# Adaptive Soundness of Static Equivalence *

Steve Kremer and Laurent Mazaré

LSV, ENS Cachan & CNRS & INRIA Futurs
{kremer|mazare}@lsv.ens-cachan.fr

**Abstract.** We define a framework to reason about implementations of equational theories in the presence of an adaptive adversary. We particularly focus on soundess of static equivalence. We illustrate our framework on different equational theories: symmetric encryption, modular exponentiation and also joint theories of encryption and modular exponentiation. Finally, we define a model for symbolic analysis of dynamic group key exchange protocols, and show its computational soundness.

## 1 Introduction

The need for rigorous proofs of security protocols was recognized very early and two distinct, competing approaches have been developed: the symbolic approach and the computational one. Proofs in the symbolic model can be (partially) automated, but it is not clear whether this abstract model captures all possible attacks. Proofs in the computational model provide stronger security guarantees but are generally harder and difficult to automate. A recent trend tries to get the best of both worlds: an abstract model with strong computational guarantees. In their seminal paper, Abadi and Rogaway [3] have shown a first such *soundness result* for symmetric encryption in the presence of a passive attacker.

Recently, Baudet *et al.* [5] presented a general framework for reasoning about sound implementations of equational theories. Instead of a fixed set of cryptographic primitives, they allow a specification by the means of an equational theory. The formal indistinguishability relation they consider is static equivalence, a well-established security notion coming from cryptographic pi calculi [2] whose verification can often be automated. Studying soundness of equational theories is motivated by the numerous recent works on extending the classical Dolev-Yao result with equations which are intended to capture algebraic properties of cryptographic primitives (see [6] for a survey on such algebraic properties). Showing a soundness result for an equational theory proves that indeed "enough" equations have been considered.

In this paper we consider the question of soundness of static equivalence in the presence of an *adaptive adversary*. This extends the work by Baudet *et al.* in a similar way as the work of Micciancio and Panjwani [8] extended the work of Abadi and Rogaway [3]. We define the notion of adaptive soundness of static equivalence in a general framework. Our notion is strictly stronger than the purely passive soundness from [5]. We give adaptive soundness results for symmetric encryption provided that the encryption scheme respects a length-concealing IND-CPA security notion (this is similar to the main result in [8]) and modular exponentiation in an Abelian group provided that the *Decisional Diffie-Hellman* (DDH) assumption is verified. Finally, we use a combination technique to derive adaptive soundness for the joint theory of encryption and modular exponentiation. We believe these are the first adaptive soundness results for modular exponentiation. Their importance is motivated by real-life protocols such as SSL/TLS that rely on Diffie-Hellman key exchange and thus use modular exponentiation.

To illustrate the usefulness of adaptive adversaries we define a symbolic model for the analysis of dynamic group key exchange (DKE) protocols and use our adaptive soundness result to show that this symbolic model is sound with respect to a corresponding computational model.

*Related work.* As discussed above this paper is most obviously related to the works by Baudet *et al.* [5] and Micciancio and Panjwani [8]. Our paper generalizes both of these works. Abadi *et al.* [1] also use the framework of [5] to show soundness of an equational theory useful for reasoning about offline guessing attacks modeled as a static equivalence. In [4], Bana *et al.* argue that the notion of static equivalence is too coarse and not sound for many interesting equational theories. As an example they show that the DDH

* Work partly supported by the ARA SSIA Formacrypt.

assumption is not sufficient to imply soundness of static equivalence. They introduce a general notion of *formal indistinguishability relation*. In this paper we prefer to stick to static equivalence which has the advantage of being a well-established, tool-supported equivalence relation. We address the problems highlighted in [4] by proving soundness for a restricted set of *well-formed* frames (in the same vein Abadi and Rogaway used restrictions to forbid key cycles).

A long version of this paper is available as [7].

## 2 Abstract and computational algebras

*Abstract model.* Our abstract models consist of term algebras defined over a many-sorted first-order signature and equipped with equational theories. Specifically, a *signature* $(\mathcal{S}, \mathcal{F})$ is made of a set of *sorts* $\mathcal{S} = \{s, s_1 \ldots\}$ and a set of *symbols* $\mathcal{F} = \{f, f_1 \ldots\}$ together with arities of the form $\mathrm{ar}(f) = s_1 \times \ldots \times s_k \to s$, $k \geq 0$. Symbols in $\mathcal{F}$ are intended to model cryptographic primitives, whereas names are used to model secrets, *e.g.*, keys. The abstract semantics of symbols is described by an equational theory $E$. For instance, symmetric encryption can be modeled by the classical theory $E_{\mathsf{enc}} = \{\mathrm{dec}(\mathrm{enc}(x, y), y) = x\}$.

We use *frames* to represent sequences of messages observed by an attacker. Formally, a *frame* is an expression $\varphi = \nu\tilde{a}.\{x_1 = t_1, \ldots, x_n = t_n\}$ where $\tilde{a}$ is a set of *restricted names*, and $t_i$ are closed terms. For simplicity, we only consider frames $\varphi = \nu\tilde{a}.\{x_1 = t_1, \ldots, x_n = t_n\}$ which restrict every name in use and assimilate such frames $\varphi$ to their *underlying substitutions* $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ also denoted $\{x_i \mapsto t_i\}_{1 \leq i \leq n}$. We consider two frames to be formally indistinguishable if they are *statically equivalent* [2].

**Definition 1 (Static equivalence).** *Two frames $\varphi_1$ and $\varphi_2$ are* statically equivalent *in a theory $E$, written $\varphi_1 \approx_E \varphi_2$, iff $\mathrm{dom}(\varphi_1) = \mathrm{dom}(\varphi_2)$, and for all terms $M$ and $N$ such that $\mathrm{var}(M, N) \subseteq \mathrm{dom}(\varphi_1)$ and $\mathrm{names}(M, N) \cap \mathrm{names}(\varphi_1, \varphi_2) = \emptyset$, $M\varphi_1 =_E N\varphi_1$ is equivalent to $M\varphi_2 =_E N\varphi_2$.*

*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 $[\![s]\!]_A \subseteq \{0,1\}^*$ for each sort $s \in \mathcal{S}$;
- an effective procedure to draw random elements from $[\![s]\!]_A$, denoted $x \xleftarrow{R} [\![s]\!]_A$.
- a computable function $[\![f]\!]_A : [\![s_1]\!]_A \times \ldots \times [\![s_k]\!]_A \to [\![s]\!]_A$ for all $f \in \mathcal{F}$, $\mathrm{ar}(f) = s_1 \times \ldots \times s_k \to s$;

Assume a fixed $(\mathcal{S}, \mathcal{F})$-computational algebra $A$. We associate to each frame $\varphi = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ a distribution $\psi = [\![\varphi]\!]_A$, of which the drawings $\widehat{\psi} \xleftarrow{R} \psi$ are computed as follows:

1. for each name $a$ of sort $s$ appearing in $t_1, \ldots, t_n$, draw a value $\widehat{a} \xleftarrow{R} [\![s]\!]_A$;
2. for each $x_i$ $(1 \leq i \leq n)$ of sort $s_i$, compute $\widehat{t_i} \in [\![s_i]\!]_A$ recursively on the structure of terms: $\widehat{f(t'_1, \ldots, t'_m)} = [\![f]\!]_A(\widehat{t'_1}, \ldots, \widehat{t'_m})$;
3. return the value $\widehat{\psi} = \{x_1 \mapsto \widehat{t_1}, \ldots, x_n \mapsto \widehat{t_n}\}$.

Such values $\phi = \{x_1 = e_1, \ldots, x_n = e_n\}$ with $e_i \in [\![s_i]\!]_A$ are called *concrete frames*. We extend the notation $[\![.]\!]_A$ to (tuples of) closed terms in the obvious way.

We focus on asymptotic notions of cryptographic security and consider families of computational algebra $(A_\eta)$ indexed by a complexity parameter $\eta \geq 0$. The *concrete semantics* of a frame $\varphi$ is a family of distributions over concrete frames $([\![\varphi]\!]_{A_\eta})$.

Families of distributions (*ensembles*) over concrete frames benefit from the usual notion of cryptographic indistinguishability. Intuitively, two families of distributions. $(\psi_\eta)$ and $(\psi'_\eta)$ 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 $\psi_\eta$ or $\psi'_\eta$ with a probability significantly greater than $\frac{1}{2}$.

## 3 Adaptive soundness

We first recall the original notion of soundness for static equivalence which considers a passive adversary [5].

**Definition 2 ($\approx_E$-soundness).** *Let $E$ be an equational theory. A family of computational algebras $(A_\eta)$ is* $\approx_E$-sound *iff for every frames $\varphi_1, \varphi_2$ with the same domain, $\varphi_1 \approx_E \varphi_2$ implies that $(\llbracket\varphi_1\rrbracket_{A_\eta}) \approx (\llbracket\varphi_2\rrbracket_{A_\eta})$.*

Baudet *et al.* also introduce a strong notion of soundness that holds without restriction on the computational power of adversaries.

**Definition 3 (Unconditional $\approx_E$-soundness).** *Let $E$ be an equational theory. A family of computational algebras $(A_\eta)$ is* unconditionally $\approx_E$-sound *iff for every frames $\varphi_1, \varphi_2$ with the same domain, $\varphi_1 \approx_E \varphi_2$ implies $(\llbracket\varphi_1\rrbracket_{A_\eta}) = (\llbracket\varphi_2\rrbracket_{A_\eta})$.*

The adaptive setting is formalized through the following cryptographic game. Let $(A_\eta)$ be a family of computational algebras and $\mathcal{A}$ be an adversary. $\mathcal{A}$ has access to a left-right evaluation oracle $\mathcal{O}_{LR}$ which given a pair of symbolic terms $(t_0, t_1)$ outputs either the implementation of $t_0$ or of $t_1$. This oracle depends on a selection bit $b$ and uses a local store to record values generated for the different names (these values are used when processing further queries). With a slight abuse of notation, we omit this store and write: $\mathcal{O}^b_{LR,A_\eta}(t_0, t_1) = \llbracket t_b\rrbracket_{A_\eta}$. Adversary $\mathcal{A}$ plays an indistinguishability game with the objective of finding the value of $b$. Formally the advantage of $\mathcal{A}$ is defined by:

$$\mathrm{Adv}^{\mathsf{ADPT}}_{\mathcal{A},A_\eta}(\eta) = \left|\mathbb{P}\left[\mathcal{A}^{\mathcal{O}^1_{LR,A_\eta}} = 1\right] - \mathbb{P}\left[\mathcal{A}^{\mathcal{O}^0_{LR,A_\eta}} = 1\right]\right|$$

Without further restrictions on the queries made by the adversary, having a non-negligible advantage is easy in most cases: the adversary could simply submit a pair $(0, 1)$ to his oracle. We therefore require the adversary to be *legal*.

**Definition 4 (Adaptive soundness).** *An adversary $\mathcal{A}$ is* legal *if for any sequence of queries $(t^i_0, t^i_1)_{1\le i\le n}$ made by $\mathcal{A}$ to its left-right oracle, queries are statically equivalent:*

$$\left\{x_1 \mapsto t^1_0, \ldots, x_n \mapsto t^n_0\right\} \approx_E \left\{x_1 \mapsto t^1_1, \ldots, x_n \mapsto t^n_1\right\}$$

*A family of computational algebras $(A_\eta)$ is*

- $\approx_E$-ad-sound *iff $\mathrm{Adv}^{\mathsf{ADPT}}_{\mathcal{A},A_\eta}(\eta)$ is negligible for any probabilistic polynomial-time legal adversary $\mathcal{A}$.*
- unconditionally $\approx_E$-ad-sound *iff $\mathrm{Adv}^{\mathsf{ADPT}}_{\mathcal{A},A_\eta}(\eta)$ is $0$ for any legal adversary $\mathcal{A}$.*

We show that adaptive soundness implies the original soundness notion for static equivalence while the converse is not true in general.

**Proposition 1.** *Let $(A_\eta)$ be a family of computational algebras. If $A_\eta$ is $\approx_E$-ad-sound then $A_\eta$ is also $\approx_E$-sound but the converse is false in general.*

Interestingly, for unconditional soundness, the adaptive and non-adaptive case coincide.

**Proposition 2.** *Let $(A_\eta)$ be a family of computational algebras. $A_\eta$ is unconditionally $\approx_E$-ad-sound iff $A_\eta$ is unconditionally $\approx_E$-sound.*

## 4 Adaptively sound theories

*Symmetric encryption.* We consider probabilistic symmetric encryption and pairs modeled by an equational theory $E_{\mathsf{sym}}$ generated by:

$$\begin{aligned} \mathrm{dec}(\mathrm{enc}(x,y),y) &= x & \qquad \pi_l(\mathrm{pair}(x,y)) &= x \\ \pi_r(\mathrm{pair}(x,y)) &= y & \qquad \mathrm{samekey}(\mathrm{enc}(x,y),\mathrm{enc}(z,y)) &= 1 \\ \mathrm{tenc}(\mathrm{enc}(x,y)) &= 1 & \qquad \mathrm{tpair}(\mathrm{pair}(x,y)) &= 1 \end{aligned}$$

Intuitively, the function symbols $\mathrm{tenc}, \mathrm{tpair}$ are type testers. The symbol $\mathrm{samekey}$ tests whether two encryptions have been encrypted using the same key. The meaning of the remaining symbols should be clear. As usual $\mathrm{enc}(t,k)$ is also written $\{t\}_k$ and $\mathrm{pair}(t,t')$ is also written $(t,t')$. A name $k$ is used at a key position in a term $t$ if there exists a sub-term $\mathrm{enc}(t',k)$ of $t$. Else $k$ is used at a plaintext position. We assume that the implementation of the symmetric encryption scheme is length-concealing IND-CPA secure.

As in [3] and [8], we have to restrict ourselves to *well-formed* frames to avoid problems related to key-cycles and selective decommitment. Let $\prec$ be a total order among keys. A *frame* $\varphi = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ *is well-formed for* $\prec$ if

- $\varphi$ is acyclic for $\prec$;
- the terms $t_i$ only use symbols $\mathrm{enc}$, $\mathrm{pair}$, $0$ and $1$, and only names are used at key positions;
- if $k$ is used as plaintext in $t_i$, then $k$ cannot be used at a key position in $t_j$ for $j < i$.

An *adversary is well-formed for* $\prec$ if the sequence of queries $(t_0^i, t_1^i)_{1 \le i \le n}$ that he makes to his oracle yields two well-formed frames $\{x_1 \mapsto t_0^1, \ldots, x_n \mapsto t_0^n\}$ and $\{x_1 \mapsto t_1^1, \ldots, x_n \mapsto t_1^n\}$ for $\prec$.

We show adaptive $\approx_E$-soundness for *well-formed* frames for an implementation based on length-concealing IND-CPA encryption.

**Proposition 3.** *Let $\prec$ be a total order among keys. In the remainder of this proposition we only consider well-formed adversaries for $\prec$. Let $(A_\eta)$ be a family of computational algebras based on a symmetric encryption scheme $\mathcal{SE}$. $(A_\eta)$ is $\approx_{E_{\mathsf{sym}}}$-ad-sound if $\mathcal{SE}$ is* IND-CPA *but the converse is false.*

*Modular exponentiation* We study soundness of modular exponentiation. The symbolic model relies on the following equational theory $E_{\mathsf{DH}}$:

$$\begin{array}{ccc} x+y = y+x & x \cdot y = y \cdot x & (x+y)+z = x+(y+z) \\ x \cdot (y+z) = x \cdot y + x \cdot z & (x \cdot y) \cdot z = x \cdot (y \cdot z) & x + (-x) = 0_R \\ 0_R + x = x & 1_R \cdot x = x & \exp(x) * \exp(y) = \exp(x+y) \end{array}$$

We put two restrictions on formal terms: products have to be *power-free, i.e.,* $x^n$ is forbidden for $n > 1$, and products must not contain more than $l$ elements for some fixed bound $l$, i.e. $x_1 \cdot \ldots \cdot x_n$ is forbidden for $n > l$. Both restrictions come from the DDH assumption and seem difficult to avoid.

The underlying cryptographic assumption is hardness of the *Decisional Diffie-Hellman* (DDH) problem. An Instance Generator $IG$ is a polynomial-time (in $\eta$) algorithm that outputs a cyclic group $\mathbb{G}$ (defined by a generator $g$, an order $q$ and a polynomial-time multiplication algorithm) of prime order $q$. The family of computational algebras $(A_\eta)$ depends on an instance generator $IG$ which generates a cyclic group $\mathbb{G}$ of generator $g$ and of order $q$: the concrete domain $[\![R]\!]_{A_\eta}$ is $\mathbb{Z}_q$ with the uniform distribution. Symbols $+$, $\cdot$, $\exp$, $0_R$ and $1_R$ are implemented as expected. The domain $[\![G]\!]_{A_\eta}$ contains all bit-string representations of elements of $\mathbb{G}$. A family of computational algebras satisfies the DDH assumption if its instance generator satisfies the assumption: for every probabilistic polynomial-time adversary $\mathcal{A}$, his advantage

$$\begin{array}{rl} \mathrm{Adv}^{\mathsf{DDH}}_{IG,\mathcal{A}}(\eta) = & \left| \mathbb{P}\left[(g,q) \leftarrow IG(\eta) \ : \ a,b \leftarrow \mathbb{Z}_q \ : \ \mathcal{A}(g^a, g^b, g^{ab}) = 1\right]\right. \\ - & \left. \mathbb{P}\left[(g,q) \leftarrow IG(\eta) \ : \ a,b,c \leftarrow \mathbb{Z}_q \ : \ \mathcal{A}(g^a, g^b, g^c) = 1\right]\right| \end{array}$$

is negligible in $\eta$.

Under these assumptions we show that hardness of DDH is both necessary and sufficientto imply adaptive $\approx_{E_{\mathsf{DH}}}$-soundness.

**Proposition 4.** *We have that* $\{x_1 \mapsto \exp(p_1), ..., x_n \mapsto \exp(p_n)\} \approx_{E_{\mathsf{DH}}} \{x_1 \mapsto \exp(q_1), ..., x_n \mapsto \exp(q_n)\}$ *iff for any sequence of integer $a_0, a_1, \ldots a_n$ we have* $a_0 + \sum_{i=1}^n a_i p_i = 0 \Leftrightarrow a_0 + \sum_{i=1}^n a_i q_i = 0$

*Combining encryption with exponentiation.* We also show soundness for the joint theory of encryption and modular exponentiation where group elements can be used either as plain text or as encryption keys. The implementation relies on a *key extractor* algorithm that transforms group elements into valid keys.

## 5 Analysis of dynamic group key exchange

We examplify the usefullness of our model on *dynamic group key exchange protocols* (DKE) protocols. We take a simple model for DKE in the adaptive setting. A DKE protocol is described by four operations which specify the protocol. We suppose that this specification is given by four polynomial-time algorithms $(\mathcal{S}, \mathcal{J}, \mathcal{L}, \mathcal{K})$:

- $\mathcal{S}$ initializes a new group. The algorithm takes as an input a list of users and outputs the internal state $s_0$ of the protocol as well as a list of formal terms which model the messages that have been exchanged during the setup phase.
- $\mathcal{J}$ and $\mathcal{L}$ take as input the state of the protocol $s$ and a list of users $U_1$ to $U_n$ (to be respectively added to or suppressed from the group) and output the updated state of the protocol $s'$ as well as a list of formal terms representing message exchanges.
- $\mathcal{K}$ takes as input the state of the group $s$ and outputs a formal term representing the shared key of the group.

The internal state of the protocol can be thought of as the internal state of the four algorithms that describe the protocol.

We allow an adversary to first statically corrupt some users, setup a new group with users chosen by the adversary and then let the adversary adaptively decide which users join and leave the group. Using our soundness result we prove that symbolic security, expressed in terms of static equivalence, implies concrete security, *i.e.*, the adversary cannot efficiently distinguish the group key from a random key.

## 6 Conclusion

We defined a framework for reasoning about the soundness of equational theories in the presence of adaptive adversaries. The framework is illustrared on several equational theories: symmetric encryption, modular exponentiation as well as the joint theory of encryption and modular exponentiation. Finally we demonstrate the usefulness of adaptive soundness by giving a sound symbolic model for the analysis of DKE protocols.

This work opens the possibility for studying other interesting equational theories in an adaptive setting, such as the theory used in [1] in the context of offline guessing attacks. A natural future work is to use the symbolic model for DKE protocols defined in this paper on case studies. An ambitious extension is the soundness in the presence of a both active and adaptive adversary.

## References


1. M. Abadi, M. Baudet, and B. Warinschi. Guessing attacks and the computational soundness of static equivalence. In *Proc. 9th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'06)*, volume 3921 of *Lecture Notes in Computer Science*, pages 398–412. Springer, 2006.
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. ACM Press, 2001.
3. M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In *IFIP International Conference on Theoretical Computer Science (IFIP TCS'00)*, volume 1872 of *Lecture Notes in Computer Science*. Springer, 2000.
4. G. Bana, P. Mohassel, and T. Stegers. The computational soundness of formal indistinguishability and static equivalence. In *Proc. 11th Asian Computing Science Conference (ASIAN'06)*, Lecture Notes in Computer Science. Springer, 2006. To appear.
5. M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *Lecture Notes in Computer Science*, pages 652–663. Springer, 2005.
6. V. Cortier, S. Delaune, and P. Lafourcade. A Survey of Algebraic Properties Used in Cryptographic Protocols. *Journal of Computer Security*, To appear, 2005.
7. S. Kremer and L. Mazaré. Adaptive soundness of static equivalence. Research Report LSV-07-09, Laboratoire Spécification et Vérification, ENS Cachan, France, Feb. 2007. 27 pages.
8. D. Micciancio and S. Panjwani. Adaptive security of symbolic encryption. In *Proc. 2nd Theory of cryptography conference (TCC'05)*, volume 3378 of *Lecture Notes in Computer Science*, pages 169–187. Springer, 2005.