

Computationally sound implementations of equational theories against passive adversaries

Mathieu Baudet¹, Véronique Cortier², and Steve Kremer¹

¹ LSV/ CNRS UMR 8643 & INRIA Futurs projet SECSI & ENS Cachan, France
{baudet, kremer}@lsv.ens-cachan.fr

² Loria/CNRS UMR 7503 & INRIA Lorraine projet Cassis, France
cortier@loria.fr

Abstract. In this paper we study the link between formal and cryptographic models for security protocols in the presence of a passive adversary. In contrast to other works, we do not consider a fixed set of primitives but aim at results for an arbitrary equational theory. We define a framework for comparing a cryptographic implementation and its idealization *w.r.t.* various security notions. In particular, we concentrate on the computational soundness of static equivalence, a standard tool in cryptographic pi calculi. We present a soundness criterion, which for many theories is not only sufficient but also necessary. Finally, we establish new soundness results for the exclusive OR and a theory of ciphers and lists.

1 Introduction

Today's ubiquity of computer networks increases the need for theoretic foundations for cryptographic protocols. For more than twenty years now, two communities separately developed two families of models. Both views have been very useful in increasing the understanding and quality of security protocol design. On the one hand *formal* or *logical* models have been developed, based on the seminal work of Dolev and Yao [9]. These models view cryptographic operations in a rather abstract and idealized way. On the other hand *cryptographic* or *computational* models [10] are closer to implementations: cryptographic operations are modeled as algorithms manipulating bit-strings. Those models cover a large class of attacks, namely all those implementable by a probabilistic polynomial-time Turing machine.

The advantage of formal models is that security proofs are generally simpler and suitable for automatic procedures, even for complex protocols. Unfortunately, the high degree of abstraction and the limited adversary power raise serious questions regarding the security offered by such proofs. Potentially, justifying symbolic proofs with respect to standard computational models has tremendous benefits: protocols can be analyzed using automated tools and still benefit from the security guarantees of the computational model.

Recently, a significant research effort has been directed at linking these two approaches. In their seminal work [3], Abadi and Rogaway prove the computational soundness of formal (symmetric) encryption in the case a passive attacker. Since then, many results [5, 11, 12] have been obtained. Notably, Backes *et al.* [5] prove the soundness of

a rich language including digital signatures, public-key and symmetric key encryption in the presence of an active attacker. Laud [11] presents an automated procedure for computationally sound proofs of confidentiality in the case of an active attacker and symmetric encryption when the number of sessions is bounded.

Each of these results considers a fixed set of primitives, *e.g.* symmetric or public-key encryption. In this paper, we aim at presenting general results for arbitrary equational theories, such as encryption, but also less studied ones, *e.g.* groups or exclusive OR. We concentrate on *static equivalence*, a now standard notion originating from the applied pi calculus [2]. Intuitively, static equivalence asks whether an attacker can distinguish between two tuples of terms, by exhibiting an equation which holds on one tuple but not on the other. This provides an elegant means to express security properties against passive attackers. Moreover there exist exact [1] and approximate [8] algorithms to decide static equivalence for a large family of equational theories.

Our first contribution is a general framework for comparing formal and computational models in the presence of a passive attacker. We define the notions of *soundness* and *faithfulness* of a cryptographic implementation *w.r.t.* equality, static equivalence and deducibility. Soundness holds when each formal proof has a computational interpretation. Faithfulness is the converse, *i.e.* the formal model does not provide false attacks.

Our second contribution is a sufficient criterion for soundness *w.r.t.* static equivalence: intuitively the usual computational semantics of terms has to be indistinguishable to an idealized one. We also provide a general definition of patterns for arbitrary equational theories that encompasses the notion usually defined for symmetric and public encryption. Those patterns allow us to characterize a large class of theories for which our soundness criterion is necessary.

Our third contribution consists in applying our framework to obtain two novel soundness results. The first theory deals with the exclusive OR. Interestingly, our proof reflects the unconditional security (in the information-theoretic sense) of the One-Time Pad encryption scheme. Second we consider a theory of symmetric encryption and lists. In some sense, the result is similar to the one of Abadi and Rogaway [3]. However, we consider deterministic, length-preserving, symmetric encryption schemes *a.k.a.* ciphers. To the best of our knowledge, this is the first result on such schemes, whose specificity is that decryption always succeeds.

Outline of the paper. In the next section, we introduce our abstract and concrete models together with the notions of indistinguishability. We then define the notions of soundness and faithfulness and illustrate some consequences of soundness *w.r.t.* static equivalence on groups. In Section 4, we define the ideal semantics of abstract terms, present our soundness criterion and also show that for a large family of interesting equational theories, the soundness criterion is a necessary condition. As an illustration (Section 5), we prove the soundness for the theories modeling exclusive OR, as well as ciphers and lists. We then conclude and give directions for future work. Note that, due to lack of space most proofs have been omitted; those can be found in the extended version [7].

2 Modeling cryptographic primitives with abstract algebras

In this section we introduce some notations and set our abstract and concrete models.

2.1 Abstract algebras

Our abstract models—which we call *abstract algebras*—consist of term algebras defined on a first-order signature with sorts and equipped with equational theories.

Specifically a *signature* $(\mathcal{S}, \mathcal{F})$ is made of a set of *sorts* $\mathcal{S} = \{s, s_1 \dots\}$ and a set of *symbols* $\mathcal{F} = \{f, f_1 \dots\}$ together with arities of the form $\text{ar}(f) = s_1 \times \dots \times s_k \rightarrow s$, $k \geq 0$. Symbols that take $k = 0$ arguments are called *constants*; their arity is simply written s . We fix an infinite set of *names* $\mathcal{N} = \{a, b \dots\}$ and an infinite set of *variables* $\mathcal{X} = \{x, y \dots\}$. We assume that names and variables are given with sorts. The set of *terms of sort* s is defined inductively by

$$\begin{array}{l}
 T ::= \quad \text{term of sort } s \\
 \quad | \quad x \quad \text{variable } x \text{ of sort } s \\
 \quad | \quad a \quad \text{name } a \text{ of sort } s \\
 \quad | \quad f(T_1, \dots, T_k) \text{ application of symbol } f \in \mathcal{F}
 \end{array}$$

where for the last case, we further require that T_i is a term of some sort s_i and $\text{ar}(f) = s_1 \times \dots \times s_k \rightarrow s$. As usual, we write $\text{var}(T)$ and $\text{names}(T)$ for the set of variables and names occurring in T respectively. A term is *ground* or *closed* iff it has no variables.

Substitutions are written $\sigma = \{x_1 = T_1, \dots, x_n = T_n\}$ with domain $\text{dom}(\sigma) = \{x_1, \dots, x_n\}$. We only consider *well-sorted* substitutions, that is, substitutions $\sigma = \{x_1 = T_1, \dots, x_n = T_n\}$ for which x_i and T_i have the same sort. σ is *closed* iff all of the T_i are closed. We extend the notation $\text{names}(\cdot)$ from terms to substitutions in the obvious way. The application of a substitution σ to a term T is written $\sigma(T) = T\sigma$.

Symbols in \mathcal{F} are intended to model cryptographic primitives, whereas names in \mathcal{N} are used to model nonces *i.e.* concretely random numbers. The abstract semantics of symbols is described by an equational theory E , that is an equivalence relation (also written $=_E$) which is stable by application of contexts and well-sorted substitutions of variables. We further require that E is stable under substitution of names. All the equational theories that we consider in this paper satisfy these properties. For instance, symmetric and deterministic encryption is modeled by the theory E_{enc} generated by the classical equation $E_{\text{enc}} = \{\text{dec}(\text{enc}(x, y), y) = x\}$.

2.2 Frames, deducibility and static equivalence

Following [2, 1], a *frame* is an expression $\varphi = \nu \tilde{a} . \sigma$ where \tilde{a} is a set of *bound* (or *restricted*) names and σ is a well-sorted substitution. Intuitively, frames represent sequences of messages learned by an attacker during the execution of a protocol.

For simplicity we only consider frames $\nu \tilde{a} . \sigma$ which restrict *every* name occurring in σ , that is $\tilde{a} = \text{names}(\sigma)$. In other words, names a must be disclosed *explicitly* by adding a mapping $x_a = a$ to the substitution. Thus we tend to assimilate frames and their underlying substitutions.

A term T is *deducible* from a closed frame φ , written $\varphi \vdash_E T$ iff there exists a term M with $\text{var}(M) \subseteq \text{dom}(\varphi)$ and $\text{names}(M) \cap \text{names}(\varphi) = \emptyset$ such that $M\varphi =_E T$. Consider for instance the theory E_{enc} and the frame $\varphi_1 = \nu k_1, k_2, k_3, k_4 . \{x_1 = \text{enc}(k_1, k_2), x_2 = \text{enc}(k_4, k_3), x_3 = k_3\}$: the name k_4 is deducible from φ_1 since $\text{dec}(x_2, x_3)\varphi_1 =_{E_{\text{enc}}} k_4$ but neither k_1 nor k_2 are deducible.

Deducibility is not always sufficient to account for the knowledge of an attacker. *E.g.* it lacks partial information on secrets. This is why the notion of static equivalence is used. Two closed frames φ_1 and φ_2 are *statically equivalent*, written $\varphi_1 \approx_E \varphi_2$, iff (i) $\text{dom}(\varphi_1) = \text{dom}(\varphi_2)$, (ii) for all terms M, N with variables included in $\text{dom}(\varphi_i)$ and using no names occurring in φ_1 or φ_2 , $M\varphi_1 =_E N\varphi_1$ is equivalent to $M\varphi_2 =_E N\varphi_2$.

For instance, the two frames $\nu k. \{x = \text{enc}(0, k)\}$ and $\nu k. \{x = \text{enc}(1, k)\}$ are statically equivalent with respect to E_{enc} , whereas the two frames $\nu k. \{x = \text{enc}(0, k), y = k\}$ and $\nu k, k'. \{x = \text{enc}(0, k'), y = k\}$ are not.

2.3 Concrete semantics

We now give terms and frames a concrete semantics, parameterized by an implementation of the primitives. Provided a set of sorts \mathcal{S} and a set of symbols \mathcal{F} as above, a $(\mathcal{S}, \mathcal{F})$ -computational algebra A consists of

- a non-empty set of bit-strings $\llbracket s \rrbracket_A \subseteq \{0, 1\}^*$ for each sort $s \in \mathcal{S}$;
- a computable function $f_A : \llbracket s_1 \rrbracket_A \times \dots \times \llbracket s_k \rrbracket_A \rightarrow \llbracket s \rrbracket_A$ for each $f \in \mathcal{F}$ with $\text{ar}(f) = s_1 \times \dots \times s_k \rightarrow s$;
- a computable congruence $=_{A,s}$ for each sort s , in order to check the equality of elements in $\llbracket s \rrbracket_A$ (the same element may be represented by different bit-strings); by congruence, we mean a reflexive, symmetric, transitive relation such that $e_1 =_{A,s_1} e'_1, \dots, e_k =_{A,s_k} e'_k \Rightarrow f_A(e_1, \dots, e_k) =_{A,s} f_A(e'_1, \dots, e'_k)$ (in the remaining we often omit s and write $=_A$ for $=_{A,s}$);
- an effective procedure to draw random elements from $\llbracket s \rrbracket_A$; we denote such a drawing by $x \stackrel{R}{\leftarrow} \llbracket s \rrbracket_A$; the drawing may not follow a uniform distribution, but no $=_{A,s}$ -equivalence class should have probability 0.

Assume a fixed $(\mathcal{S}, \mathcal{F})$ -computational algebra A . We associate to each closed frame $\varphi = \{x_1 = T_1, \dots, x_n = T_n\}$ a distribution $\psi = \llbracket \varphi \rrbracket_A$, of which the drawings $\hat{\psi} \stackrel{R}{\leftarrow} \psi$ are computed as follows:

1. for each name a of sort s appearing in T_1, \dots, T_n , draw a value $\hat{a} \stackrel{R}{\leftarrow} \llbracket s \rrbracket_A$;
2. for each x_i ($1 \leq i \leq n$) of sort s_i , compute $\hat{T}_i \in \llbracket s_i \rrbracket_A$ recursively on the structure of terms: $f(\widehat{T_1}, \dots, \widehat{T_m}) = f_A(\widehat{T_1}, \dots, \widehat{T_m})$;
3. return the value $\hat{\psi} = \{x_1 = \hat{T}_1, \dots, x_n = \hat{T}_n\}$.

Such values $\phi = \{x_1 = e_1, \dots, x_n = e_n\}$ with $e_i \in \llbracket s_i \rrbracket_A$ are called *concrete frames*. We extend the notation $\llbracket \cdot \rrbracket_A$ to (sets of) closed terms in the obvious way. We also generalize the notation to terms or frames with variables, by specifying the concrete values for all of them: $\llbracket \cdot \rrbracket_{A, \{x_1=e_1, \dots, x_n=e_n\}}$. Notice that when a term or a frame contains no names, the translation is deterministic; in this case, we use the same notation to denote the distribution and its unique value.

(Families of) distributions over concrete frames benefit from the usual notion of cryptographic indistinguishability. Let us note $\eta \geq 0$ the complexity parameter. Intuitively, two families (ψ_η) and (ψ'_η) of distributions over concrete frames are *indistinguishable*, written $(\psi_\eta) \approx (\psi'_\eta)$, iff no probabilistic polynomial-time adversary \mathcal{A}

can guess whether he is given a sample from ψ_η or ψ'_η with a probability significantly greater than $\frac{1}{2}$. Rigorously, we ask the *advantage* of \mathcal{A} ,

$$\text{Adv}^{\text{IND}}(\mathcal{A}, \eta, \psi_\eta, \psi'_\eta) = \mathbb{P}[\widehat{\psi} \stackrel{R}{\leftarrow} \psi_\eta; \mathcal{A}(\eta, \widehat{\psi}) = 1] - \mathbb{P}[\widehat{\psi} \stackrel{R}{\leftarrow} \psi'_\eta; \mathcal{A}(\eta, \widehat{\psi}) = 1]$$

to be a *negligible* function of η , that is, to remain eventually smaller than any η^{-n} ($n > 0$) for sufficiently large η .

3 Relating abstract and computational algebras

In the previous section we have defined abstract and computational algebras. We now relate formal notions such as equality, (non-)deducibility and static equivalence to their computational counterparts, *i.e.* equality, one-wayness and indistinguishability.

3.1 Soundness and faithfulness

We introduce the notions of sound, *resp.* faithful, computational algebras with respect to the formal relations studied here: equality, static equivalence and deducibility. In the remaining of the paper we only consider families of computational algebras (A_η) such that each required operation on algebras is feasible by a (uniform) polynomial-time algorithm in the complexity parameter η . We also require that for every sort s , either there exists no name of sort s , or the probability of collision of two random elements in $\llbracket s \rrbracket_{A_\eta}$, $\mathbb{P}[e_1, e_2 \stackrel{R}{\leftarrow} \llbracket s \rrbracket_{A_\eta}; e_1 =_{A_\eta} e_2]$, is negligible.

Specifically a family of computational algebras (A_η) is

- $=_E$ -*sound* iff for every closed terms T_1, T_2 of the same sort, $T_1 =_E T_2$ implies that $\mathbb{P}[e_1, e_2 \stackrel{R}{\leftarrow} \llbracket T_1, T_2 \rrbracket_{A_\eta}; e_1 \neq_{A_\eta} e_2]$ is negligible;
- $=_E$ -*faithful* iff for every closed terms T_1, T_2 of the same sort, $T_1 \neq_E T_2$ implies that $\mathbb{P}[e_1, e_2 \stackrel{R}{\leftarrow} \llbracket T_1, T_2 \rrbracket_{A_\eta}; e_1 =_{A_\eta} e_2]$ is negligible;
- \approx_E -*sound* iff for every closed frames φ_1, φ_2 with the same domain, $\varphi_1 \approx_E \varphi_2$ implies that $(\llbracket \varphi_1 \rrbracket_{A_\eta}) \approx (\llbracket \varphi_2 \rrbracket_{A_\eta})$;
- \approx_E -*faithful* iff for every closed frames φ_1, φ_2 of the same domain, $\varphi_1 \not\approx_E \varphi_2$ implies that there exists a polynomial-time adversary \mathcal{A} for distinguishing concrete frames, such that $1 - \text{Adv}^{\text{IND}}(\mathcal{A}, \eta, \llbracket \varphi_1 \rrbracket_{A_\eta}, \llbracket \varphi_2 \rrbracket_{A_\eta})$ is negligible;
- $\not\vdash_E$ -*sound* iff for every closed φ and T , $\varphi \not\vdash_E T$ implies that for each polynomial-time adversary \mathcal{A} , $\mathbb{P}[\phi, e \stackrel{R}{\leftarrow} \llbracket \varphi, T \rrbracket_{A_\eta}; \mathcal{A}(\phi) =_{A_\eta} e]$ is negligible;
- $\not\vdash_E$ -*faithful* iff for every closed φ and T , $\varphi \vdash_E T$ implies that there exists a polynomial-time adversary \mathcal{A} such that $1 - \mathbb{P}[\phi, e \stackrel{R}{\leftarrow} \llbracket \varphi, T \rrbracket_{A_\eta}; \mathcal{A}(\phi) =_{A_\eta} e]$ is negligible.

Sometimes, it is possible to prove stronger notions of soundness that hold without restriction on the computational power of adversaries. In particular, (A_η) is *unconditionally* $=_E$ -*sound* iff for every closed terms T_1, T_2 of the same sort, $T_1 =_E T_2$ implies that $\mathbb{P}[e_1, e_2 \stackrel{R}{\leftarrow} \llbracket T_1, T_2 \rrbracket_{A_\eta}; e_1 =_{A_\eta} e_2] = 1$; *unconditionally* \approx_E -*sound* iff for every

closed frames φ_1, φ_2 with the same domain, $\varphi_1 \approx_E \varphi_2$ implies $(\llbracket \varphi_1 \rrbracket_{A_\eta}) = (\llbracket \varphi_2 \rrbracket_{A_\eta})$; *unconditionally* $\not\vdash_E$ -sound iff for every closed φ and T s.t. $\varphi \not\vdash_E T$, the distributions for φ and T are independent: for all ϕ_0, e_0 , $\mathbb{P}[\phi, e \stackrel{R}{\leftarrow} \llbracket \varphi, T \rrbracket_{A_\eta}; \phi = \phi_0 \text{ and } e = e_0] = \mathbb{P}[\phi \stackrel{R}{\leftarrow} \llbracket \varphi \rrbracket_{A_\eta}; \phi = \phi_0] \times \mathbb{P}[e \stackrel{R}{\leftarrow} \llbracket T \rrbracket_{A_\eta}; e = e_0]$.

Generally, (unconditional) $=_E$ -soundness is given by construction. Indeed true formal equations correspond to the expected behavior of primitives and should hold in the concrete world with overwhelming probability. The other criteria are however more difficult to fulfill. Therefore it is often interesting to restrict frames to *well-formed* ones in order to achieve soundness or faithfulness: for instance Abadi and Rogaway [3] do forbid encryption cycles (c.f. Section 5.2).

It is worth noting that the notions introduced above are not independent.

Proposition 1. *Let (A_η) be a $=_E$ -sound family of computational algebras. Then (A_η) is $\not\vdash_E$ -faithful. If moreover (A_η) is $=_E$ -faithful, then it is also \approx_E -faithful.*

For many interesting theories, we have that \approx_E -soundness implies all the other notions of soundness and faithfulness. As an illustration, let us consider an arbitrary theory which includes keyed hash functions.

Proposition 2. *Let (A_η) be a family of \approx_E -sound computational algebras. Assume that free binary symbols $h_s : s \times \text{Key} \rightarrow \text{Hash}$ are available for every sort s , and the sorts *Hash* and *Key* have infinitely many names. Then (A_η) is $=_E$ -faithful and $\not\vdash_E$ -sound. Besides, if the implementations for the h_s are collision-resistant, then (A_η) is $=_E$ -sound, \approx_E -faithful and $\not\vdash_E$ -faithful.*

3.2 \approx_E -soundness implies classical assumptions on groups

Inspired by the work of Rivest on pseudo-freeness [14], we now study some consequences of \approx_E -soundness on *groups*. Let E_G be the equational theory modeling a free group G with exponents taken over a free commutative ring A . Assume a \approx_{E_G} -sound family of computational algebras (A_η) . Then the static equivalence $\nu g, a, b. \{x_1 = g, x_2 = g^a, x_3 = g^b, x_4 = g^{a \cdot b}\} \approx_{E_G} \nu g, a, b, c. \{x_1 = g, x_2 = g^a, x_3 = g^b, x_4 = g^c\}$ implies the hardness of the decisional Diffie-Hellman problem for this implementation.

In a similar way we prove that \approx_{E_G} -soundness implies the hardness of RSA. More details can be found in [7].

4 A sufficient (and often necessary) criterion for \approx_E -soundness

We now present useful results for proving \approx_E -soundness properties in general. Notably, we provide a sufficient criterion for \approx_E -soundness in Section 4.1 and prove it necessary under additional assumptions in Section 4.2.

4.1 Ideal semantics and \approx_E -soundness criterion

Given an implementation of the primitives, what we called the concrete semantics maps every closed frame φ to a distribution $\llbracket \varphi \rrbracket_{A_\eta}$ in the expected way. We now define the

ideal semantics of a φ , intuitively as the uniform distribution over sequences of bit-strings (in the appropriate space) that pass all the formal tests verified by φ .

Given a closed frame φ , let us write $\text{eq}_E(\varphi)$ for the set of tests that are true in φ : $\text{eq}_E(\varphi) = \{(M, N) \mid \text{var}(M) \cup \text{var}(N) \subseteq \text{dom}(\varphi), (\text{names}(M) \cup \text{names}(N)) \cap \text{names}(\varphi) = \emptyset \text{ and } M\varphi =_E N\varphi\}$. Notice that $\varphi \approx_E \varphi'$ iff $\text{eq}_E(\varphi) = \text{eq}_E(\varphi')$.

We say that (A_η) *has uniform distributions* iff for every η and every sort s , $\llbracket s \rrbracket_{A_\eta}$ is a finite set, $=_{A_\eta, s}$ is the usual equality and, the distribution associated to s by A_η is the uniform one over $\llbracket s \rrbracket_{A_\eta}$.

Definition 1 (Ideal semantics). *Let (A_η) be an unconditionally $=_E$ -sound family of computational algebras, having uniform distributions. Let $\varphi = \{x_1 = t_1, \dots, x_n = t_n\}$ be a closed frame and s_i the sort of x_i . The ideal semantics $\llbracket \varphi \rrbracket_{A_\eta}^{\text{ideal}}$ of φ is the uniform distribution over the finite (non-empty) set of concrete frames:*

$$\left\{ \{x_1 = e_1, \dots, x_n = e_n\} \mid (e_1, \dots, e_n) \in \llbracket s_1 \rrbracket_{A_\eta} \times \dots \times \llbracket s_n \rrbracket_{A_\eta} \text{ and} \right. \\ \left. \forall (M, N) \in \text{eq}_E(\varphi) \cdot \llbracket M \rrbracket_{A_\eta, \{x_1=e_1, \dots, x_n=e_n\}} = \llbracket N \rrbracket_{A_\eta, \{x_1=e_1, \dots, x_n=e_n\}} \right\}$$

For instance, let $\varphi = \nu n_1, n_2. \{x_1 = n_1, x_2 = n_2\}$ with n_1 and n_2 of sort s . Then $\text{eq}_E(\varphi) \subseteq \{(M, N) \mid M =_E N\}$ implies that $\llbracket \varphi \rrbracket_{A_\eta}^{\text{ideal}}$ is simply the uniform distribution over $\llbracket s \rrbracket_{A_\eta} \times \llbracket s \rrbracket_{A_\eta}$. A more general definition of the ideal semantics, which does not restrict (A_η) to uniform distributions is given in [7].

We can now state our \approx_E -soundness criterion: intuitively, the two semantics, concrete and ideal, should be indistinguishable.

Theorem 1 (\approx_E -soundness criterion). *Let (A_η) be an unconditionally $=_E$ -sound family of computational algebras. Assume that for every closed frame φ it holds that $(\llbracket \varphi \rrbracket_{A_\eta}) \approx (\llbracket \varphi \rrbracket_{A_\eta}^{\text{ideal}})$. Then (A_η) is \approx_E -sound.*

4.2 Patterns revisited

Patterns have been introduced by Abadi and Rogaway [3] and used in subsequent work [12, 6] as a way to define computationally sound formal equivalences. Typically frames are mapped to patterns by replacing non-decipherable terms by boxes \square . Two frames are then equivalent iff they yield the same pattern (up to renaming of names). For example, the pattern associated to the frame $\varphi_1 = \{x_1 = \text{enc}(\text{enc}(k_4, k_3), k_1), x_2 = \text{enc}(k_1, k_2), x_3 = k_2\}$ is $\{x_1 = \text{enc}(\square, k_1), x_2 = \text{enc}(k_1, k_2), x_3 = k_2\}$.

In this section we propose a general, novel definition of patterns and study some of their properties. We then use these properties to prove that our soundness criterion is necessary in many cases.

Definition 2. *A closed frame φ is a pattern if each of its subterms is deducible from φ .*

Equivalently a pattern is a closed frame of the form $\varphi = \{x_1 = C_1[a_1, \dots, a_m], \dots, x_n = C_n[a_1, \dots, a_m]\}$ where the $C_1 \dots C_n$ are closed (not necessarily linear) contexts and the $a_1 \dots a_m$ are distinct deducible names: $\varphi \vdash_E a_i$. For example, φ_1 as defined above is not a pattern, while $\varphi_2 = \{x_1 = \text{enc}(n_1, k_1), x_2 = \text{enc}(k_1, k_2), x_3 = k_2\}$ is.

The following proposition finitely characterizes the equations verified by a pattern.

Proposition 3. *Let $\varphi = \{x_1 = C_1[a_1, \dots, a_m], \dots, x_n = C_n[a_1, \dots, a_m]\}$ be a pattern, using the notations above. For each a_i , let ζ_{a_i} be a term such that $\text{var}(\zeta_{a_i}) \subseteq \{x_1, \dots, x_n\}$, $\text{names}(\zeta_{a_i}) \cap \text{names}(\varphi) = \emptyset$ and $\zeta_{a_i}\varphi =_E a_i$. Then every equation which holds in φ is a logical consequence (in the first-order theory of equality) of E and the equations $x_j = C_j[\zeta_{a_1}, \dots, \zeta_{a_m}]$.*

Interestingly the concrete and the ideal semantics of patterns often coincide.

Proposition 4. *Let (A_η) be an unconditionally $=_E$ -sound family of computational algebras, having uniform distributions. Let φ be a pattern. The concrete and the ideal semantics of φ yield the same family of distributions: for all η , $\llbracket \varphi \rrbracket_{A_\eta} = \llbracket \varphi \rrbracket_{A_\eta}^{\text{ideal}}$.*

The idea of the proof is that, using the finite characterization of $\text{eq}_E(\varphi)$ (Proposition 3), one can draw a bijection between the drawing of nonces and the eligible values for the ideal semantics.

A theory E admits patterns iff for every closed frame φ , there exists a (not necessarily unique) pattern $\overline{\varphi}$ such that $\varphi \approx_E \overline{\varphi}$. In practice many theories useful in cryptography satisfy this property, *e.g.* the theories considered in Section 5. Note that we have proved *en passant* that \approx_E is decidable for equational theories that admit patterns and for which $=_E$ is decidable, provided the construction of patterns is effective. Indeed, given two frames φ_1 and φ_2 , we associate to each of them one of its statically equivalent pattern $\overline{\varphi}_1$ and $\overline{\varphi}_2$, respectively. It is then straightforward to check whether $\overline{\varphi}_1$ and $\overline{\varphi}_2$ are equivalent using the finite characterization of $\text{eq}_E(\overline{\varphi}_i)$ by Proposition 3.

The following theorem states that our soundness criterion is actually very tight: whenever a theory admits patterns, our criterion is a necessary condition.

Theorem 2. *Assume that the theory E admits patterns. Let (A_η) be a family of computational algebras, such that (A_η) has uniform distributions, is \approx_E - and unconditionally $=_E$ -sound. Then the soundness criterion of Theorem 1 is satisfied: for every closed frame φ , $(\llbracket \varphi \rrbracket_{A_\eta}) \approx (\llbracket \varphi \rrbracket_{A_\eta}^{\text{ideal}})$.*

5 Examples

We now apply the framework of Sections 3 and 4 to establish two novel \approx_E -soundness results, concerning the theory of exclusive OR and that of ciphers and lists.

5.1 Exclusive OR

We study the soundness and faithfulness problems for the usual theory and implementation of the exclusive OR (XOR).

The formal model consists of a single sort $Data$, an infinite number of names, the infix symbol $\oplus : Data \times Data \rightarrow Data$ and two constants $0, 1 : Data$. Terms are equipped with the equational theory E_\oplus generated by:

$$\begin{array}{ll} x \oplus y = y \oplus x & x \oplus x = 0 \\ (x \oplus y) \oplus z = x \oplus (y \oplus z) & x \oplus 0 = x \end{array}$$

As an implementation, we define the computational algebras A_η , $\eta \geq 0$: the concrete domain $\llbracket Data \rrbracket_{A_\eta}$ is $\{0, 1\}^\eta$ equipped with the uniform distribution; \oplus is interpreted by the usual XOR function over $\{0, 1\}^\eta$, $\llbracket 0 \rrbracket_{A_\eta} = 0^\eta$, $\llbracket 1 \rrbracket_{A_\eta} = 1^\eta$.

In this setting, statically equivalent frames enjoy an algebraic characterization. Indeed, let φ and φ' be two frames with $\text{names}(\varphi) \cup \text{names}(\varphi') \subseteq \{a_1, \dots, a_n\}$ and $\text{dom}(\varphi) = \text{dom}(\varphi') = \{x_1, \dots, x_m\}$. We associate to φ a $(m+1) \times (n+1)$ -matrix $\alpha = (\alpha_{i,j})$ over the two element field \mathbb{F}_2 : the 0-th row of α is $(1, 0 \dots 0)$ and for $1 \leq i \leq m$, $1 \leq j \leq n$ (resp. $j = 0$) $\alpha_{i,j}$ is the number of occurrences of a_j (resp. of 1) in $\varphi(x_i)$, taken modulo 2. In the same way, a matrix α' is associated to φ' . Using classical manipulations on matrices, it is easy to show that $\varphi \approx_{E_\oplus} \varphi'$ iff the two associated matrices α and α' have the same image, that is $\alpha(\mathbb{F}_2^{n+1}) = \alpha'(\mathbb{F}_2^{n+1})$.

This characterization is the key point of our main result for the theory of XOR.

Theorem 3. *The usual implementation of the XOR theory is unconditionally $=_{E_\oplus}$ -, \approx_{E_\oplus} - and \forall_{E_\oplus} -sound. It is also $=_{E_\oplus}$ -, \approx_{E_\oplus} - and \forall_{E_\oplus} -faithful.*

This result is comparable to the work of Bana [6], who shows the unconditional soundness of the One-Time Pad encryption in a setting similar to that of Abadi and Rogaway [3]. In some sense our result is more precise as we model the XOR symbol itself and not a particular use of it.

5.2 Symmetric, deterministic, length-preserving encryption and lists

We now detail the example of symmetric, deterministic and length-preserving encryption schemes. Such schemes, also known as *ciphers* [13], are widely used in practice, the most famous examples being DES and AES.

Our formal model consists of a set of sorts $\mathcal{S} = \{Data, List_0, List_1 \dots List_n \dots\}$, an infinite number of names for every sort $Data$ and $List_n$, $n \neq 0$, and the symbols:

$$\begin{array}{ll} \text{enc}_n, \text{dec}_n : List_n \times Data \rightarrow List_n & \text{encryption, decryption} \\ \text{cons}_n : Data \times List_n \rightarrow List_{n+1} & \text{list constructor} \\ \text{head}_n : List_{n+1} \rightarrow Data & \text{head of a list} \\ \text{tail}_n : List_{n+1} \rightarrow List_n & \text{tail of a list} \\ \text{nil} : List_0 \quad 0, 1 : Data & \text{empty list, constants} \end{array}$$

We consider the equational theory E_{sym} generated by (for every $n \geq 0$)

$$\begin{array}{ll} \text{dec}_n(\text{enc}_n(x, y), y) = x & \text{cons}_n(\text{head}_n(x), \text{tail}_n(x)) = x \\ \text{enc}_n(\text{dec}_n(x, y), y) = x & \text{enc}_0(\text{nil}, x) = \text{nil} \\ \text{head}_n(\text{cons}_n(x, y)) = x & \text{dec}_0(\text{nil}, x) = \text{nil} \\ \text{tail}_n(\text{cons}_n(x, y)) = y & \end{array}$$

When oriented from left to right, the equations E_{sym} form an (infinite) convergent rewriting system, written \mathcal{R} . The equations $\text{enc}_n(\text{dec}_n(x, y), y) = x$ are characteristic of length-preserving encryption schemes. Indeed, encryption and decryption functions under each key then form a pair of mutually inverse bijections. The concrete meaning of sorts and symbols is given by the computational algebras A_η , $\eta > 0$, defined as follows:

- the carrier sets are $\llbracket \text{Data} \rrbracket_{A_\eta} = \{0, 1\}^\eta$ and $\llbracket \text{List}_n \rrbracket_{A_\eta} = \{0, 1\}^{n\eta}$ equipped with the uniform distribution and the usual equality relation;
- $\text{enc}_n, \text{dec}_n$ are implemented by a cipher for data of size $n\eta$ and keys of size η (we discuss the required cryptographic assumptions later);
- $\llbracket \text{nil} \rrbracket_{A_\eta}$ is the empty bit-string, $\llbracket \text{cons}_n \rrbracket_{A_\eta}$ is the usual concatenation, $\llbracket 0 \rrbracket_{A_\eta} = 0^\eta$, $\llbracket 1 \rrbracket_{A_\eta} = 1^\eta$, $\llbracket \text{head}_n \rrbracket_{A_\eta}$ returns the η first digits of bit-strings (of size $(n + 1)\eta$) whereas $\llbracket \text{tail}_n \rrbracket_{A_\eta}$ returns the last $n\eta$ digits.

Obviously, the above implementation is unconditionally $=_{E_{\text{sym}}}$ -sound. Before studying the $\approx_{E_{\text{sym}}}$ -soundness, we need to characterize statically equivalent frames. Specifically we show that this theory admits patterns, in the sense of Section 3.

Proposition 5. *Let φ be a closed frame. There exists a pattern $\bar{\varphi}$ such that $\varphi \approx_{E_{\text{sym}}} \bar{\varphi}$.*

Proof (outline). We associate a pattern to any frame φ by the following procedure:

1. normalize φ using the rules \mathcal{R} (the result is still denoted φ);
2. while φ is not a pattern, repeat: find any subterm T of the form $T = \text{enc}_n(U, V)$, $T = \text{dec}_n(U, V)$, $T = \text{head}_n(V)$ or, $T = \text{tail}_n(V)$, with $\varphi \not\vdash_{E_{\text{sym}}} V$ and replace T everywhere in φ by a fresh name a of the appropriate sort.

We prove in [7] that this procedure always terminates on a pattern statically equivalent to the initial frame.

We now study the $\approx_{E_{\text{sym}}}$ -soundness problem under realistic cryptographic assumptions. Classical assumptions on ciphers include the notions of super pseudo-random permutation (SPRP) and several notions of indistinguishability (IND-Pi-Cj, $i, j = 0, 1, 2$). In particular, IND-P1-C1 denotes the indistinguishability against lunchtime chosen-plaintext and chosen-ciphertext attacks. These notions and the relations between them have been studied notably in [13].

Initially, the SPRP and IND-P1-C1 assumptions apply to (block) ciphers specialized to plaintexts of a given size. Interestingly, this is not sufficient to imply $\approx_{E_{\text{sym}}}$ -soundness for frames which contain plaintexts of heterogeneous sizes, encrypted under the same key. Thus we introduce a strengthened version of IND-P1-C1, applying to a *collection* of ciphers $(\mathcal{E}_{\eta,n}, \mathcal{D}_{\eta,n})$, where η is the complexity parameter and $n \geq 0$ is the number of blocks of size η contained in plaintexts and ciphertexts.

We define the ω -IND-P1-C1 assumption by considering the following experiment \mathcal{G}_η involving a 2-stage adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$:

- first a key k is randomly chosen from $\{0, 1\}^\eta$;
- (Stage 1) \mathcal{A}_1 is given access to the encryption oracles $\mathcal{E}_{\eta,n}(\cdot, k)$ and the decryption oracles $\mathcal{D}_{\eta,n}(\cdot, k)$; it outputs two plaintexts $m_0, m_1 \in \{0, 1\}^{n_0\eta}$ for some n_0 , and possibly some data d ;
- (Stage 2) a random bit $b \in \{0, 1\}$ is drawn; \mathcal{A}_2 receives the data d , the *challenge ciphertext* $c = \mathcal{E}_{\eta,n_0}(m_b, k)$ and outputs a bit b' ;
- \mathcal{A} is *successful* in \mathcal{G}_η iff $b = b'$ and it has never submitted m_0 or m_1 to an encryption oracle, nor c to a decryption oracle.

Define the *advantage* of \mathcal{A} as: $\text{Adv}_{\mathcal{A}}^{\omega\text{-IND-P1-C1}}(\eta) = 2 \times \mathbb{P}[\mathcal{A} \text{ is successful in } \mathcal{G}_\eta] - 1$. The $\omega\text{-IND-P1-C1}$ assumption holds for $(\mathcal{E}_{\eta,n}, \mathcal{D}_{\eta,n})$ iff the advantage of any probabilistic polynomial-time adversary is negligible. It holds for the *inverse* of the encryption scheme, iff it holds for the collection of ciphers $(\mathcal{D}_{\eta,n}, \mathcal{E}_{\eta,n})$.

As in previous work [3, 12, 4, 11], we restrict frames to those with only atomic keys and no encryption cycles. Specifically a closed frame φ *has only atomic keys* if for all subterms $\text{enc}_n(u, v)$ and $\text{dec}_n(u, v)$ of φ , v is a name. Given two (atomic) keys k_1 and k_2 , we say that k_1 *encrypts* k_2 in φ , written $k_1 >_\varphi k_2$, iff there exists a subterm U of φ of the form $U = \text{enc}_n(T, k_1)$ or $U = \text{dec}_n(T, k_1)$ such that k_2 appears in T *not used as a key*, i.e. k_2 appears in T at a position which is not the right-hand argument of a $\text{enc}_{n'}$ or a $\text{dec}_{n'}$. An *encryption cycle* is a tuple $k_1 \dots k_m$ such that $k_1 >_\varphi \dots >_\varphi k_m >_\varphi k_1$.

The effect of the condition “not used as a key” is to allow considering more terms as free of encryption cycles, for instance $\text{enc}_n(\text{enc}_n(a, k), k)$. This improvement is already suggested in [3].

We now state our $\approx_{E_{\text{sym}}}$ -soundness theorem. A closed frame is *well-formed* iff its \mathcal{R} -normal form has only atomic keys, contains no encryption cycles and uses no head and tail symbols.

Theorem 4 ($\approx_{E_{\text{sym}}}$ -soundness). *Let φ_1 and φ_2 be two well-formed frames of the same domain. Assume that the concrete implementations for the encryption and its inverse satisfy both the $\omega\text{-IND-P1-C1}$ assumption. If $\varphi_1 \approx_{E_{\text{sym}}} \varphi_2$ then $(\llbracket \varphi_1 \rrbracket_{A_\eta}) \approx (\llbracket \varphi_2 \rrbracket_{A_\eta})$.*

Note on the cryptographic assumptions. Cryptographic assumptions of Theorem 4 may appear strong compared to existing work on passive adversaries [3, 12]. Nevertheless if φ_1 and φ_2 contain no decryption symbols, our proofs are easily adapted to work when the encryption scheme is $\omega\text{-IND-P1-C0}$ only, where $\omega\text{-IND-P1-C0}$ is defined similarly to $\omega\text{-IND-P1-C1}$ except that the adversary has no access to the decryption oracle.

Also, it is possible to recover the classical assumptions IND-P1-C1 by modeling the ECB mode (Electronic Code Book). Let us add two symbols $\text{enc} : \text{Data} \times \text{Data} \rightarrow \text{Data}$ and $\text{dec} : \text{Data} \times \text{Data} \rightarrow \text{Data}$, and define the symbols enc_n and dec_n (formally and concretely) recursively by

$$\begin{aligned} \text{enc}_{n+1}(x, y) &= \text{cons}_n(\text{enc}(\text{head}_n(x), y), \text{enc}_n(\text{tail}_n(x), y)) \quad \text{and} \\ \text{dec}_{n+1}(x, y) &= \text{cons}_n(\text{dec}(\text{head}_n(x), y), \text{dec}_n(\text{tail}_n(x), y)). \end{aligned}$$

Define well-formed frames as those of which the normal forms contain no encryption cycles. The $\approx_{E_{\text{sym}}}$ -soundness property holds for well-formed frames as soon as the implementations for enc and dec are both IND-P1-C1, or equivalently [13] enc is SPRP.

6 Conclusion and future work

In this paper we developed a general framework for relating formal and computational models of security protocols in the presence of a passive attacker. These are the first results on abstract models allowing arbitrary equational theories. We define the soundness and faithfulness of cryptographic implementations *w.r.t.* abstract models. We also provide a soundness criterion which for a large number of theories—those that admit a

general notion of patterns—is not only sufficient but also necessary. Finally, we provide new soundness results for the exclusive OR and a theory of ciphers and lists.

As future work, we foresee to study the soundness of other theories. An interesting case would be the combination of the two theories considered in this paper: in a theory combining XOR, ciphers and lists, one can precisely model the *Cipher Block Chaining* (CBC) mode, which is commonly used with block ciphers such as DES or AES. Another ambitious extension is to consider the case of an active attacker.

Acknowledgments. This work has been partially supported by the ACI-SI Rossignol, the ACI JC 9005 and the RNTL project PROUVÉ 03V358 and 03V360.

References

1. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. In *Proc. 31st International Colloquium on Automata, Languages and Programming (ICALP'04)*, volume 3142 of *LNCS*, pages 46–58, 2004.
2. M. Abadi and C. Fournet. Mobile values, new names, and secure communications. In *Proc. 28th Annual ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, 2001.
3. M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In *Proc. 1st IFIP International Conference on Theoretical Computer Science (IFIP-TCS'00)*, volume 1872 of *LNCS*, pages 3–22, 2000.
4. M. Backes and B. Pfizmann. Symmetric encryption in a simulatable Dolev-Yao style cryptographic library. In *Proc. 17th IEEE Computer Science Foundations Workshop (CSFW'04)*, pages 204–218, 2004.
5. M. Backes, B. Pfizmann, and M. Waidner. A composable cryptographic library with nested operations. In *Proc. 10th ACM Conference on Computer and Communications Security (CCS'03)*, 2003.
6. G. Bana. *Soundness and Completeness of Formal Logics of Symmetric Encryption*. PhD thesis, University of Pennsylvania, 2004.
7. M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. Research Report 2005/074, Cryptology ePrint Archive, Mar. 2005. 28 pages.
8. B. Blanchet. Automatic proof of strong secrecy for security protocols. In *Proc. 25th IEEE Symposium on Security and Privacy (SSP'04)*, pages 86–100, 2004.
9. D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, IT-29(12):198–208, 1983.
10. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
11. P. Laud. Symmetric encryption in automatic analyses for confidentiality against active adversaries. In *Proc. IEEE Symposium on Security and Privacy (SSP'04)*, pages 71–85, 2004.
12. D. Micciancio and B. Warinschi. Completeness theorems for the Abadi-Rogaway logic of encrypted expressions. *Journal of Computer Security*, 12(1):99–129, 2004.
13. D. H. Phan and D. Pointcheval. About the security of ciphers (semantic security and pseudo-random permutations). In *Proc. Selected Areas in Cryptography (SAC'04)*, volume 3357 of *LNCS*, pages 185–200, 2004.
14. R. L. Rivest. On the notion of pseudo-free groups. In *Proc. 1st Theory of Cryptography Conference (TCC'04)*, volume 2951 of *LNCS*, pages 505–521, 2004.