

Step 2. EP sends to the server S: $\mathsf{hash}(b^N \bmod r, S, N_s, M, M_t)$, where M_t is the amount payed;

Step 3. The server S challenges EP sending a $\mathsf{nonce}\ N_c$;

Step 4. EP sends back $N - s \times N_c, M, M_t$ and subtract M_t from his account;

Step 5. S checks that the the message received at the second step is consistent with the message received at the fourth step and then increases its account in the amount M_t. S also stores the messages M, N_S, N_{EP} and M_t.

The most important and difficult step is **Step 5**, since S should be able to verifify consistence of the previous steps. For doing it, S shold perform the following operations:

$$\begin{aligned} \mathsf{hash}((b^s)^{N_c} \times b^{N - s\times N_c} \mathsf{mod} r, S, N_S, N_{EP}, M, M_t) = \\ \mathsf{hash}(b^{s\times N_c} \times b^{N - s\times N_c} \mathsf{mod} r, S, N_S, N_{EP}, M, M_t) = \\ \mathsf{hash}(b^{s\times N_c + N - s\times N_c} \bmod r, S, N_S, N_{EP}, M, M_t) = \\ \mathsf{hash}(b^N \bmod r, S, N_S, N_{EP}, M, M_t) \end{aligned}$$

In addition to Abelian group properties for both $\times$ and $+$, the following equational properties are used:

$$\mathsf{exp}(\mathsf{exp}(b,y),z) = \mathsf{exp}(b, y \times z) \text{ and } \mathsf{exp}(b,x) \times \mathsf{exp}(b,y) = \mathsf{exp}(b, y+z)$$

This introduces a problem because the properties

$$\begin{aligned} &(1)\ \ \mathsf{exp}(\mathsf{exp}(x,y),z) = \mathsf{exp}(x, y \times z) \\ &(2)\ \ \mathsf{exp}(x,y) \times \mathsf{exp}(x,z) = \mathsf{exp}(x, y+z) \end{aligned}$$

derive distributivity of exponentiation over the multiplication operator. In fact:

$$\begin{aligned} \mathsf{exp}(\mathsf{exp}(x,y_1) \times \mathsf{exp}(x,y_2),z) &=_2 \mathsf{exp}(\mathsf{exp}(x, y_1+y_2),z) \\ &=_1 \mathsf{exp}(x,(y_1+y_2) \times z) \\ &= \mathsf{exp}(x, y_1 \times z + y_2 \times z) \\ &=_2 \mathsf{exp}(x, y_1 \times z) \times \mathsf{exp}(x, y_2 \times z) \\ &=_1 \mathsf{exp}(\mathsf{exp}(x,y_1),z) \times \mathsf{exp}(\mathsf{exp}(x,y_2),z) \end{aligned}$$

Consequently, the unification and hence security becomes undecidable (*e.g.* [9]). Since exponential needs to be applied to constant bases only, to solve this problem an additional unary function symbol h is adopted, whose meaning is $h(x) = \mathsf{exp}(b,x)$. This adaptation will provide an equational theory EP with decidable unification problem [6].

Actually, the distributivity rule does not need to be considered. The following restriction to a homomorphism axiom is sufficient: $h(x) \bullet h(y) = h(x+y)$.

Thus, the equational theory EP used to model the protocol is composed by the following equational axioms:

$$\begin{aligned} \mathsf{AG}(+, J_+, e_+) \qquad & h(x) \bullet h(y) = h(x+y) \\ \mathsf{AG}(\star, J_\star, e_\star) \qquad & \mathsf{exp}(h(x),y) = h(x \star y) \\ \mathsf{AG}(\bullet, J_\bullet, e_\bullet) \qquad & \mathsf{exp}(\mathsf{exp}(x,y),z) = \mathsf{exp}(x, y \star z) \end{aligned}$$

where $\mathsf{AG}(\circ, J_\circ, e_\circ)$ are the axioms of Abelian groups for $\circ \in \{\bullet, +, \star\}$.

These equational axioms are sufficient for modeling the protocol. The following equalities express the main test executed by the server (during **Step 5**):

$$\begin{aligned} \mathsf{exp}(h(s), N_c) \bullet h(N + J_+(s \star N_c)) &= h(s \star N_c) \bullet h(N + J_+(s \star N_c)) \\ &= h(s \star N_c + N + J_+(s \star N_c)) \\ &= h(N) \end{aligned}$$

The role of the two multiplication used is to differentiate between the multiplication in the basis of exponentials and the multiplication of exponents.

2.3 The convergent rewriting system $\mathcal{R}$ equivalent to the equational theory EP

Standard rewriting notation and notions are used (e.g. [2,4]). A rewriting system is a set $\mathcal{R}$ of oriented equations over terms in a given signature. For terms s and t, $s \to_{\mathcal{R}} t$ denotes that s rewrites into t using one application of a rewriting rule in $\mathcal{R}$. The inverse of $\to_{\mathcal{R}}$ is denoted by ${}_{\mathcal{R}}\leftarrow$. The transitive, reflexive-transitive and equivalence closures of $\to_{\mathcal{R}}$ are denoted by $\overset{+}{\to}_{\mathcal{R}}$, $\overset{*}{\to}_{\mathcal{R}}$ and $\overset{*}{\leftrightarrow}_{\mathcal{R}}$, respectively. Analogously, the transitive and reflexive-transitive closures of ${}_{\mathcal{R}}\leftarrow$ are denoted by ${}_{\mathcal{R}}\overset{+}{\leftarrow}$ and ${}_{\mathcal{R}}\overset{*}{\leftarrow}$, respectively. The equivalence clousure of the rewriting relation, $\overset{*}{\leftrightarrow}_{\mathcal{R}}$, is also denoted by $\approx_{\mathcal{R}}$. Composition of relations is denoted by $\circ$.

A term s is in $\mathcal{R}$-normal form if there is no term t such that $s \to_{\mathcal{R}} t$; $s \downarrow_{\mathcal{R}}$ denotes a normal form of s (i.e., a term t such that $s \to_{\mathcal{R}} t$ and t is in $\mathcal{R}$-normal form).

$\mathcal{R}$ is said to be convergent whenever it is terminant and confluent, *i.e.*, respectively:

$$\text{there is no infinite chain } s_0 \to_{\mathcal{R}} s_1 \to_{\mathcal{R}} s_2 \cdots \text{ and}$$

$$({}_{\mathcal{R}}\leftarrow \circ \to_{\mathcal{R}}) \subseteq (\overset{*}{\to}_{\mathcal{R}} \circ {}_{\mathcal{R}}\overset{*}{\leftarrow})$$

Given an equational theory E, it is said that E is equivalent to $\mathcal{R}$ whenever $\approx_{\mathcal{R}} = \approx_E$. Subscripts are omitted when they are clear from the context.

The rewriting system $\mathcal{R}$ associated with the equational theory EP, introduced in [6], has as signature

$$\Sigma_{\mathsf{EP}} = \{+,\ e_+,\ J_+,\ \star,\ e_\star,\ J_\star, \bullet,\ e_\bullet, J_\bullet, h, \mathsf{exp}\}$$

and consists of the union of the rewriting systems below.

$\mathcal{R}_{\mathsf{AG}(\circ)}$, for $\circ \in \{+, \star, \bullet\}$, denotes the rewriting system modulo AC for $\circ$, given by the set of rules:

$$\mathcal{R}_{AG(\circ)} := \begin{cases} x \circ e_\circ \to x & x \circ J_\circ(x) \to e_\circ \\ J_\circ(x) \circ J_\circ(y) \to J_\circ(x \circ y) & J_\circ(e_\circ) \to e_\circ \\ J_\circ(J_\circ(x)) \to x & J_\circ(x) \circ x \circ y \to y \\ J_\circ(x) \circ J_\circ(y) \circ z \to J_\circ(x \circ y) \circ z & J_\circ(x \circ y) \circ x \to J_\circ(y) \\ J_\circ(x \circ y) \circ x \circ z \to J_\circ(y) \circ z & J_\circ(J_\circ(x) \circ y) \to x \circ J_\circ(y) \end{cases}$$

$\mathcal{R}_0$ is given by the rules.

$$\mathcal{R}_0 := \begin{cases} \mathsf{exp}(h(x), y) \to h(x \star y) & J_\bullet(h(x)) \to h(J_+(x)) \\ \mathsf{exp}(\mathsf{exp}(x, y), z) \to \mathsf{exp}(x, y \star z) & h(e_+) \to e_\bullet \\ h(x) \bullet h(y) \to h(x + y) & J_\bullet(h(x) \bullet y) \to h(J_+(x)) \bullet J_\bullet(y) \\ h(x) \bullet h(y) \bullet z \to h(x + y) \bullet z & \mathsf{exp}(e_\bullet, x) \to h(e_+ \star x) \end{cases}$$

The rewriting system $\mathcal{R} := \mathcal{R}_{\mathsf{AG}(\star)} \cup \mathcal{R}_{\mathsf{AG}(\bullet)} \cup \mathcal{R}_{\mathsf{AG}(+)} \cup \mathcal{R}_0$ was proved convergent modulo AC in [6]. This implies that any equational theorem in EP, namely, $s =_{\mathsf{EP}} t$, can be effectively proved using $\mathcal{R}$, by normalizing s: $s \to^*_{\mathcal{R}} s\!\downarrow$, and t: $t \to^*_{\mathcal{R}} t\!\downarrow$, and checking whether $s\!\downarrow =_{AC} t\!\downarrow$.

2.4 Sequent calculus for the intruder

The set of inference rules $\mathcal{S}$ for the intruder deduction, presented in Table 1 is essentially the same as in [12], except that the (id) rule considers the equational theory EP and the symbol $=_{AC}$ will be interpreted as equality modulo AC for the operators $\{+, \star, \bullet\}$.

Table 1. System $\mathcal{S}$: Sequent Calculus for the Intruder

$$\frac{M \approx_{\mathsf{EP}} C[M_1,\ldots,M_k] \quad \text{C[ ] an EP-context, and } M_1,\ldots,M_k \in \Gamma}{\Gamma \vdash M}\ (id) \qquad \frac{\Gamma \vdash M \qquad \Gamma, M \vdash T}{\Gamma \vdash T}\ (cut)$$

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

$$\frac{\Gamma, \{M\}_k \vdash K \qquad \Gamma, \{M\}_k, M, K \vdash N}{\Gamma, \{M\}_k \vdash N}\ (e_L) \qquad \frac{\Gamma \vdash M \qquad \Gamma \vdash K}{\Gamma \vdash \{M\}_k}\ (e_R)$$

$$\frac{\Gamma, \mathsf{sign}(M,K),\ \mathsf{pub}(L), M \vdash N}{\Gamma, \mathsf{sign}(M,K),\ \mathsf{pub}(L) \vdash N}\ (\mathsf{sign}_L) K =_{AC} L$$

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

$$\frac{\Gamma, \mathsf{blind}(M,K) \vdash K \qquad \Gamma, \mathsf{blind}(M,K), M, K \vdash N}{\Gamma, \mathsf{blind}(M,K) \vdash N}\ (\mathsf{blind}_{L_1})$$

$$\frac{\Gamma, \mathsf{sign}(\mathsf{blind}(M,R),K) \vdash R \qquad \Gamma, \mathsf{sign}(\mathsf{blind}(M,R),K), \mathsf{sign}(M,K), R \vdash N}{\Gamma, \mathsf{blind}(M,K) \vdash N}\ (\mathsf{blind}_{L_2})$$

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

As in [12], the rule (gs), called *analytic cut*, is necessary to introduce the function symbols in Σ_{EP}. This rule is necessary to "abstract" EP-alien subterms in a sequent in order to prove cut rule *admissibility*.

A sequent $\Gamma \vdash M$ is in *normal form* if M and all the terms in Γ are in normal form. Unless stated otherwise, it is assumed that sequents are in normal form. Moreover, $\Gamma \Vdash_{\mathcal{S}} M$ denotes that the sequent $\Gamma \vdash M$ is derivable in $\mathcal{S}$.

Definition 1 (Admissible rules). *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.*

Admissibility of the cut rule holds. The proof is based on induction on the height of the left premise derivation immediately above the cut rule as in [12].

Theorem 1 (Admissibility of the cut rule). *The cut rule is admissible for $\mathcal{S}$.*

Proof (Sketch). The cut reduction is driven by the left premise derivation of the cut. The proof is divided in several cases, based on the last rule of the left premise derivation.

For instance, suppose the left premise of the cut ends with the (id)-rule :

$$\dfrac{\dfrac{}{\Gamma \vdash M}\,(id) \qquad \dfrac{\Pi_1}{\Gamma, M \vdash R}}{\Gamma \vdash R}\,(cut)$$

where $M = C[M_1, \ldots, M_k]\downarrow$, $C[\ldots]$ is an EP-context and $M_1, \ldots, M_k \in \Gamma$. By induction hypothesis $\Gamma, M \vdash R$ is cut-free derivable, hence applying a lemma of preservation of $\mathcal{S}$-derivability on the decomposition of EP-contexts to Π_1 one can obtain a cut-free derivation Π' of $\Gamma \vdash R$. □

3 Elementary Intruder Deduction Under the EP Theory

The decidability of the intruder deduction problem for the EPP without blind signatures is already known to be polynomial [6]. This result was obtained following McAllester's approach which states that there is a polynomial algorithm provided a *locality* property for the inference rules is guaranteed [10]. Here, the techniques in [12] are followed to prove that the decidability result for the EPP with blind signatures can be reduced to the EDP.

For doing this, it is necessary an improvement on the boundary created to guarantee the locality property for the intruder's rules for the EPP in [6], in which all intermediate formulas contained in every derivation were bounded by a notion of subterms involving only terms in the signature Σ_{EP}. Here, since one deals with the system $\mathcal{S}$ and terms headed by constructors are allowed inside the (id) rule, a new bound will be necessary to preserve the subformula property. This bound is built as a combination of the previous notion of subterms and the saturated set of Γ (intruder's knowledge).

Definition 2 (Elementary deduction problem). *The* elementary deduction problem *for EP, written $\Gamma \Vdash_{\mathsf{EP}} M$, is the problem of deciding whether the* (id) *rule is applicable to the sequent $\Gamma \vdash M$, by checking whether there exists an EP-context $C[\ldots]$ and terms $M_1, \ldots, M_k \in \Gamma$ such that $C[M_1, \ldots, M_k] \approx_{\mathsf{EP}} M$.*

For $\circ \in \{\star, \bullet, +\}$ define $\mathsf{inv}_\circ(u)$ as the term $J_\circ(u)\downarrow$. The following definitions are essential for the next results.

Definition 3. *Denote by top(t) the root symbol of the term t.* $\mathrm{TOP}(u)$ *is defined recursively as*

$$\mathrm{TOP}(t) := \begin{cases} \circ, & \text{if } t = J_\circ(u \circ v), \text{ for } \circ \in \{\star, \bullet, +\} \\ \bullet, & \text{if } t = h(v + w) \\ \bullet, & \text{if } t = h(J_+(v + w)) \\ top(t), & \text{otherwise.} \end{cases}$$

Definition 4 (EP-decomposition subterms). *Let* $\circ \in \{\star, \bullet, +\}$*, the set of EP-decomposition subterms, denoted by* $\mathrm{DS}_\circ(u)$*, is defined as*

1. $\mathrm{DS}_\circ(u \circ v) = \mathrm{DS}_\circ(u) \cup \mathrm{DS}_\circ(v)$,
2. $\mathrm{DS}_\circ(J_\circ(u)) = \{J_\circ(v) | v \in \mathrm{DS}_\circ(u)\}$,
3. $DS_\bullet(h(u)) = \{h(v) | v \in DS_+(u)\}$, *and*
4. $\mathrm{DS}_\circ(u) = \{u\}$ if $\mathrm{TOP}(u) \neq \circ$.

Definition 5 (EP-subterms). *Let t be a term in EP-normal form,* $Sub(t)$ *is the smallest set of terms such that* $t \in Sub(t)$ *and if* $u \in Sub(t)$ *then*

1. *either* $\circ = \mathrm{TOP}(u) \in \{\star, \bullet, +\}$ *and* $\mathrm{DS}_\circ(u) \subseteq Sub(t)$
2. *or else* $u = f(u_1, \ldots u_n)$ *and* $u_1, \ldots, u_n \in Sub(t)$.

If T is a set of terms, $Sub(T)$ *is defined as:* $Sub(T) := \bigcup_{u \in T} Sub(u)$.

Although the modifications made in the (id) rule, it is possible to see that this rule still preserves the *subformula property*: in any sequent $\Gamma \vdash M$ derivable using the new (id) rule only subformulas of Γ and M occur. In order to obtain this property it is necessary a suitable notion of subterms F, which is a function that associates a term to the set of its subterms.

The function above is basically the same introduced by Bursuc *et alii* in [6] except by a slight alteration in the subset $\{\mathsf{inv}_\circ(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) \in \{\star, +, \bullet\}\}$ used in the composition of F.

$$\begin{aligned} F(T) = \mathrm{Sub}(T) & \\ & \cup \{h(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) = +\} \\ & \cup \{h(\mathsf{inv}_+(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) = +\} \\ & \cup \{\mathsf{inv}_\circ(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) \in \{\star, +, \bullet\}\} \\ & \cup \{h(t) \,|\, \exists\, t \in \mathrm{Sub}(T) \text{ s.t. } \mathrm{TOP}(u) = \circ \in \{\star, +\}, t \in \mathrm{DS}_\circ(u)\} \\ & \cup \{\mathsf{inv}_\circ(t) \,|\, \exists\, u \in \mathrm{Sub}(T) \text{ s.t. } \mathrm{TOP}(u) = \circ \in \{\star, +, \bullet\}, \quad t \in \mathrm{DS}_\circ(u)\} \\ & \cup \{h(\mathsf{inv}_\circ(t)) \,|\, \exists\, u \in \mathrm{Sub}(T) \text{ s.t. } \mathrm{TOP}(u) = \circ \in \{\star, +\}, \quad t \in \mathrm{DS}_\circ(u)\} \end{aligned}$$

Notice that the size of $F(T)$ is linear in the size of T.

Nevertheless the cut-free system $\mathcal{S}$ does not enjoy the *subformula property*, since in (blind_{L_2}) the premisse has a term which is not a subterm of any term in the conclusion. Notice that reading the rules bottom up, the terms introduced are smaller than the terms in the conclusion. Thus a proof search strategy will eventually terminate.

Normal derivations in a deduction system satisfy the following conditions: left rules appear neither above a right rule nor immediately above the left-premise of a branching left rule.

$\Gamma \Vdash_{\mathcal{R}} M$ denotes the fact that the sequent $\Gamma \vdash M$ is provable using only right rules and (id). The system $\mathcal{L}$ given in Table 2 is a linear deduction system for the intruder. The difference with the system in [12] is essentially the new interpretation of the (id) rule and the equality modulo AC used in the rule (sign).

Table 2. System $\mathcal{L}$: a linear proof system for intruder deduction

$$\frac{\Gamma \Vdash_{\mathcal{R}} M}{\Gamma \vdash M}\ (\mathrm{r}) \qquad \frac{\Gamma, \{M\}_K, M, K \vdash N}{\Gamma, \{M\}_K \vdash N}\ (l_e),\ \text{where } \Gamma, \{M\}_K \Vdash_{\mathcal{R}} K$$

$$\frac{\Gamma, \langle M, N\rangle, M, N \vdash T}{\Gamma, \langle M, N\rangle \vdash T}\ (l_p) \qquad \frac{\Gamma, \mathsf{sign}(M, K),\ \mathsf{pub}(L), M \vdash N}{\Gamma, \mathsf{sign}(M, K),\ \mathsf{pub}(L) \vdash N}\ (\mathsf{sign}),\ K =_{AC} L$$

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

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

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

Standard DAG representation of Γ with maximum sharing of subterms is assumed (see, e.g. [1]). As in [12], $st(\Gamma)$ denotes the set of subterms of the terms in Γ. A term M is a *proper subterm* of N if M is a subterm of N and $M \neq N$. Denote with $pst(\Gamma)$ the set of proper subterms of Γ, and define

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

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

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

As in [12], the next complexity results are stated with relation to the size of $St(\Gamma \cup \{M\})$ combined with the notion of EP-subterms.

Definition 6 (Polynomial reducibility to elementary deduction). *Let $\Gamma \Vdash_{\mathcal{L}} M$ be a deduction problem and let n be the size of $St(\Gamma \cup \{M\})$. Suppose that the EDP in EP has complexity $\mathcal{O}(f(m))$, where m is the size of the input. The problem $\Gamma \Vdash_{\mathcal{L}} M$ is said to be* polynomially reducible *to the EDP $\Vdash_{\mathsf{EP}}$ if it has complexity $\mathcal{O}(n^k \times f(n))$ for some constant k.*

In order to adapt the proof of the following lemma from [12] it is only necessary to interpret the (id) rule inside the equational theory EP.

Lemma 1 ($\Vdash_{\mathcal{R}}$ reducible polynomially to $\Vdash_{\mathsf{EP}}$). *The decidability of the relation $\Vdash_{\mathcal{R}}$ is polynomially reducible to the decidability of elementary deduction $\Vdash_{EP}$.*

Proof. It is enough to assume a simple proof search procedure for $\Gamma \vdash M$ using only right-rules:

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

Notice that the number of iterations is bound by the number n of distinct subterms of M and that elementary deducibility is checked on problems of size less or equal to n. □

In order to prove the main result, one has to consider the notion of a *principal term* in a left-rule in the proof system $\mathcal{L}$ which was defined in [12]. Given a sequent $\Gamma \vdash M$ and a pair of principal-term and left-rule (N, ρ), the pair (N, ρ) is *applicable* to the sequent if

- ρ is (ls), N is a guarded subterm 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.

Assume that the complexity of $\Vdash_E$ is $\mathcal{O}(f(n))$ and let n be the size of $St(\Gamma \cup \{M\})$. Given a sequent $\Gamma \vdash M$ and a pair (N, ρ), observe the following facts:

F1. the complexity of checking whether (N, ρ) is applicable to $\Gamma \vdash M$ is equal to $\mathcal{O}(n^l f(n))$ 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:

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

For **F1** it is necessary to assume DAG representation of sequents with maximal sharing of subterms. The complexity of checking if a rule is applicable or not then consists of: pointer comparisons; pattern match a subgraph with a rule; checking equality modulo AC (for the rule sign); checking $\Vdash_{\mathcal{R}}$. Pointer comparisons and pattern matching can be done in polynomial time and checking $\Vdash_{\mathcal{R}}$ is polynomially reducible to $\Vdash_{\mathsf{EP}}$ (Lemma 1). The following result shows the polynomiality of the third operation.

Lemma 2 ($=_{AC}$ is polynomially decidable). *Let M, N terms in normal form. The problem whether $M =_{AC} N$ is decidable in polynomial time.*

Proof. By induction on the structure of M. Suppose that $M = f(M_1, \ldots, M_n)$.

1. If $f \notin \{+, \star, \bullet\}$ it is enough to apply induction hypothesis to the subterms $M_1, \ldots, M_n$ of M.
2. Suppose $f \in \{+, \star\}$. To make the computation easier, write: $M = M_1 \circ M_2 \circ \ldots \circ M_n$. Since M is in normal form and according to the rewrite rules,

   $$M = M'_1 \circ M'_2 \circ \ldots \circ M'_k \circ J_\circ(M"_1 \circ M"_2 \circ \ldots \circ M"_s)$$

   It is possible to count the occurrences of each subterm in M. Hence,

   $$M = \alpha_1 M'_1 \circ \alpha_2 M'_2 \circ \ldots \alpha_p \circ M'_p \circ J_\circ(\beta_1 M''_1 \circ \beta_2 M''_2 \circ \ldots \circ \beta_q M''_q)$$

   where $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$ are integers (at least one of them non null) and $p \leq k, q \leq s$. Hence, $M =_{AC} N$ iff $|M|_{M'_i} = |N|_{M'_i}$ and $|M|_{M''_j} = |N|_{M''_j}$, $1 \leq i \leq p$ and $1 \leq j \leq q$. And a simple enumeration gives a polynomial algorithm.
   The problematic case happens when

   $$N = \gamma_1 N'_1 \circ \gamma_2 N'_2 \circ \ldots \circ \gamma_p N'_p \circ J_\circ(\varphi_1 N''_1 \circ \varphi_2 N''_2 \circ \ldots \circ \varphi_q N''_q),$$

   and for each $1 \leq i \leq p$ (resp. $1 \leq j \leq q$) there exists a $1 \leq l \leq p$ (resp. $1 \leq r \leq q$) such that $M'_i =_{AC} N'_l$ (resp. $M''_j =_{AC} N''_r$). Applying the induction hypothesis, the result follows.
3. Suppose $f = \bullet$. Then, $M = M_1 \bullet \ldots \bullet M_p \bullet J_\bullet(M'_1 \bullet \ldots \bullet M'_q) \bullet h(M''_1 + \ldots + M''_r)$. Reordering the subterms which appear repeteadly,

   $$M = \chi_1 M_1 \bullet \ldots \bullet \chi_u M_p \bullet J_\bullet(\mu_1 M'_1 \bullet \ldots \bullet \mu_q M'_q) \bullet h(\rho_1 M''_1 + \ldots + \rho_w M''_w).$$

   Analogously to the previous case, a simple enumeration gives a polynomial algorithm.

This completes the proof. □

The polynomial reducibility of $\Vdash_{\mathcal{L}}$ to $\Vdash_{\mathsf{EP}}$ can be proved by a deterministic proof search strategy which systematically tries all applicable rules following the same proof methodology as in [12].

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

Proof (Sketch). Three auxiliary results are used:

- Weakening: if Π is an $\mathcal{L}$-derivation of $\Gamma \vdash M$ and $\Gamma \subseteq \Gamma'$, then there exists an $\mathcal{L}$-derivation Π' of $\Gamma' \vdash M$ such that $|\Pi'| = |\Pi|$.
- Let Π be an $\mathcal{L}$-derivation of $\Gamma \vdash M$. Then for every sequent $\Gamma' \vdash M'$ occurring in Π, $\Gamma' \cup \{M'\} \subseteq St(\Gamma \cup \{M\})$.
- 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 quadratic with respect to the size of $\Gamma \cup \{M\}$.

Suppose $\Gamma \vdash M$ is provable in $\mathcal{L}$. Let $M_1, \ldots, M_n$ be an enumeration of the set $St(\Gamma \cup \{M\})$. There is a shortest proof of $\Gamma \vdash M$ where each sequent appears exactly once in each branch of the proof. 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 is applicable, successively, to $\Gamma \vdash M$. Since no repetitions of sequents are possible, $q \leq n$. Also, it should be noticed that the rules of $\mathcal{L}$ are inversible: one does not lose provability at any point of the proof search. Suppose, both principal-term and rule pairs (N, ρ) and (N', ρ') are applicable to $\Gamma \vdash M$; then if $\Gamma' \vdash M$ is the unique premise determined by either (N, ρ) or (N', ρ'), then, respectively, either (N', ρ') or (N, ρ) applies to $\Gamma' \vdash M$.

A proof search strategy for $\Gamma \vdash M$ is based on repeatedly try all possible applicable pairs (M', ρ') for each possible $M' \in St(\Gamma \cup \{M\})$ and each left-rule ρ' (that is bounded by $6\,n$) and for all generated sequents taking in care elimination of redundancies based on the previous observations and weakening. For all generated sequent $\Delta \vdash M$, before trying possible applicable pairs, one should check whether $\Delta \Vdash_{\mathcal{R}} M$. By Lemma 1, checking $\Vdash_{\mathcal{R}}$ takes $\mathcal{O}(n^a f(n))$ for some constant a. By (**F1**), checking applicability takes $\mathcal{O}(n^l f(n))$ for some constant l. Therefore the whole procedure takes $\mathcal{O}(n^{c+l} f(n))$. □

4 Conclusion

It was shown that the decidability of the intruder deduction problem of an electronic purse protocol with the theory of blind signatures can be polynomially reduced to the elementary intruder deduction problem. For doing this, the techniques used by Bursuc *et alii* in [6] to model the algebraic power of the protocol via a convergent rewriting system were applied together with the techniques introduced by Tiu and Goré in [12] in order to represent the intruder's deduction capacity via a sequent calculus taking into account blind signatures. In the latter work, the equational part is composed by a disjoint combination of equational

theories, each one containing at most one AC operator. In this sense, the present paper slightly extends these results since the equational theory considered, which is essential for the execution of the protocol, is composed by three different AC operators and the equational theory cannot be split into disjoint theories. Although the proof techniques were proved to be straightforwardly adaptable, this study is of practical interest since the analysis was extended to EPP in which authority parties can blindly authorize electronic transactions.

As future work, one can consider more complex algebraic equational theories in security analysis of cryptographic protocols (e.g. [7]), using the approach of proof search in sequent calculus and, even more, try to establish similar results for deduction problems in which the constructors interact with the equational theories. Another interesting challenge is to obtain deducibility results with respect to active attacks.

A Proof of Theorem 1

Before presenting the proof, a sequence of preliminar results similar to the ones introduced in [12] are necessary.

Definition 7 (Quasi-EP term). *A term M is a* quasi-*EP* term *if every EP-alien subterm of M is in EP-normal form.*

Given the equational theory EP, the function v_{EP} is a variant of v_E defined in the original paper, which assigns a variable V to each ground term such that $v_{EP}(M) = v_{EP}(N)$ if and only if $M \approx_{EP} N$.

Definition 8 (EP abstraction function). *The EP* abstraction function F_{EP} *is a function mapping ground terms to pure EP terms, defined recursively as follows:*

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

Note that, the new abstraction function F_{EP} still preserves the equivalence relation $=_{AC}$. That is, if $M =_{AC} N$ then $F_{EP}(M) =_{AC} F_{EP}(N)$.

For obtaining the following results, original proofs in [12] require some slight changes on the interpretation of the proofs, mainly in the cases where either AC function symbols are considered or the rule (id) is considered.

Proposition 1 (Preservation of R_{EP}-reducibility between quasi-EP terms for F_{EP}). *If M is a quasi-EP term and $M \xrightarrow{*}_{R_{EP}} N$, then N is a quasi-EP term and $F_{EP}(M) \xrightarrow{*}_{R_{EP}} F_{EP}(N)$.*

*Proof (**Sketch**).* It is enough to show that the lemma holds for one-step rewrite $M \rightarrow_{R_{EP}} N$. The proof follows by induction on the structure of M. The only

non-trivial case is when $M = f(u_1, \ldots, u_k)$ and the redex is M. Then there must be a rule in $\mathcal{R}_{EP}$ of the form

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

where $C[\ldots]$ and $C'[\ldots]$ are EP-contexts, such that

$$M =_{AC} (C[x_1, \ldots, x_l])\sigma \text{ and } N =_{AC} (C[x_1, \ldots, x_l])\sigma$$

for some substitution σ. Since M is a quasi-EP term, it follows that each $x_i\sigma$ is also a quasi-EP term and then N is a quasi-EP term. From de definition of F_{EP} follows that

$$\begin{aligned} F_{EP}(M) &=_{AC} F_{EP}(C[x_1, \ldots, x_l]\sigma) \\ &= C[F_{EP}(x_1\sigma), \ldots, F_{EP}(x_l\sigma)] \\ &= C[x_1, \ldots, x_l]\sigma' \end{aligned}$$

where σ' is the substitution $\{x_1 \mapsto F_{EP}(x_1\sigma), \ldots, x_l \mapsto F_{EP}(x_l\sigma)\}$. Therefore,

$$F_{EP}(M) =_{AC} C[x_1, \ldots, x_l]\sigma' \to C'[x_1, \ldots, x_l]\sigma' =_{AC} F_{EP}(N).$$

□

Proposition 2 (Lifting). *If M and N are quasi-EP terms $F_{EP}(M) \xrightarrow{*}_{R_{EP}} F_{EP}(N)$, then $M \xrightarrow{*}_{R_{EP}} N$.*

*Proof (**Sketch**).* The proof follows by induction on the structure of M. Let $x_1, \ldots, x_l$ be the free variables in $F_{EP}(M)$ and $M_1, \ldots, M_k$ be normal EP-terms such that $v_{EP}(M_j) = x_j$ for each $j \in \{1, \ldots, l\}$ where $M = f(M_1, \ldots, /M_k)$. In addition, let

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

One can shows by induction on the structure of M and N, and using the hypothesis that they are quasi-EP terms, that

$$F_{EP}(M)\sigma =_{AC} M \text{ and } F_{EP}(N)\sigma =_{AC} N$$

Notice that, the free variables of $F_{EP}(N)$ are among the free variables in $F_{EP}(M)$ since they are related by rewriting.

Suppose there is a rewrite rule in $\mathcal{R}_{EP}$

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

where C[...] and C'[...] are EP-contexts such that $F_{EP}(M) =_{AC} C[x_1, \ldots, x_l]\theta$ and $F_{EP}(M) =_{AC} C'[x_1, \ldots, x_l]\theta$, for some substitution θ. Then

$$M =_{AC} C[x_1, \ldots, x_l](\theta \circ \sigma) \text{ and } N =_{AC} C'[x_1, \ldots, x_l](\theta \circ \sigma)$$

Hence $M \to_{\mathcal{R}_{EP}} N$. □

Lemma 3 (Preservation of $\mathcal{S}$-derivability on AC-terms). *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 $M_i =_{AC} M'_i$ and $N =_{AC} N'$, there is a derivation Π' of $M'_1, \ldots, M'_k \vdash N'$ such that $|\Pi| = |\Pi'|$.*

Lemma 4 (Preservation of $\mathcal{S}$-derivability on the decomposition of constructors). *Let X and Y be terms in normal form and let f be a binary construtor. If $\Gamma, f(X,Y) \vdash M$ is cut-free derivable, then so is $\Gamma, X, Y \vdash M$.*

*Proof (**Sketch**).* Let Π be a cut-free derivation of $\Gamma, f(X,Y) \vdash M$. It will be constructed a cut-free derivation Π' of $\Gamma, X, Y \vdash M$ by induction of $|f(X,Y)|$ with subinduction on π. Suppose Π ends with the (id). The only non trivial case is when $f(X,Y)$ is used in the rule, that is

$$M \approx_{EP} C[f(X,Y)^n, M_1, \ldots, M_k]$$

where $M_1, \ldots M_k \in \Gamma, C[\ldots]$ is an EP-context and $f(X,Y)$ fills n-holes in $C[\ldots]$. Assume that there is no subterm A of $M, M_1, \ldots M_k$ such that $A =_{AC} f(X,Y)$. Since M is in normal form

$$C[f(X,Y)^n, M_1, \ldots M_k] \xrightarrow{*}_{R_{EP}} M$$

and both $C[f(X,Y)^n, M_1, \ldots, M_k]$ and M are quasi-EP terms. Let $x = v_{EP}(f(X,Y))$. It follows from Proposition 1 that

$$C[x^n, F_{EP}(M_1), \ldots F_{EP}(M_k)] \xrightarrow{*}_{R_{EP}} F_{EP}(M).$$

Since no subterms of M and $M_1, \ldots M_k$ are equivalent to $f(X,Y)$, x does not appear in any of $F_{EP}(M)$, $F_{EP}(M_1), \ldots, F_{EP}(M_k)$. Now let a be a name that does not occur in Γ, X, Y or M. Then

$$C[a^n, F_{EP}(M_1), \ldots F_{EP}(M_k)] \xrightarrow{*}_{R_{EP}} F_{EP}(M).$$

Now by Proposition 2,

$$C[a^n, M_1, \ldots M_k] \xrightarrow{*}_{R_{EP}} M.$$

By substituting X for a,

$$C[X^n, M_1, \ldots M_k] \xrightarrow{*}_{R_{EP}} M.$$

Hence, the sequent $\Gamma, X \vdash M$ is derivable using an instance of (id) rule. By weakening follows that $\Gamma, X, Y \vdash M$ and the lemma holds. □

Lemma 5 (Preservation of $\mathcal{S}$-derivability on the decomposition of Σ_{EP}-terms). *Let $N_1, \ldots, N_k$ be normal terms and let Π be a cut-free derivation of $\Gamma, f(N_1, \ldots, N_k) \downarrow \vdash M$, where $f \in \Sigma_{EP}$. Then there exists a cut-free derivation Π' of $\Gamma, N_1, \ldots, N_k \vdash M$.*

*Proof (**Sketch**).* The proof follows by induction on $|\Pi|$.

Suppose that Π ends with an application of (id). The non trivial case is when $f(N_1, \ldots, N_k)\downarrow$ is used in the rule, that is,

$$M \approx_{\mathsf{EP}} C[f(N_1, \ldots, N_k)\downarrow^n, M_1, \ldots, M_r]$$

where $M_1, \ldots, M_r \in \Gamma$, $C[\ldots]$ is an EP-context and $f(N_1, \ldots, N_k)\downarrow$ fills n-holes in $C[\ldots]$.

- The case where there is a guarded subterm A in M or some M_i, such that $A =_{AC} f(N_1, \ldots, N_k)\downarrow$ is similar to the proof of Lemma 4.
- Suppose there is no guarded subterm A of $M, M_1, \ldots, M_r$ such that $A =_{AC} f(N_1, \ldots, N_k)\downarrow$. Since M is in normal form, one has that

  $$C[f(N_1, \ldots, N_k)\downarrow^n, M_1, \ldots, M_r] \xrightarrow{*}_{R_{EP}} M.$$

  Substituting each one of the n occurrences of $f(N_1, \ldots, N_k)\downarrow$ in the EP-context $C[\ldots]$ by $f(N_1, \ldots, N_k)$, follows that

  $$C[f(N_1, \ldots, N_k)^n, M_1, \ldots, M_r] \xrightarrow{*}_{\mathcal{R}_{EP}} C[f(N_1, \ldots, N_k)\downarrow^n, M_1, \ldots, M_r] \xrightarrow{*}_{R_{EP}} M.$$

  Since $C[\ldots]$ is formed using only function symbols in Σ_{EP} and $f \in \Sigma_{\mathsf{EP}}$, there is an EP-context $C'[\ldots]$ such that $C'[N_1, \ldots, N_k, M_1, \ldots, M_r] \approx_{\mathsf{EP}} M$. Thus, there is a derivation a cut-free derivation of $\Gamma, N_1, \ldots, N_k \vdash M$ using the (id) rule.

□

Lemma 6 (Preservation of $\mathcal{S}$-derivability on the decomposition of EP-contexts). *Let $M_1, \ldots, M_k$ be normal terms and let $C^k[]$ be an EP-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 (**Sketch**).* By induction on the size of $C[\ldots]$.

Firstly, notice that

$$C[M_1, \ldots, M_k] \xrightarrow{*}_{\mathcal{R}_{ep}} C[M_1, \ldots, M_k]\downarrow .$$

S ince $C[\ldots]$ is a context formed using only function symbols in Σ_{EP}. Consider the case where $C[\ ] = J_\circ(\ )$, where $\circ \in \{+, \bullet, \star\}$.

Hence,

$$C[M_1, \ldots, M_k] = J_\circ(C'[M_1, \ldots, M_k])$$

for some EP-context $C'[\ ]$ which is smaller than $C[\ ]$.

From the hypothesis follows that $\Gamma, J_\circ(C'[M_1, \ldots, M_k])\downarrow \vdash M$ and by Lemma 6,

$$\Gamma, C'[M_1, \ldots, M_k] \vdash M.$$

Thus, by induction hypothesis, one can compute a cut-free derivation of $\Gamma, M_1, \ldots, M_k \vdash M$. The cases where $C[\ ]$ is headed by another function symbol are treated analogously.

□

Now, the main result is proved by induction on the height of the *left premise derivation* immediately above the cut rule. As usual in cut elimination, the proof proceeds by eliminating the topmost instances of cut with the highest rank.

*Proof (**Theorem 1 (Sketch)**).*

The cut reduction is driven by the left premise derivation of the cut. The proof is divided in several cases, based on the last rule of the left premise derivation.

For instance, suppose the left premise of the cut ends with the (id)-rule :

$$\dfrac{\dfrac{}{\Gamma \vdash M}\,(id) \qquad \dfrac{\Pi_1}{\Gamma, M \vdash R}}{\Gamma \vdash R}\,(cut)$$

where $M = C[M_1, \ldots, M_k]\downarrow$, $C[\ldots]$ is an EP-context and $M_1, \ldots, M_k \in \Gamma$. By induction hypothesis $\Gamma, M \vdash R$ is cut-free derivable, hence applying Lemma 6 to Π_1 one can obtain a cut-free derivation Π' of $\Gamma \vdash R$. □

B Proof of Theorem 2

Although the changes in the equational theory, the proof of the theorem remains close to the one presented in the extended version of [12].

Lemma 7 (Saturated set closeness of $\mathcal{L}$-derivations). *Let Π be an $\mathcal{L}$-derivation of $\Gamma \vdash M$. Then for every sequent $\Gamma' \vdash M'$ occurring in Π, $\Gamma' \cup \{M'\} \subseteq St(\Gamma \cup \{M\})$.*

*Proof (**Sketch**).*

The proof follows by induction on $|\Pi|$.

During the proof it will be shown that for each rule ρ in $\mathcal{L}$ other than (r) such that

$$\dfrac{\Gamma' \vdash M'}{\Gamma \vdash M}\,\rho$$

one has $St(\Gamma \cup \{M\}) = St(\Gamma \cup \{M'\})$.

Consider the case where ρ is the rule (sign):

$$\dfrac{\Gamma_1, \mathsf{sign}(M, K),\ \mathsf{pub}(L), M \vdash N}{\Gamma_1, \mathsf{sign}(M, K),\ \mathsf{pub}(L) \vdash N}\,(\mathsf{sign}),\ \ K =_{AC} L$$

where $\Gamma := \Gamma_1 \cup \{\mathsf{sign}(R, K), \mathsf{pub}(L)\}$ and $\Gamma' := \Gamma_1 \cup \{\mathsf{sign}(R, K), \mathsf{pub}(L), R\}$. Then $St(\Gamma \cup \{M\}) = St(\Gamma \cup \{\mathsf{sign}(R, K), \mathsf{pub}(L), M\}) = St(\Gamma' \cup \{M\})$, that is, $\Gamma' \cup \{M\} \subseteq St(\Gamma \cup \{M\})$, trivially.

The non-trivial case is the rule (blind_2):

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

where $\Gamma = \Gamma_1 \cup \{\mathsf{sign}(\mathsf{blind}(N, R), K)\}$.

Notice that $St(\Gamma \cup \{M\}) = St(\Gamma \cup \{\mathsf{sign}(\mathsf{blind}(N, R), K), M\})$ which contains the proper subterms N and K. Hence, the term $\mathsf{sign}(N, K) \in sst(\Gamma \cup \{M\})$. Therefore $\Gamma' \cup \{M'\} \subseteq St(\Gamma' \cup \{M'\}) = St(\Gamma \cup \{M\})$ follows the result. □

Lemma 8 (Quadratic bound on $\mathcal{L}$-derivation length). *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 quadratic with respect to the size of $\Gamma \cup \{M\}$.*

*Proof (**Sketch**).*

Let Π be an $\mathcal{L}$-derivation of $\Gamma \vdash M$, by Lemma 7, each sequent $\Gamma' \vdash M'$ occurring in Π is such that $\Gamma' \cup \{M'\} \subseteq St(\Gamma \cup \{M\})$. Replace the derivation Π by a derivation Π' in which each sequent appears only once in each branch. Moreover, analyzing the rules in $\mathcal{L}$ one can notice that, when read from the conclusion to the premise, the left-hand sides of the rules preserve their principal formula and more rules are added. Assuming that in each step, one term from $St(\Gamma \cup \{M\})$ is added into the premise, at most $|St(\Gamma \cup \{M\})|$ rules can be applied. Hence, the lenght of the derivation is bounded by the size of $St(\Gamma \cup \{M\})$, which is quadratic in the size of $\Gamma \cup \{M\}$. □

*Proof (**Theorem 2 (sketch)**).*

Assume $|St(\Gamma \cup \{M\})| = n$. For the proof, one has to use Lemmas 7 and 8 and *weakening* property:

- Weakening: if Π is an $\mathcal{L}$-derivation of $\Gamma \vdash M$ and $\Gamma \subseteq \Gamma'$, then there exists an $\mathcal{L}$-derivation Π' of $\Gamma' \vdash M$ such that $|\Pi'| = |\Pi|$.

Suppose $\Gamma \vdash M$ is provable in $\mathcal{L}$. Let $M_1, \ldots, M_n$ be an enumeration of the set $St(\Gamma \cup \{M\})$. There is a shortest proof of $\Gamma \vdash M$ where each sequent appears exactly once in each branch of the proof. 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 is applicable, successively, to $\Gamma \vdash M$. Since no repetitions of sequents are possible, $q \leq n$. Also, it should be noticed that the rules of $\mathcal{L}$ are invertible: one does not lose provability at any point of the proof search. That is, suppose both principal-term and rule pairs (N, ρ) and (N', ρ') are applicable to $\Gamma \vdash M$; then if $\Gamma' \vdash M$ is the unique premise determined by either (N, ρ) or (N', ρ'), then, respectively, either (N', ρ') or (N, ρ) applies to $\Gamma' \vdash M$.

A proof search strategy for $\Gamma \vdash M$ is based on repeatedly try all possible applicable pairs (M', ρ') for each possible $M' \in St(\Gamma \cup \{M\})$ and each left-rule ρ' (that is bounded by $6\,n$) and for all generated sequents taking in care elimination of redundancies based on the previous observations and weakening. For all generated sequent $\Delta \vdash M$, before trying possible applicable pairs, one should check whether $\Delta \Vdash_{\mathcal{R}} M$. By Lemma 1, checking $\Vdash_{\mathcal{R}}$ takes $\mathcal{O}(n^a f(n))$ for some constant a. By (**F1**), checking applicability takes $\mathcal{O}(n^l f(n))$ for some constant l. Therefore the whole procedure takes $\mathcal{O}(n^{c+l} f(n))$.

The pseudo-algorithm works in the following way:

1: **Input**: $k := 0$ and $\Delta := \Gamma$
2: **if** $\Delta \Vdash_{\mathcal{R}} M$ **then** YES
3: **else**"not polynomially reducible to EDP"
4: **while** $k \leq n$ and "not polynomially reducible to EDP" **do**
5: $i := 1$
6: **while** $i \leq n$ and "not applicable" **do**
7: **if** there exists a left-rule ρ such that (M_i, ρ) is applicable to the sequent $\Delta \vdash M$, let $\Gamma_{i,\rho} \vdash M$ be the unique premise of ρ determined by **F2** **then** $\Delta := \Gamma_{i,\rho}$
8: **else** $i := i + 1$
9: **end if**
10: **end while**
11: **if** $\Delta \Vdash_{\mathcal{R}} M$ **then** YES
12: **else** k:=k+1
13: **end if**
14: **end while**
15: **end if**

References

1. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 367(1-2):2–32, 2006.
2. F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.
3. V. Bernat and H. Comon-Lundh. Normal proofs in intruder theories. In *ASIAN*, volume 4435 of *Lecture Notes in Computer Science*, pages 151–166. Springer-Verlag, 2006.
4. M. Bezem, J.W. Klop, and R. de Vrijer, editors. *Term Rewriting Systems by TeReSe.* Number 55 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2003.
5. J. Bull and D. J. Otwary. The authetication protocol. Technical Report CIS3/PROJ/CORBA/SC/1/CSM/436-04/03, Defense Research Agency, 1997.
6. B. Bursuc, H. Comon-Lundh, and S. Delaune. Deducibility constraints, equational theory and electronic money. In *Rewriting, Computation and Proof*, volume 4600 of *Lecture Notes in Computer Science*, pages 196–212. Springer-Verlag, 2007.
7. 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.
8. S. Delaune. *Vérification des protocoles cryptographiques et propriétés algébriques.* PhD thesis, École Normale Supérieure de Cachan, 2006.
9. D. Kapur, P. Narendran, and L. Wang. An E-unification algorithm for analyzing protocols that use modular exponentiation. In *Proc. 14th Int. Conf. on Term Rewriting and Applications*, volume 2706 of *Lecture Notes in Computer Science*, pages 165–179. Springer-Verlag, 2003.
10. D. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, 40:284–303, 1990.
11. B. Schneier. *Applied Cryptography.* John Wiley & Sons, Inc., 1996.
12. A. Tiu and G. Rajeev. A proof theoretic analysis of intruder theories. In *Proc. 20th Int. Conf. on Term Rewriting and Applications*, volume 5595 of *Lecture Notes in Computer Science*, pages 103–117. Springer-Verlag, 2009.