P. Lafourcade

Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption

Research Report LSV-05-21
November 2005

Laboratoire Spécification et Vérification

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Ecole Normale Supérieure de Cachan
61, avenue du Président Wilson
94235 Cachan Cedex France

Intruder Deduction for the Equational Theory of *Exclusive-or* with Commutative and Distributive Encryption

Pascal Lafourcade[1,2⋆]

[1] LSV, ENS de Cachan & CNRS UMR 8643 & INRIA Futurs project SECSI, 94235 Cachan, France, http://www.lsv.ens-cachan.fr/lafourca
[2] LIF, Université Aix-Marseille 1 & CNRS UMR 6166, 13453 Marseille Cedex 13, France, http://www.cmi.univ-mrs.fr/laforuca

Abstract. The first step in the verification of cryptographic protocols is to decide the intruder deduction problem, that is the vulnerability to a passive attacker. We extend the *Dolev-Yao* model in order to model this problem in presence of the equational theory of a commutative encryption operator which distributes over the *exclusive-or* operator. These operators are frequently used in cryptographic protocols. For instance the well-known RSA encryption is a commutative encryption, and the *exclusive-or* is used in several cryptographic protocols. The interaction between the commutative distributive law of the encryption and *exclusive-or* offers more possibilities to decrypt an encrypted message than in the non-commutative case. We prove decidability of the intruder deduction problem for a commutative encryption which distributes over *exclusive-or* with a DOUBLE-EXP-TIME procedure.

1 Introduction

Today, the number of interactive services proposed on internet blows up. Most of them use cryptographic protocols to guarantee some level of security. For instance they are employed in internet banking, video on demand services, wireless communications, *etc.* They can be seen as relatively simple programs which are executed in an untrusted environment.

There are different approaches for modeling cryptographic protocols and analyzing their security properties. One of them is the approach of Dolev and Yao [10], which consists in modeling the attacker capabilities by a deduction system. This model is often used to analyze the security of protocols against a *passive* attacker, *i.e* an intruder which obtains some informations by eavesdropping on the network the communication between honest participants and deduces some information from these messages using the deduction system. The question whether a passive attacker gets a certain information from observed messages on the network is called the *intruder deduction problem.*

⋆ This work was partially supported by the research programs ACI-SI Rossignol, and RNTL PROUVÉ (n° 03 V 360).

Usually the capabilities of the intruder are based on the so-called *perfect cryptography assumption*, *i.e.* it is impossible to obtain any information about an encrypted message without knowing the exact key necessary to decrypt this message. Unfortunately, this perfect cryptography assumption is too idealistic: There are protocols which can be proved secure under the perfect cryptography assumption, but which are in reality insecure since an attacker can use properties of the cryptographic primitives in combination with the protocol rules to learn some secret informations (see [7] for a survey). It is necessary to relax this assumption by increasing the deductive power of the intruder. One possibility is to add the capability to take into account some algebraic properties to model an intruder in more realistic way, which may find new attacks.

Solutions to the intruder deduction problem modulo an equational theory are known for the cases of *exclusive-or*, of Abelian groups [5, 2], of a homomorphism symbol alone [6], and of combinations of these theories [11, 8]. We have already studied the case of non-commutative encryption which distributes over the *exclusive-or* symbol in [12]. In this paper we investigate the case of commutative encryption, *i.e.* $\{\{u\}_{k1}\}_{k2} = \{\{u\}_{k2}\}_{k1}$, which distributes over the *exclusive-or* symbol *i.e.* $\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$. The commutativity of encryption requires to define new notions and to find new proof transformations, since one encrypted message can be partially decrypted by several different keys. This raises some difficulties to design a normalization of proof. In the non-commutative case it is enough to consider the applications of the *exclusive-or* symbol as early as possible. In the case of the commutative encryption we have to apply as early as possible the decryption and after as early as possible the *exclusive-or*. We obtain a decision procedure in DOUBLE-EXP-TIME for the intruder deduction problem with the equational theory of the *exclusive-or* and commutative distributive encryption over this operator. The combination algorithm proposed in [4] can not be applied since the equational theories of the $\oplus$ operation and of the commutative encryption operation are not disjoint.

2 Preliminaries

We referee the reader to [9, 1] for an overview of rewriting.
Let Σ be a signature. $T(\Sigma, X)$ denotes the set of terms over the signature Σ and the set of variables X, that is the smallest set such that:

1. $X \subseteq T(\Sigma, X)$;
2. if $t_1, \ldots, t_n \in T(\Sigma, X)$, and $f \in \Sigma$ has arity $n \geq 0$, then $f(t_1, \ldots, t_n) \in T(\Sigma, X)$.

We abbreviate $T(\Sigma, \emptyset)$ as $T(\Sigma)$; elements of $T(\Sigma)$ are called *Σ-ground terms*. The set of variables occurring in a term t is denoted by $\mathcal{V}(t)$.

The *set of occurrences* of a term t is defined recursively as $\mathcal{O}(f(t_1, \ldots, t_n)) = \{\epsilon\} \cup \bigcup_{i=1\ldots n} i \cdot \mathcal{O}(t_i)$. For instance, $\mathcal{O}(f(a, g(b, x))) = \{\epsilon, 1, 2, 21, 22\}$. The *size* $|t|$ of a term t is defined as its number of occurrences, that is $|t| = \mathit{cardinality}(\mathcal{O}(t))$. We extend the notion of size to a set of terms T by $|T| = \Sigma_{t \in T}|t|$. If $o \in \mathcal{O}(t)$ then the *subterm of t at position o* is defined recursively by:

– $t\,|_\epsilon = t$
– $f(t_1, \ldots, t_n)\,|_{j \cdot o} = t_j\,|_o$

A term r is a *subterm* of a term t if r is a subterm of t at some position of t.

A Σ*-equation* is a pair $(l, r) \in T(\Sigma, X)$, commonly written as $l = r$. The relation $=_E$ generated by a set of Σ-equations E is the smallest congruence on $T(\Sigma)$ that contains all ground instances of all equations in E.

A Σ*-rewriting system* R is a finite set of so-called *rewriting rules* $l \to r$ where $l \in T(\Sigma, X)$ and $r \in T(\Sigma, \mathcal{V}(l))$. A term t is in *normal form* if there is no term s with $t \to s$. If $t \to^* s$ and s is a normal form then we say that s is a *normal form of* t, and write $s = t\!\downarrow$.

Let T be a set of terms, the mapping $S : T \to T$ is idempotent if for every $X \subseteq T$: $S(S(X)) = S(X)$. The mapping S is monotone if for all $X, Y \subseteq T$: if $X \subseteq Y$ then $S(X) \subseteq S(Y)$. S is transitive if for all $X, Y, Z \subseteq T$, $X \subseteq S(Y)$ and $Y \subseteq S(Z)$ implies $X \subseteq S(Z)$. The following Proposition is straightforward.

Proposition 1 *Let S be a mapping from sets of terms to sets of term. If S is idempotent and monotone then S is transitive.*

3 A Dolev-Yao Model for Rewriting Modulo AC

We consider the classic model of deduction rules introduced by Dolev and Yao [10] in order to model the deductive capacities of a passive intruder. We present an extension of this model with the equational theory XCDE (*eXclusive-or* with a Commutative Distributive Encryption over $\oplus$).

The knowledge of the intruder is represented by terms built over a finite signature $\Sigma = \{\langle\cdot,\cdot\rangle, \{\cdot\}_\cdot, \oplus\} \uplus \Sigma_0$, where Σ_0 is a set of constant symbols. The term $\langle u, v\rangle$ represents the pairing of the two terms u and v. The term $\{u\}_K$ represents the encryption of the term u by a finite multiset of keys K and we consider that $\{u\}_\emptyset = u$. For the sake of simplicity we here only consider symmetric commutative encryption.

The equational theory XCDE is represented by the following convergent rewriting system R: $0 \oplus x \to x$; $x \oplus x \to 0$; $\{0\}_z \to 0$; $\{x \oplus y\}_z \to \{x\}_z \oplus \{y\}_z$. R is terminating and confluent modulo associativity and commutativity of $\oplus$, and such that for all terms $t, s \in T(\Sigma)$ we have that $t =_E s$ if and only if $t\!\downarrow =_{AC} s\!\downarrow$. The deduction system of Figure 1 corresponds to the deductive capabilities of an attacker considering the equational theory XCDE.

Definition 1 *A proof P of $T \vdash w$ is a finite tree such that:*

– *every leaf of P is label by $v \in T$.*
– *every node of P with n sons ($n \geq 1$) labeled with $T \vdash v_1, \ldots, T \vdash v_n$, is labeled with $T \vdash v$ such that $\dfrac{T \vdash v_1 \quad \ldots \quad T \vdash v_n}{T \vdash v}(R)$ is an instance of the rule of Figure 1.*
– *the root of P is labeled with $T \vdash w$.*

A sub-proof P' *of a proof* P *is a sub-tree of* P*. The* size *of a proof* P *is the number of nodes in* P*, denoted by* $|P|$*.*

$$(A)\frac{u \in T}{T \vdash u\downarrow} \qquad (UL)\frac{T \vdash r}{T \vdash u\downarrow} \quad \textit{if } \langle u, v\rangle = r$$

$$(P)\frac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v\rangle\downarrow} \qquad (UR)\frac{T \vdash r}{T \vdash v\downarrow} \quad \textit{if } \langle u, v\rangle = r$$

$$(C_K)\frac{T \vdash u \qquad T \vdash K}{T \vdash \{u\}_K\downarrow} \qquad (GX)\frac{T \vdash u_1 \qquad \ldots \qquad T \vdash u_n}{T \vdash u_1 \oplus \ldots \oplus u_n\downarrow}$$

$$(D_K)\frac{T \vdash r \qquad T \vdash K}{T \vdash u\downarrow} \quad \textit{if } r =_E \{u\}_K$$

Fig. 1. A Dolev-Yao proof system working on normal forms by a rewrite system R modulo AC for a commutative encryption, where $K = \{k_1^{\alpha_1}, \ldots, k_n^{\alpha_n}\}$is a multiset of keys, where α_i represents the multiplicity of the keys k_i in K.

This proof system is composed of the following rules: (A) the intruder may use any term which is in his initial knowledge, (P) the intruder can build a pair of two messages, (UL, UR) he can extract each member of a pair, (C) he can encrypt a message u with a multiset K of keys, (D) if he knows a multiset K of keys then he can decrypt a message encrypted by K. Let $K = \{k_1^{\alpha_1}, \ldots, k_n^{\alpha_n}\}$ be a multiset of keys, the sequent $T \vdash K$ is short for: α_1 times the sequent $T \vdash k_1, \ldots, \alpha_n$ times the sequent $T \vdash k_n$. Sometimes, we shall annotate the rules (C) and (D) by the multiset of keys that they use, yielding rules (C_K) and (D_K). Because of the algebraic properties of the $\oplus$ operator, we add a family of rules (GX) which allows the intruder to build a new term from an arbitrary number of already known terms by using the $\oplus$ operator.

In fact, this proof system is equivalent in deductive power to a variant of the system in which terms are not automatically normalized, but in which arbitrary equational proofs are allowed at any moment of the deduction. The equivalence of the two proof systems has been shown in [6] without AC axioms; in [11] this has been extended to the case of a rewrite system modulo AC. We assume that all terms are normalized terms, we will omit the symbol $\downarrow$.

4 Locality Result and Complexity

Our starting point is the locality technique introduced by McAllester [13]. He considers deduction systems which are represented by finite sets of Horn clauses. He shows that there exists a polynomial-time algorithm to decide the deducibility of a term w from a finite set of terms T if the deduction system has the so-called *locality property*. A deduction system has the *locality property* if any proof can be transformed into a *local proof*, that is a proof where all nodes are syntactic subterms of $T \cup \{w\}$. The idea of the proof is to check existence of a local proof

by a saturation algorithm which computes all syntactic subterms of $T \cup \{w\}$ that are deducible from T. In [12] we generalize McAllester's approach, we just recall the definition of a local proof and the locality Theorem. In the rest of the paper we denote $T \cup \{w\}$ by T, w.

Definition 2 *Let S be a function which maps a set of terms to a set of terms. A proof P of $T \vdash w$ is* S-local *if all nodes are labeled by some $T \vdash v$ with $v \in S(T, w)$. A proof system is* S-local *if whenever there is a proof of $T \vdash w$ then there is also a S-local proof of $T \vdash w$.*

Theorem 1 *Let S be a function mapping a set of terms to a set of terms, and P a proof system. Let T be a set of terms, let w be a term and let n be $|T, w|$. If:*

1. *one-step deducibility of $S \vdash u$ in P is decidable in time $g(|S, u|)$ for any term u and set of terms S,*
2. *the set $S(T, w)$ can be constructed in time $f(n)$,*
3. *P is S-local,*

then provability of $T \vdash w$ in the proof system P is decidable in time $f(n) + f(n) * f(n) * g(f(n))$ (non-deterministic if one of (2), (1) is non-deterministic).

We say that u is one-step deducible from a set of hypotheses H if there exists an instance $\dfrac{T \vdash r_1 \quad \ldots \quad T \vdash r_n}{T \vdash r}(R)$ of some deduction rule such that $r = u$ and $r_i \in H$. The one-step deducibility is decidable in polynomial time for the equational theory XCDE. Observe first that all rules of deduction of Figure 1 are binary excepted the rule (GX) (rule (C_K) (resp. (D_K)) are shorts for finite number of consecutive applications of rule (C_{k_i}) (resp. (D_{k_i})). For all these binary rules proving the one-step deducibility takes a polynomial time. For the rule (GX) the problem can reduce to solve system of equations in $\mathbb{Z}/2\mathbb{Z}$ as in [12]. We illustrate the idea of this reduction, with the following example.

Example 1 *Let $T = \{a_1 \oplus a_2 \oplus a_3, a_1 \oplus a_4, a_2 \oplus a_4\}$ and $w = a_1 \oplus a_2$, where every a_i contains no $\oplus$. We introduce one numerical variable x_0, x_1, x_2 for each element of T:*

$$x_0 \text{ for } a_1 \oplus a_2 \oplus a_3$$
$$x_1 \text{ for } a_1 \oplus a_4$$
$$x_2 \text{ for } a_2 \oplus a_4$$

For every element of the sum we create an equation, we get the equation system:

$$\begin{cases} a_1 : x_0 \oplus x_1 = 1 \\ a_2 : x_0 \oplus x_2 = 1 \\ a_3 : x_0 = 0 \\ a_4 : x_1 \oplus x_2 = 0 \end{cases}$$

The system has a solution over $\mathbb{Z}/2\mathbb{Z}$ if and only if w is deducible in one-step from T by (GX). In this example the system has a solution: $x_0 = 0, x_1 = 1, x_2 = 1$.

In the rest of the paper, to prove locality, we define a new notion of subterms (Definition 6) and some transformations of proof which enable us to prove that any proof can be transformed into a normal proof. Hence we prove that a normal proof is in fact a local proof in Theorem 2, yielding the decidability of the intruder deduction problem, using Theorem 1.

5 Terms and Subterms

Definition 3 *Let u be a term in normal form, u is* headed with $\oplus$ *if u is of the form $u_1 \oplus \ldots \oplus u_n$ with $n > 1$. Otherwise u is* not headed with $\oplus$. *A term u in normal form is called* headed with $\{.\}_K$ *if u is of the form $u = \{t\}_K$. Otherwise u is* not headed with $\{.\}_K$. *We define the function atoms(u):*

- *If $u = u_1 \oplus \ldots \oplus u_n$, where each of the u_i is not headed with $\oplus$, then atoms$(u) = \{u_1, \ldots, u_n\}$. The u_i's are called the* atoms *of u.*
- *If u is not headed with $\oplus$ then atoms$(u) = \{u\}$.*

Example 2 *$t_1 = u \oplus \langle v, w\rangle$ is headed with $\oplus$, but $t_2 = \langle u, v \oplus w\rangle$ is not, hence atoms$(t_2) = \{t_2\}$ and atoms$(t_1) = \{u, \langle v, w\rangle\}$.*

The definition of atoms(T) is generalized to sets of terms T in normal form by setting atoms$(T) := \bigcup_{t\in T}$ atoms(t). According to the definition, the function atoms is monotone and idempotent. $\mathcal{P}[K]$ denotes the set of all the partitions of the set K.

Definition 4 *Define the set of* syntactic subterms *of a term t as the smallest set $S(t)$ such that:*

- *$t \in S(t)$.*
- *if $\langle u, v\rangle \in S(t)$ then $u, v \in S(t)$.*
- *if $\{u\}_K \in S(t)$ and $K = \{k_1^{\alpha_1}, \ldots, k_p^{\alpha_p}\}$ then $u \in S(t)$ and $k_i \in S(t)$ for all i $1 \leq i \leq p$.*
- *if $u = u_1 \oplus \ldots \oplus u_n \in S(t)$ then atoms$(u) \subseteq S(t)$.*

The definition of S is extended to a set T of terms in normal form by setting $S(T) := \bigcup_{t\in T} S(t)$. Since the encryption is commutative, the number of subterms is exponential in the size of the set of keys of T (consider all the possible combinations of keys for an encrypted term).

Example 3 *If $u = \{a\}_{k1,k2,k3}$ then*
$S(u) = \{u, a, k_1, k_2, k_3, \{a\}_{k1}, \{a\}_{k2}, \{a\}_{k3}, \{a\}_{k1,k2}, \{a\}_{k2,k3}, \{a\}_{k1,k3}\}$

In the definition of $S(t)$ we do not take care of the distributivity of encryption. Because we work only on normal forms the notion of a syntactic subterm ignores the fact that the term $\{a\}_K \oplus \{b\}_K \oplus \{c\}_K$ is equal to $\{a \oplus b \oplus c\}_K$, and that $a \oplus b \oplus c$ should be considered to be a subterm of $\{a\}_K \oplus \{b\}_K \oplus \{c\}_K$ and also all sums encrypted with the set $\mathcal{P}[K]$.

Definition 5 *For any term t, $S_T(t)$ is the smallest set such that:*

- $S(t) \subseteq S_T(t)$.
- *If* $n > 1$, $K = \{k_1^{\alpha_1}, \ldots, k_p^{\alpha_p}\}$ *and* $\{u_1\}_K \oplus \ldots \oplus \{u_n\}_K \in S_T(t)$ *then* $u_1 \oplus \ldots \oplus u_n \in S_T(t)$.

By definition $S(T) \subseteq S_T(T)$. The definition is extended to a set T of terms in normal form by setting $S_T(T) := \bigcup_{t \in T} S_T(t)$. As in Definition 4, Definition 5 considers also all the possible combinations of keys for an encrypted sum of terms.

Proposition 2 *For any set of terms $M \subseteq T_\Sigma$, we have:*

- *atoms*$(M) \subseteq S(M)$ *for any set of terms* $M \subseteq T_\Sigma$.
- *atoms*$(S_T(M)) \subseteq S_T(M)$.
- $S(S(M)) = S(M)$ *and* $S_T(S_T(M)) = S_T(M)$.

Proof. Obvious from the definitions of S, atoms and S_T.

Definition 6 *Define $S_\oplus$ as all combinations of terms of $S_T(T)$ by $\oplus$:*

$$S_\oplus(T) := \left\{ (\bigoplus_{s \in M} s)\downarrow \mid M \subseteq S_T(T) \right\}$$

Note that the size of $S_\oplus$ is double-exponential in the size of T and $S_T(T) \subseteq S_\oplus(T)$: one exponential for the computation of $S(T) \subseteq S_T(T)$ and the second exponential for all the partial sums.

Proposition 3 *Let A and B be two sets of terms in normal form, the mappings S, S_T and $S_\oplus$ are monotone and have the property:*

- $S(A \cup B) = S(A) \cup S(B)$.
- $S_T(A \cup B) = S_T(A) \cup S_T(B)$.
- $S_\oplus(A) \cup S_\oplus(B) \subseteq S_\oplus(A \cup B)$.

Proof. Monotonicity is obvious from the definitions of $S(T)$, $S_T(T)$ and $S_\oplus(T)$.

Let $A = \{a\}$ and $B = \{b\}$, $S_\oplus(A) = \{0, a\}$ and $S_\oplus(B) = \{0, b\}$ then $S_\oplus(A) \cup S_\oplus(B) = \{0, a, b\} \subseteq S_\oplus(A \cup B) = \{0, a \oplus b, a, b\}$ but $S_\oplus(A) \cup S_\oplus(B) \neq S_\oplus(A \cup B)$.

The following Proposition is proved in Appendix.

Proposition 4 *Let M be a set of terms then $S_\oplus(S_\oplus(M)) = S_\oplus(M)$. The mappings S, S_T and $S_\oplus$ are transitive.*

6 Different Kinds of Proofs

Definition 7 *Let P be a proof of $T \vdash w$. P is* flat *if there is no (GX) (respectively (C) and (D)) rule immediately above another (GX) (respectively (C) and (D)) rule. P is* simple *if* (1) *each node $T \vdash v$ occurs at most once on each branch,* (2) *each node $T \vdash v$ occurs at most once as hypothesis of a rule (GX),* (3) *there is no consecutive application of (C_K) and $(D_{K'})$ (in either order) if $K \cap K' \neq \emptyset$.*

In any proof we can always merge two consecutive applications of a rule (C_K) (respectively (D_K) and (GX)) and get a flat proof. Any proof can be transformed into a simple proof since we can always cut some branch or piece of branch of the proof.

Proposition 5 *Let K and K' be two sets of keys such that $K \cap K' = \emptyset$. Applying the rule (D_K) to a term u and then the rule $(C_{K'})$ yields the same result as applying the rule $(C_{K'})$ to u and then the rule (D_K).*

Proof. The fact that $K \cap K' = \emptyset$ is the key of this result.

Intuitively, in a *D-eager* proof the (D) rule is applied as early as possible and in a *$\oplus$-eager* proof the (GX) rule is applied as early as possible.

Definition 8 *Let P be a proof of $T \vdash w$. P is a **D-eager** proof if:* (1) *there is no hypothesis of a rule (GX) which is headed with $\{.\}_K$ and a rule $(D_{K'})$ just after a (GX) such that $K \cap K' \neq \emptyset$,* (2) *there is no (C) just above rule (D). P is a **$\oplus$-eager** proof if all the rules (C_{K_i}) immediately above a (GX) in P have $K_i \cap K_j = \emptyset$ for all i, j such that $i \neq j$.*

We precise $S(T)$-local proof instead of S-local, where T is the set of terms on which S is applied. A *normal* proof consists of initial subproofs which are $S_\oplus(T)$-local, followed by a proof tree consisting of the rules (GX), (C), (P) only.

Definition 9 *Let P be a proof of $T \vdash u$. P is a* normal proof *if :*

- *either $u \in S_\oplus(T)$ and P is an $S_\oplus(T)$-local proof,*
- *or $P = C[P_1, \ldots, P_n]$ where every proof P_i is a normal proof of some $T \vdash v_i$ with $v_i \in S_\oplus(T)$ and the context C is built using the inference rules (P), (C), (GX) only.*

7 Transformations of Proofs

Lemma 1 *Let P be a simple and flat proof of $T \vdash w$. Then there exists a proof P' of $T \vdash w$ such that P' is a simple, flat and D-eager proof.*

Proof. Let P be a simple and flat proof of $T \vdash w$. We transform this proof into a simple, flat and *D-eager* proof of $T \vdash w$ by induction on the number of nodes of P. We consider the last rule of the proof, if it is:

– (A): the result holds.
– (GX), (P), (UR), (UL), (C): we apply the induction hypotheses on all direct sub-proofs.
– (D_{K_2}): we always apply the induction hypotheses on the key part of the rule (D_{K_2}), for the encrypted part we consider the rule above (D_{K_2}) is :
  • (A), (P), (UR), (UL) we apply the induction hypotheses on all direct sub-proofs.
  • (C): we can switch the two rules using Proposition 5 and simplicity (to get a *D-eager* proof) and apply the induction hypotheses on the sub-proofs.
  • (GX) if all encrypted hypotheses of the (GX) are encrypted by sets of keys K_i such that $K_i \cap K_2 = \emptyset$ then we apply the induction hypotheses on the sub-proofs. Otherwise we consider that the hypotheses of the rule (GX) can be split into smaller sums which all give an encrypted term and we apply the transformation described in Figure 3. In certain cases some additional transformations are required to preserve simplicity: we cut the same hypotheses of the rule (GX) or branch of the proof for the new nodes introduced. Moreover if a rule (GX) has just one hypothesis, this rule can be deleted. Since $K_2 \cap K_1 \neq \emptyset$ and $n \geq 2$, the size of the initial proof is $\Sigma_{i=1}^{i=n}|\pi_{B_i}| + |\pi_{K_2}| + 2$ is greater or equal than $\Sigma_{i=1}^{i=n_1}|\pi_{B_i}| + |\pi_{K_2 \cap K_1}| + 2$ the size of this sub-proof, hence we apply the induction hypotheses on the sub-proof ended by the rule $(D_{K_2 \cap K_1})$.□

$$(GX)\dfrac{(GX)\dfrac{T \vdash x_1 \quad \dots \quad T \vdash x_n}{T \vdash x_1 \oplus \ldots \oplus x_n} \quad T \vdash y_1 \quad \dots \quad T \vdash y_m}{T \vdash x_1 \oplus \ldots \oplus x_n \oplus y_1 \oplus \ldots \oplus y_m}$$

$$\Downarrow$$

$$(GX)\dfrac{T \vdash x_1 \quad \dots \quad T \vdash x_n \quad T \vdash y_1 \quad \dots \quad T \vdash y_m}{T \vdash x_1 \oplus \ldots \oplus x_n \oplus y_1 \oplus \ldots \oplus y_m}$$

Fig. 2. Transformation of (GX)-(GX) into (GX)

Proposition 6 *The transformations of proofs given in Figures 2 and 4 decrease the number of nodes of the initial proof.*

Proof. We denote by π_x the subproof of P with root $T \vdash x$. These transformations transform a proof with some hypotheses and a conclusion into a proof of the same hypotheses and the same conclusion. Figure 2: It is obvious.
Figure 4: The number of nodes of the initial proof is:
$\alpha_I = \Sigma_{i=1}^{i=m}|\pi_{z_i}| + |\pi_{x_1}| + |\pi_{x_2}| + |\pi_{K_1}| + |\pi_{K_2}| + 3$
The number of nodes of the transformed proof is:

Fig. 3. Transformation *D-eager* $K_2 \cap K_1 \neq \emptyset$ and $n \geq 2$

$$
\dfrac{\dfrac{\dfrac{T \vdash x_1 \quad T \vdash K_1}{T \vdash \{x_1\}_{K_1}}(C_{K_2}) \quad \dfrac{T \vdash x_2 \quad T \vdash K_2}{T \vdash \{x_2\}_{K_2}}(R_1) \dfrac{\vdots}{T \vdash z_1} \ldots (R_m) \dfrac{\vdots}{T \vdash z_m}}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2} \oplus z_1 \oplus \ldots \oplus z_m}(GX)}{K_1 \cap K_2 \neq \emptyset}
$$

$$
\Downarrow
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{T \vdash x_1 \quad T \vdash K_1 \setminus K_2}{T \vdash \{x_1\}_{K_1 \setminus K_2}}(C_{K_1 \setminus K_2}) \quad \dfrac{T \vdash x_2 \quad T \vdash K_2 \setminus K_1}{T \vdash \{x_2\}_{K_2 \setminus K_1}}(C_{K_2 \setminus K_1})}{T \vdash \{x_1\}_{K_1 \setminus K_2} \oplus \{x_2\}_{K_2 \setminus K_1}}(GX) \quad T \vdash K_1 \cap K_2}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2}}(C_{K_1 \cap K_2}) \quad \dfrac{\vdots}{T \vdash z_1} \ldots (R_m) \dfrac{\vdots}{T \vdash z_m}}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2} \oplus z_1 \oplus \ldots \oplus z_m}(GX)
$$

Fig. 4. Transformation $\oplus$-*eager*, $K_1 \cap K_2 \neq \emptyset$ and all (R_i) are different of (C)

$\alpha_T = \Sigma_{i=1}^{i=m}|\pi_{z_i}| + |\pi_{x_1}| + |\pi_{x_2}| + |\pi_{K_1\setminus K_2}| + |\pi_{K_2\setminus K_1}| + |\pi_{K_1\cap K_2}| + 5$
Observe that $|\pi_{K_1}| = |\pi_{K_1\cap K_2}| + |\pi_{K_1\setminus K_2}|$ and $|\pi_{K_2}| = |\pi_{K_1\cap K_2}| + |\pi_{K_2\setminus K_1}|$.

$$\begin{aligned}\alpha_I - \alpha_T &= |\pi_{K_1}| + |\pi_{K_2}| - |\pi_{K_1\setminus K_2}| - |\pi_{K_2\setminus K_1}| - |\pi_{K_1\cap K_2}| - 2\\ &= |\pi_{K_1\cap K_2}| + |\pi_{K_1\setminus K_2}| + |\pi_{K_2}| - |\pi_{K_1\setminus K_2}| - |\pi_{K_2\setminus K_1}| - |\pi_{K_1\cap K_2}| - 2\\ &= |\pi_{K_1\cap K_2}| + |\pi_{K_2\setminus K_1}| - |\pi_{K_2\setminus K_1}| - 2\\ &= |\pi_{K_1\cap K_2}| - 2\end{aligned}$$

Since $K_1 \cap K_2 \neq \emptyset$, hence $|\pi_{K_1\cap K_2}| \geq 2$ and the number of nodes is decreasing.□

Lemma 2 *If there is a simple, flat and D-eager proof of $T \vdash w$ then there is also a simple, flat, D-eager and $\oplus$-eager of $T \vdash w$.*

Proof. Let P be a simple, flat and *D-eager* proof of $T \vdash w$, we apply many times the proof transformation rules given in Figures 2 and 4. The application of these transformations terminates since Proposition 6 shows that they decrease the number of nodes of a proof and the transformation of a proof into a simple and flat proof decreases obviously the number of nodes. Moreover these transformations do not make appear any rule (D) just after a rule (GX) and any rule (D) just after a rule (C), hence the proof is again *D-eager*.□

8 Properties of Proofs

Lemma 3 shows that all nodes stemmed from a rule (UR)(UL) are in $S(T)$ for simple proof. Lemma 4 proves that all nodes stemmed from a rule (D) have the encrypted hypothesis in $S_\oplus(T)$ for a simple, flat, *D-eager* and *$\oplus$-eager* proof. In Lemma 5 we prove that such a proof can be transformed in a normal proof using Lemma 3 and Lemma 4. The proofs of these lemmata are in Appendix.

Lemma 3 *Let P be a simple proof of $T \vdash u$ or $T \vdash v$. If P is one of*

$$(UL)\frac{\begin{array}{c}\vdots\\ T \vdash \langle u, v\rangle\end{array}}{T \vdash u} \qquad (UR)\frac{\begin{array}{c}\vdots\\ T \vdash \langle u, v\rangle\end{array}}{T \vdash v}$$

then $\langle u, v\rangle \in S(T)$.

Lemma 4 *Let P be a simple, flat, D-eager and $\oplus$-eager proof of $T \vdash u$. If P is*

$$(D_K)\frac{(R)\dfrac{\begin{array}{c}\vdots\\ T \vdash \{u\}_K\downarrow = r\end{array}} \quad \dfrac{\begin{array}{c}\vdots\\ T \vdash K\downarrow\end{array}}}{T \vdash u}$$

then $\{u\}_K \in S_\oplus(T)$.

Lemma 5 *Let P be a flat, simple, $\oplus$-eager and D-eager proof of $T \vdash u$. There is a normal proof of $T \vdash u$.*

9 Locality Result

In this section, we prove Theorem 2 which says that a normal proof is equivalent to a $S_\oplus(T, w)$-proof. Thanks to Theorem 1 we conclude that there is a DOUBLE-EXP-TIME procedure complexity (computation of the set $S_\oplus(T, w)$) to decide the intruder deduction problem in equational theory XCDE.

Theorem 2 *Let P be a flat, simple, D-eager and $\oplus$-eager proof of $T \vdash w$ then P is normal $\Leftrightarrow$ P is $S_\oplus(T, w)$-local.*

Proof. $\Leftarrow$ Let us assume that P is $S_\oplus(T, w)$-local and prove that P is normal:

- If $w \in S_\oplus(T)$ then P is $S_\oplus(T)$-local *i.e.* P is normal.
- If $w \notin S_\oplus(T)$ then we proceed by structural induction on P. The base case (A) is trivial, consider the last rule:
  - (UR), (UL), (D) impossible since Lemma 3 and Lemma 4 show that $w \in S_\oplus(T)$ which contradicts the hypothesis.
  - (P), (C), (GX) by induction hypothesis, the hypotheses w_i of the rule stem from normal proofs. Since the last rule is (P), (C),(GX) P is normal.

$\Rightarrow$ Let us assume that P is normal and prove that P is $S_\oplus(T, w)$-local:

- If $w \in S_\oplus(T)$: P is $S_\oplus(T)$-local, hence P is $S_\oplus(T, w)$-local.
- If $w \notin S_\oplus(T)$ we proceed by structural induction on P. The base case is trivial, consider the last rule:
  - (UR), (UL), (D): impossible by definition of normal proof.
  - (P), (C) are similar, we just give the proof for (C). P is s.t. $\dfrac{T \vdash w_1 \quad T \vdash w_2}{T \vdash \{w_1\}_{w_2}}$
    By definition for $i = 1, 2$ $w_i \in S_\oplus(T, w_i)$, $w_i \in S_T(\{w_1\}_{w_2}) = S_T(w) \subseteq S_\oplus(w)$, and induction hypothesis which guarantees that all nodes of the sub-proof are in $S_\oplus(T, w_i)$, we conclude that P is $S_\oplus(T, w)$-local.
  - (GX) P is s.t. $\dfrac{(R_1)\dfrac{T \vdash B_1}{T \vdash B'_1} \quad \ldots \quad (R_n)\dfrac{T \vdash B_n}{T \vdash B'_n}}{T \vdash w}(GX)$. We will prove that all B'_i are in $S_\oplus(T, w)$, consider the different cases for the (R_i):
    - (A): by definition $B'_i \in S_\oplus(T)$,
    - (UR), (UL), (D): by Lemma 3 and Lemma 4 we get $B'_i \in S_\oplus(T)$.
    - (GX): impossible since P is flat.
    - (P): if $B'_i \in S_\oplus(T)$ the claim holds, otherwise $B'_i \notin S_\oplus(T)$. Either B'_i is not canceled in a sum, then $B'_i \in S_T(w) \subseteq S_\oplus(w)$, or otherwise B'_i is canceled by another element of the sum B'_j. Since B'_i is a pair

B'_j can not be deduced from a rule (C) neither a rule (P) since P is simple. Hence it stems from one of the rules (A), (UL), (UR) or (D) and $B'_i \in S_T(B'_j)$. According to Lemma 3 and Lemma 4 $B'_j \in S_\oplus(T)$, hence we get the result by transitivity of $S_\oplus$.

* (C_K): if $B'_i \in S_\oplus(T)$ the claim holds, otherwise $B'_i \notin S_\oplus(T)$. Note that B'_i can be partially canceled in a sum. There are two possibilities for the atoms of B'_i: to be present in w, in which case $\text{atoms}(B'_i) \in \text{atoms}(S_T(w)) \subseteq \text{atoms}(S_\oplus(w))$, or to be canceled by other elements B'_j of the sum, in which case $\text{atoms}(B'_i) \in \text{atoms}(S_\oplus(B'_j)) \subseteq \text{atoms}(S_\oplus(T))$. In the latter case, since B'_i is encrypted by the set of keys K, B'_j can not be the result of a rule $(C_{K'})$ with $K' \neq K$, nor the result of the rule (C'_K) with $K' \cap K \neq \emptyset$ since P is $\oplus$-*eager*, nor (P), hence it stems from one of the rules (A), (UL), (UR) or (D). Thanks to Lemma 3 and Lemma 4 $B'_j \in S_\oplus(T)$, we conclude with the transitivity of $S_\oplus$. In summary, for all i we get that $\text{atoms}(B'_i) \in \text{atoms}(S_\oplus(T, w))$, that is $B'_i \in S_\oplus(T, w))$. Hence P is $S_\oplus(T, w)$-local.□

10 Conclusion

Related works. The result of McAllester of locality was firstly used in the analysis of cryptographic protocols in [14], and later on by [5, 2]. In [11], we studied the case of a homomorphic operator that distributes over some binary operation $\oplus$ which is a free associative-commutative operator, the *exclusive-or* operator, or the addition of an Abelian group. The EXP-TIME result that we obtained for the intruder deduction problem for the theory of *exclusive-or* and a homomorphism has been strengthened in [8] to get a PTIME decision procedure (unfortunately the same method cannot be applied in XCDE case). In [12] we obtain a decision procedure EXP-TIME for the intruder deduction problem with the equational theory of the *exclusive-or* and a non-commutative distributive encryption over this symbol. Our contribution is to get a DOUBLE-EXP-TIME decision procedure in the same theory when the encryption is commutative *i.e.* $\{\{x\}_y\}_z = \{\{x\}_z\}_y$. The commutativity of the encryption requires to consider all combinations of keys in the subterms and to be more attentive in the normalization of proof.

Further work. Now we have a decision procedure for this equational theory, the next stage will be to find the exact complexity of this problem. Analyzing the intruder deduction problem is the first step in the verification of protocols cryptographic, the second step is verifying the case of an active intruder. The active case without equational theory but with a commutative encryption was shown decidable by [3]. Although it seems that the problem is decidable for an active intruder with a homomorphic operation which is not the encryption. In the case of the equational theory of the *exclusive-or* and commutative distributive encryption over this operator, it seems not possible to reduce the problem into equations system as usually.

References

1. F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.
2. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. In *Proc. of 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 261–270, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.
3. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with commuting public key encryption. In *Proc. Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04)*, pages 53–63, Cork (Ireland), 2004.
4. 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 *Lecture Notes in Computer Science*, pages 639–651. Springer, 2005.
5. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. of 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 271–280, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.
6. H. Comon-Lundh and R. Treinen. Easy intruder deductions. In N. Dershowitz, editor, *Verification: Theory & Practice, Essays Dedicated to Zohar Manna on the Occasion of His 64th Birthday*, volume 2772 of *Lecture Notes in Computer Science*, pages 225–242. Springer-Verlag, 2003.
7. V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 2005. To appear.
8. S. Delaune. Easy intruder deduction problems with homomorphisms. Research Report LSV-05-10, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2005. `http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/rr-lsv-2005-10.pdf`.
9. N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B - Formal Models and Semantics, chapter 6, pages 243–320. Elsevier Science Publishers and The MIT Press, 1990.
10. D. Dolev and A. Yao. On the security of public-key protocols. In *Transactions on Information Theory*, volume 29, pages 198–208. IEEE Computer Society Press, March 1983.
11. P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In J. Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 308–322, Nara, Japan, Apr. 2005. Springer-Verlag.
12. P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of exclusive-or with distributive encryption. Research Report LSV-05-19, Laboratoire Spécification et Vérification, ENS Cachan, France, Oct. 2005. 39 pages.
13. D. A. McAllester. Automatic recognition of tractability in inference relations. *J. ACM*, 40(2):284–303, April 1993.
14. M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, pages 174–190, Cape Breton (Canada), 2001. IEEE Comp. Soc. Press.

Appendix A Proofs of Lemmata

Lemma 6 *Let T be a set of terms then $S_T(S_\oplus(T)) = S_\oplus(T)$*

Proof. By definition 5, $S_\oplus(T) \subseteq S_T(S_\oplus(T))$. We prove the converse inclusion by induction on the number of applications of the rule for $\oplus$ in the construction of $S_T(S_\oplus(T))$ (step (ii) in Definition 5). Let $u \in S_T(S_\oplus(T))$, and let n be the number of applications of the rule for $\oplus$. By induction hypothesis, we assume that each term $u' \in S_T(S_\oplus(T))$ obtained with less than n applications of the rule for $\oplus$ is in $S_\oplus(T)$.

Base case $n = 0$: $u \in S_T(v)$ for some $v \in S_\oplus(T)$, where $v = v_1 \oplus \ldots \oplus v_p$ and all $v_i \in S_T(T)$. If $u = v$ then $u \in S_\oplus(T)$. Otherwise $u \neq v$. In this case $u \in S(v_i) \subseteq S_T(v_i)$ for some i (since $v_i \in S_T(T)$ and $S(S_T(T)) = S_T(T)$). Since $v \in S_\oplus(T)$ there exists a $t_i \in T$ such that $v_i \in S_T(t_i)$. Therefore $v_i \in S_T(t_i) \subseteq S_T(T)$ with $t_i \in T$, hence $u \in S_T(S_T(T)) = S_T(T) \subseteq S_\oplus(T)$ by idempotence of S_T.

Induction step: let $u = u_1 \oplus \ldots \oplus u_n$ be obtained from $\{u_1\}_K \oplus \ldots \oplus \{u_n\}_K \in S_T(S_\oplus(T))$. By induction hypothesis $\{u_1\}_K \oplus \ldots \oplus \{u_n\}_K \in S_\oplus(T)$. Hence there exists a partition $I_1 \cup \ldots \cup I_q = \{1, \ldots, n\}$ such that for every j, $1 \leq j \leq q$, $w_j = \oplus_{i \in I_j} \{u_i\}_K \in S_T(t_j)$. Hence, $\oplus_{i \in I_j} u_i \in S_T(t_j)$ by definition of S_T. As a consequence, $u \in S_\oplus(T)$.□

Proposition 4 *Let M be a set of terms then $S_\oplus(S_\oplus(M)) = S_\oplus(M)$. The mappings S, S_T and $S_\oplus$ are transitive.*

Proof. The first point is a consequence of Lemma 6 and Proposition 2. The second is a consequence of the first point and Propositions 1 and 2.□

Lemma 7 *Let P be a simple proof of the form:*

$$P = \left\{ \begin{array}{c} P_1 \ldots P_n \\ \hline T \vdash w \end{array} \right.$$

If $T \vdash u$ does not occur in any of $P_1, \ldots, P_n$ and $\langle u, v \rangle \in S(w)$ then there is at least one P_i and there exists w' such that $\langle u, v \rangle \in S(w')$ and either the root of P_i is $T \vdash w'$ or $w' \in T$.

Proof. We consider all possible rules for the root of P:

- The last rule is (A): obvious since all elements of T are normalized.
- The last rule is (UL) or (UR): $\langle u, v \rangle \in S(w)$ by hypothesis, we denote $w' = \langle u_1, u_2 \rangle$ and by construction $w \in S(\langle u_1, u_2 \rangle)$. We deduce by transitivity of the subterm relation that $\langle u, v \rangle \in S(w')$ and conclude with the induction hypothesis.

– The last rule is (D): $\langle u, v\rangle \in S(w)$ by hypothesis, we denote $w' = \{u_1\}_{u_2}$ and by construction $w \in S(\{u_1\}_{u_2})$. We deduce by transitivity of the subterm relation that $\langle u, v\rangle \in S(w')$ and conclude with the induction hypothesis.
– The last rule is (GX): $\langle u, v\rangle \in S(w)$ by hypothesis and $w = (u_1 \oplus \ldots \oplus u_n)\downarrow$. Hence by definition of the subterm relation $\langle u, v\rangle \in \cup_i S(u_i)$, more precisely there exists i such that $\langle u, v\rangle \in S(u_i)$, because $\langle u, v\rangle$ is not headed with $\oplus$ and conclude with the induction hypothesis.
– The last rule is (P): since $T \vdash u$ can not occur in P we have that $w = \langle w_1, w_2\rangle \neq \langle u, v\rangle$. But $\langle u, v\rangle \in S(w)$ by hypothesis so $\langle u, v\rangle \in S(\langle w_1, w_2\rangle)$. It is a subterm of w_1 or of w_2 and we conclude with the induction hypothesis.
– The last rule is (C): We have that $w = \{w_1\}_{w_2} \neq \langle u, v\rangle$. But $\langle u, v\rangle \in S(w)$ by hypothesis so $\langle u, v\rangle \in S(\{w_1\}_{w_2})$. It is a subterm of w_1 or of w_2 and we conclude with the induction hypothesis. □

Lemma 3 *Let P be a simple proof of $T \vdash u$ or $T \vdash v$. If P is one of*

$$(UL)\dfrac{\dfrac{\vdots}{T \vdash \langle u, v\rangle}}{T \vdash u} \qquad (UR)\dfrac{\dfrac{\vdots}{T \vdash \langle u, v\rangle}}{T \vdash v}$$

then $\langle u, v\rangle \in S(T)$.

Proof. Let us assume that the last rule is (UL), the case (UR) is similar.

$$P = \left\{ \dfrac{\dfrac{P_1 \ldots P_n}{T \vdash \langle u, v\rangle}}{T \vdash u} \right.$$

P is simple so $T \vdash u$ does not occur in any of $P_1, \ldots, P_n$. Hence, we can apply Lemma 7 to $\dfrac{P_1 \ldots P_n}{T \vdash \langle u, v\rangle}$. Either $\langle u, v\rangle \in T$, or there is some P_i with root $T \vdash w$ such that $\langle u, v\rangle \in S(w)$ and $T \vdash u$ does not occur in P_i. Lemma 7 can be applied again and the iteration of this reasoning finally leads to $\langle u, v\rangle \in T$.□

Lemma 4 *Let P be a simple, flat, D-eager and $\oplus$-eager proof of $T \vdash u$. If P is*

$$(D_K)\dfrac{(R)\dfrac{\vdots}{T \vdash \{u\}_K\downarrow = r} \quad \dfrac{\vdots}{T \vdash K\downarrow}}{T \vdash u}$$

then $\{u\}_K \in S_\oplus(T)$.

Proof. The proof is by structural induction on P.

Base case: obvious.

Induction step: we perform a case analysis on the last rule (R) used in the subproof of P with root $\{u\}_v\downarrow$

- (R) is (A), (UL), (UR): the result is true by definition (rule (A)) or Lemma 3 (rule (UL), (UR)).
- (R) is some rule (P): this cannot happen since $\{u\}_K\downarrow$ is not a pair.
- (R) is some rule $(C_{K'})$: P is *D-eager* by consequence it is impossible.
- (R) is some rule $(D_{K'})$ impossible since P is flat.
- (R) is (GX). The last deductions in the proof P are described in Figure 5 and we discuss the different cases according to the rules (R_i) and the structure of $\{u\}_K\downarrow$.

$$(D_K)\dfrac{(GX)\dfrac{(R_1)\dfrac{T\vdash B_1}{T\vdash B_1'}\quad ...\quad (R_n)\dfrac{T\vdash B_n}{T\vdash B_n'}}{T\vdash \{u\}_K\downarrow}\qquad \dfrac{\vdots}{T\vdash K\downarrow}}{T\vdash u\downarrow}$$

Fig. 5. Illustration of the case (D_K) in Lemma 4

We will show that every atom of $\{u\}_K\downarrow$ is in fact an element of $S_T(T)$. Let $a\in \text{atoms}(\{u\}_K\downarrow)$. Note that a is necessarily of the form $\{a'\}_K$, and that there is an i such that $a\in\text{atoms}(B_i')$. We consider different possible cases for the rule (R_i):

- (R_i) is (A) (UL) or (UR). By definition or Lemma 3, $B_i'\in S_\oplus(T)$.
- (R_i) is $(D_{K'})$ s.t. $(D_{K'})\ \dfrac{T\vdash \{w_1\}_{K'}\ T\vdash K'}{T\vdash w_1=B_i'}$ By induction hypothesis $\{w_1\}_{K'}\in S_\oplus(T)$, therefore $w_1=B_i'\in S_\oplus(T)$.
- (R_i) is (P): $B_i'=\langle w_1,w_2\rangle$, B_i' cannot occur in $\{u\}_K\downarrow$ by consequence B_i' is canceled by another hypotheses B_j' of (GX) such that $B_i'\in S_T(B_j')$. B_j' can not be the result of a rule (P) by simplicity, neither a rule (C) since it is a pair, neither (GX) since the proof is flat. In the other cases B_j' stems from a rule (A), (UL), (UR) or (D) by consequence $B_j'\in S_\oplus(T)$. We deduce that $B_i'\in S_\oplus(T)$.
- (R_i) is (C), since P is *D-eager* we get that B_i' is headed with $\{.\}_{K'}$ such that $K\cap K'=\emptyset$. By consequence B_i' is canceled by another hypotheses B_j' of (GX) such that $B_j'\in S_T(B_i')$. B_j' can not be the result of a rule (P) since it is an encrypted term, neither another rule (C) since P is $\oplus$-*eager*, neither (GX) since the proof is flat. In the other cases the copy B_j' stems from a rule (A), (UL), (UR) or (D) by consequence $B_j'\in S_\oplus(T)$. We deduce that $B_i'\in S_\oplus(T)$.

Therefore in all cases $\{u\}_K\downarrow=\bigoplus_{i=1,\dots,n}B_i'\downarrow=\bigoplus\{t_i\}_K$ where $\{t_i\}_K\in S_\oplus(T)\cap(\cup_{i=1,\dots,n}\text{atoms}(B_i))$ since all atoms of B_i' are in $S_\oplus(T)$ or canceled.□

Lemma 5 *Let P be a flat, simple, $\oplus$-eager and D-eager proof of $T \vdash u$. There is a normal proof of $T \vdash u$.*

Proof. Consider first the case where $u \in S_\oplus(T)$. We proceed by structural induction on the proof P and case distinction of the last rule (R) of P:

- (R) is (A): P is obviously a normal proof.
- (R) is some rule (UL) or (UR) s.t. $\dfrac{T \vdash \langle u_1, u_2\rangle}{T \vdash u}$ The induction hypothesis gives that there exists a normal proof of $\langle u_1, u_2\rangle$. P is simple, we apply Lemma 3 and get $\langle u_1, u_2\rangle \in S(T) \subseteq S_\oplus(T)$ then the normal proof of $\langle u_1, u_2\rangle$ is $S_\oplus(T)$-local so P is normal since $u \in S_\oplus(T)$.
- (R) is some rule (D) s.t. $\dfrac{T \vdash \{u\}_K \quad T \vdash K}{T \vdash u}$ The induction hypothesis gives that there exists a normal proof of $\{u\}_K$. P is flat, simple, *D-eager* and *$\oplus$-eager* with Lemma 4 we get $\{u\}_K \in S(T) \subseteq S_\oplus(T)$ and then the normal proof of $\{u\}_K$ is $S_\oplus(T)$-local so we deduce that P is normal since $u \in S_\oplus(T)$.
- (R) is some rule (P), (C) are similar. We only give the proof for $u = \{u_1\}_{u_2}$. (R) is some (C) s.t. $\dfrac{T \vdash u_1 \quad T \vdash u_2}{T \vdash \{u_1\}_{u_2}}$ Since $\{u_1\}_{u_2} = u \in S_\oplus(T)$ we deduce that $u_1 \in S_\oplus(T)$ and $u_2 \in S_\oplus(T)$. Hence applying the induction hypothesis there are normal proofs of u_1 and u_2 that are $S_\oplus$-local, hence P is normal.
- (R) is some rule (GX) s.t. $(GX)\dfrac{(R_1)\dfrac{T \vdash B_1}{T \vdash B'_1} \qquad ...(R_n)\dfrac{T \vdash B_n}{T \vdash B'_n}}{T \vdash u}$ We will show that for every (R_i) we have that $B'_i \in S_\oplus(T)$. We discuss the different cases for the rules (R_i)'s:
  - (R_i) is not (GX) since P is flat.
  - (R_i) is (A), (UL), (UR) or (D) with the definition or Lemma 3 or Lemma 4 then $B'_i \in S_\oplus(T)$. Applying the induction hypothesis there is a normal proof of B'_i which is $S_\oplus(T)$-local.
  - (R_i) is (P), there are two possibilities: B'_i is in $S_T(u)$ or not.
    - $B'_i \in S_T(u) \subseteq S_\oplus(T)$ we can apply the induction hypothesis and get a normal proof of B'_i which is $S_\oplus(T)$-local.
    - $B'_i \notin S_T(u)$ hence B'_i is canceled by some other elements B'_j. B'_j can not come from a rule (P) since P is simple, from a rule (C) since a pair is not headed with $\{.\}_.$. So B'_j come from a rule (A), (UL), (UR) or (D) with the definition or Lemma 3 or Lemma 4 then $B'_j \in S_\oplus(T)$. More precisely $\bigoplus B'_j \in S_\oplus(T)$, since $B'_i \in S_\oplus(\bigoplus B'_j)$ we deduce that $B'_i \in S_\oplus(T)$. we can apply the induction hypothesis and get a normal proof of B'_i which is $S_\oplus(T)$-local.
  - (R_i) is (C_K), this case is similar to the previous case. There are two possibilities: B'_i is in $S_T(u)$ or not:

* $B'_i \in S_T(u) \subseteq S_\oplus(T)$ we can apply the induction hypothesis and get a normal proof of B'_i which is $S_\oplus(T)$-local.
* $B'_i \notin S_T(u)$ hence B'_i is canceled by some other elements B'_j. B'_j can not stem from a rule (P) since a pair is not headed with $\{.\}_.$, from a rule $(C_{K'})$ with $K' \neq K$ since B'_i not headed with $\{.\}_K$ and not from another rule $(C_{K'})$ where $K' \cap K \neq \emptyset$ since P is $\oplus$-*eager*. So B'_j come from a rule (A), (UL), (UR) or (D) with the definition or Lemma 3 or Lemma 4 then $B'_j \in S_\oplus(T)$. More precisely $\bigoplus B'_j \in S_\oplus(T)$, since $B'_i \in S_\oplus(\bigoplus B'_j)$ we deduce that $B'_i \in S_\oplus(T)$. we can apply the induction hypothesis and get a normal proof of B'_i which is $S_\oplus(T)$-local.

Since all the subproofs of $T \vdash B'_i$ are normal we can conclude that P is normal.

In the second case, we assume that $u \notin S_\oplus(T)$ and the proof is of the form $C[P_1, \ldots, P_n]$ where $P_1, \ldots, P_n$ are maximal $S_\oplus$-local subproofs. We prove the result by structural induction on P:

- If C is empty, then $u \in S_\oplus(T)$
- If the last rule is (UL) (UR) or (D) we use the definition and Lemma 3 and Lemma 4 to get $u \in S_\oplus(T)$.
- In the others cases we apply the induction hypothesis.□