AUTOMATED VERIFICATION OF ASYMMETRIC ENCRYPTION

Van Chan NGO

June 2008

Acknowledgements

I would like to thank Cristian ENE, Yassine LAKHNECH for their tremendous support as thesis advisors, and also for introducing me to the subject and to the information security and cryptography community. I would like to thank Philippe AUDEBAUD for his much effort of reading and examining this report. I also would like to thank the Security Work Group (Groupe de Travail Sécurité - GDT Sécurité) for the great hours of research we spent on the subject, and for reading the manuscript and providing valuable suggestions. Finally, many thanks are due to all the members of Distributed and Complex Systems - DCS, VERIMAG Laboratory, Grenoble, France for their support, and for all that I learned there in math, computer science and in life matters as well.
During the work on this thesis I was supported by the Office of Scholarship of French Government (Le Bureau de Bourse du Gouvernement Francais) through the grant No. 20074041, with additional support by a VERIMAG internship.

Abstract

Automated Verification of Asymmetric Encryption

Van Chan NGO
Supervisor: Cristian ENE, Yassine LAKHNECH

In the last two decades, two major directions in cryptography have developed: formal and computational. In formal approaches, the knowledge of attackers is often treated in terms of message deducibility and indistinguishability relations. The formal approach uses simple, manageable formal languages to describe cryptographic protocols; this approach is amenable to automatization, suitable for computer tools, but its accuracy is often unclear. The computational approach is harder to handle mathematically, involves probability theory and considers limits in computing power; proofs are done by hand, but it is more accurate, hence widely accepted.

Much effort has been made to bridge the gap between the two approaches, including the work in [4, 7, 8] who considered a formal logic of asymmetric encryption and its interpretations in cryptosystems based on computational complexity. Their setting has three important ingredients: a formal language along with an equivalence notion of formal expressions, a computational cryptosystem with the notion of computational equivalence of ensembles of random distributions, and an interpreting function that assigns to each formal expression an ensemble of distributions. We say that the interpretation satisfies soundness if equivalence of formal expressions implies computational equivalence of their interpretations, and satisfies completeness if computational equivalence of the interpretations requires equivalence of the expressions.

As the previous work [7, 8] has shown that using static equivalence from cryptographic pi calculus as a notion of formal indistinguishability yields the soundness of the interpretations. But in several explicit examples in which static equivalence fails to work. To fix the problem, the work in [8] propose a notion of formal indistinguishability that is more flexible. Based on this approach, we propose a new notion of formal non-deducibility that is more flexible, manageable than the notion deducibility and non-deducibility in [4, 5, 6, 8]. We also establish general soundness for the interpretation of this notation of formal non-deducibility. The main results of this work are providing a general framework to verify the secure property (IND-CPA) of asymmetric encryption schemes automatically, to be suitable for computer tools. This general framework is constructed from the basic axioms on the encryption primitives and along with general propositions that not only help us to generate formal non-deducibility and formal indistinguishability relations, but also guaranty the soundness of the interpretations. Finally we discuss how this general framework works for some explicit examples.

Contents

List of Figures

Introduction

Designing and verifying security protocol and encryption schemes are complex problems; certain level of idealization is needed in order to provide manageable mathematical treatment of the security protocols, encryption and the notion of security. Idealizations necessarily omit some properties of the real system, which might lead to leaks in the security. Two communities separately developed two families of models. Both views have been very useful in increasing the understanding and quality of security protocol and encryption design. The two main being a highly abstract treatment with the help of formal logic based on the seminal work of Dolev and Yao [19], and a more detailed description using complexity and probability theory which are closer to implementations. In the former, cryptographic operations are modeled as functions on a space of symbolic (formal) expressions and their security properties are also treated formally. Examples are [1, 3, 19, 21, 22, 6, 7, 8, 5]. In the latter, cryptographic operations act on strings of bits, and their security properties are defined in terms of probability and computational complexity. Examples for this treatment are [4, 23, 20, 21]. The first approach has been labeled in the literature as formal view, whereas the second as computational view.

The computational view gives a more detailed description of cryptographic operations, taking limited computing power into account; probability plays an important role as well. "Good protocols are those in which adversaries cannot do something bad too often and efficiently enough" [4]. Keys, plaintexts, ciphers are all strings of bits, encryption, decryption and adversaries are all probabilistic algorithms, and a mathematically well-defined notion of computability in polynomial-time is imposed on all these algorithms. A major achievement of this approach has been that common notions of security such as secrecy, authentication, etc. were given mathematically precise definition, hence clarifying them and making them amenable to mathematical analysis. However, the detailed and less structured nature of this view makes analyzing more complex protocols a very hard task, which calls for a higher level, more abstract treatment.

On the other hand, 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 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 [4], Abadi and Rogaway prove the computational soundness of formal (symmetric) encryption in the case a passive attacker. Since then, many results have been obtained. Each of these results considers a fixed set of primitives, for instance symmetric or public-key encryption. These efforts are developing rigorous mathematical treatment of the relationship between the two models. It is hoped that they will eventually lead to a new generation of "high fidelity" automated tools for security analysis, which will be able to express and implement the methods and concepts of modern cryptography. We concentrate on non-deducibility and static equivalence, a standard notion originates from the applied pi calculus [1]. Many formal definitions explain the knowledge of an attacker in terms of message deduction. Given a set of messages S and another message M, one asks whether M can be computed from S. The messages are represented by expressions, and correspondingly the computations allowed are symbolic manipulations of those expressions. These computations can rely on any step that an eavesdropper who has obtained the messages in S can perform on its own in order to derive M. For instance, the eavesdropper can decrypt using known keys, and it can extract parts of messages. Despite its usefulness in proofs about protocol behaviors, the concept of message deduction does not always provide a sufficient account of knowledge, and it is worthwhile to consider alternatives. For instance, suppose that we are interested in a protocol that transmits an encrypted boolean value, possibly a different one in each run. We might like to express that this boolean value remains secret by saying that no attacker can learn it by eavesdropping on the protocol. On the other hand, it is unreasonable to say that an attacker cannot deduce the well-known boolean values "true" and "false"'. Instead, we may say that the attacker cannot distinguish an instance of the protocol with the value "true" from one with the value "false". More generally, we may say that two systems are equivalent when an attacker cannot distinguish them, and we may then express security guarantees as equivalences. The use of equivalences is common in computational approaches to cryptography, and it also figures prominently in several formal methods. Two systems that output messages that an attacker can tell apart are obviously distinguishable. Conversely, in order to establish equivalences between systems, an important subtask is to establish equivalences between the messages that the systems generate (for example, between the encrypted boolean values). These equivalences may be called static equivalences, because they consider only the messages, not the dynamic processes that generate them. Bi-simulation proof techniques can reduce process equivalences to static equivalences plus fairly standard bi-simulation conditions.

In this paper, we show that even though non-deducibility, static equivalence work well to obtain soundness results for the cases analyzed, they do not work well in other important cases, and a more flexible notion is needed. Our first contribution is that we define and study the useful formal notations, called the formal non-deducibility FNDR and formal indistinguishability relations FIR. We require five properties from any FNDR, and based on these properties an any initial set of relations which is a subset of $\mathcal{F}_c \times \mathcal{T}_c$ will generate a FNDR. In the similar way, four properties are required from any FIR, and through these properties an initial set of relations will generate a FIR. Each pair that is statically in-equivalent is also in-equivalent with respect to a formal indistinguishability relation. Moreover, non-deducibility is one instance of a FNDR, static equivalence is one instance of a FIR, respectively. We also propose the propositions to generate a FNDR and a FIR from a set of relations is a subset of closed frames and terms and a set of relations is a subset of closed frames.

Our second contribution is a general relation for bridging formal and computational models in the presence of a passive attacker. We define the notions of soundness and faithfulness of a cryptographic implementation with respect to equality, formal indistinguishability and formal (non-)deducibility relations. Soundness holds when a formal notion of security has a computational interpretation. For instance, formal indistinguishability relation tuples of messages (frames) should be computationally indistinguishable. Conversely, faithfulness holds when every formal attack on a given notion of security can be mapped to an efficient computational attacker. In order to test soundness with respect to a computational interpretation, it is enough to check soundness on a set of relations that generate the FNDR or FIR in question. If soundness holds on the generating set of relations, then soundness holds in total. As an illustration, we consider an equational theory modeling Abelian groups with exponents taken over a commutative ring. We show that the soundness of formal non-deducibility and indistinguishability relations are implied by the hardness of several classical problems in cryptography, notably some asymmetric encryption schemes. Although not completely surprising, this results illustrate well the expressive power of static equivalence defined over tailored equational theories. Besides introducing the above formal notions, we also make some other extensions in the theory of (non)-deducibility and static equivalence by providing some useful propositions on them.

Finally, our third contribution consists in generating the general framework for verifying the property security of an asymmetric encryption scheme. This general framework is based on the basic axioms on encryption primitives and by using the useful propositions to generate a FNDR and FIR from a set of pairs of closed frames and term a set of pairs of closed frames, respectively. If the soundness is hold in the initial sets to generate a FNDR, and a FIR, then it is still holds in total. After introducing the basic framework and proving some general propositions about FNDR, and FIR, we discuss three examples. The first is Bellare and Rogaway'93 [12] asymmetric encryption. Our second and third examples are REACT [13] and Pointcheval's Transformer [9], respectively.

Chapter 1

Two Views of Cryptography

1.1 The Formal Encryption and Equivalence

In this section we present the formal view of cryptography, specifically treating asymmetric encryption. In this formal setting, a set of *expressions* correspond to the messages that are transmitted during a cryptography protocol or the data which is processed in an encryption scheme. Encryption operates on the set of expressions, resulting new expressions. For example, the expression $\{M\}_K$ may represent an encrypted message, with plaintext M and the key K. All of $\{M\}_K, M$, and K are formal expressions, rather than sequences of bits. And various functions can be applied to such expressions, yielding other expressions. For example, decryption operation, which produces M from $\{M\}_K$ and K. In our formal approach for asymmetric encryption scheme, we concentrate on how to represent the output of an encryption scheme as a concept of *frame* based on the syntax of expressions. Then we explain a representation for the information available to an observer who has seen message exchanged in the course of a protocol execution or processes of an encryption scheme, the definitions and relations between the concepts of *deducibility, non-deducibility*, and *static equivalence*, which provide two formalizations of the knowledge that an attacker has on the basic of that information. Finally, we introduce the relating between formal and computational models and the soundness, faithfulness properties.

1.1.1 Abstract Algebras

Our abstract models - called *abstract algebras* consists of term algebras over a many sorted first order signature and equipped with equational theories. Most of the definitions here are adopted from the *applied pi calculus* [1, 2, 3]. A *signature* $\Sigma = (\mathcal{S}, \mathcal{F})$ consists of a countably infinite set of *sorts* with particular order $\leq_{\mathcal{S}}, \mathcal{S} = \{s, s_1, ...\}$ and a finite set of *function symbols*, $\mathcal{F} = \{f, f_1, ...\}$ together with arities of the form $ar(f) = s_1 \times ... \times s_k \rightarrow s, k \geq 0$. Symbols that take $k = 0$ as arguments are called *constants*. Given a signature Σ, a countably infinite set of names $\mathcal{N}$ and a countably infinite set of variables $\mathcal{X}$ such that $\mathcal{S}, \mathcal{F}, \mathcal{X}, \mathcal{N}$ are pairwise disjoint. We assume that both names and variables are sorted, that is, to each name or variable u, a subset $\mathcal{S}_u$ is assigned; we write $u : s$ and say u is of sort s whenever $s \in \mathcal{S}_u$. We require that $u : s_1$ and $s_1 \leq_{\mathcal{S}} s_2$ implies $u : s_2$, that means the subset $\mathcal{S}_u$ has a minimum denoted as $\mathbf{s}(u)$. For any subset U of the set of names or the set of variables, let $[U]_s = \{u \in U | \mathbf{s}(u) = s\}$. A renaming is a bijection $\tau : \mathcal{N} \rightarrow \mathcal{N}$ such that $\mathbf{s}(a) = \mathbf{s}(\tau(a))$. As usual, if a term T has sort s, we write $T : s$. Terms of sort s are defined by the grammar:

L,M,N,T,U,V ::=	*terms*
k,...,n,...,s	*name*
x,y,z	*variable*
$f(M_1, ..., M_l)$	*function application*
T ::=	*term of sort s*
$\|x$	*variable x of sort s*
$\|a$	*name a of sort s*
$\|f(T_1, ..., T_k)$	*application of symbol* $f \in F$

where f ranges over the function symbols of Σ and k matches the arity $ar(f) = s_1 \times ... \times s_k \rightarrow s'$, variables, names are of sort s, $s' \leq_{\mathcal{S}} s$, and each term T_i is of sort s_i for $i = 1, ..., k$. We denote *fnames(M)* and *var(T)* for the set of free names and the set of variables that occur in the term M, respectively. We use meta-variables *u,v,w* to range over names and variables. A term is closed if and only if it does not have any free variables (but it may contain names and constant symbols), that means $var(T) = \phi$.

The *size* of a term T denoted as $size|T|$ is defined as:

$$|u| = 1; |f(T_1, ..., T_k)| = 1 + \sum_{i=1}^{k} |T_i|.$$

The *DAG-size* $|T|_{DAG}$ is the number of distinct subterms of T. The set of all terms and closed terms will be denoted as $\mathcal{T}$ and $\mathcal{T}_c$, respectively.
For instance, assume that the the finite set of sorts $\mathcal{S}$ consists these sort $A, Hash$ and $Data$ such that $A, Hash \leq_{\mathcal{S}} Data,$. Then the term $T = H(a) \oplus m$, where $a : A, H(a) : Hash, m, T : Data$.

Definition 1 (Substitution) *A substitution σ is written as $\sigma = \{x_1 = T_1, ..., x_n = T_n\}$ with domain $dom(\sigma) = \{x_1, ..., x_n\}$.*

We only consider *well-sorted* substitutions, that is, substitution $\sigma = \{x_1 = T_1, ..., x_n = T_n\}$ for which x_i and T_i have the same sort. A substitution is called closed if and only if all of the terms T_i are closed. We let $var(\sigma) = \cup_i var(T_i), names(\sigma) = \cup_i fnames(T_i)$, and extend the notations var(.) and names(.) to tuples and set of terms and substitutions in the obvious way. The application of a substitution σ to a term T is written as $\sigma(T) = T\sigma$. If p is a position of T, the expression $T|_p$ denotes the subterm of T at the position p. The expression $T[T']_p$ denotes the term that is obtained after replacing the subterm in position p on T by T'.
Symbols in $\mathcal{F}$ are intended to model cryptographic primitives, whereas names in $\mathcal{N}$ are used to model secrets, that is, concretely random numbers. The abstract semantics of symbols is described by an equational theory E, that is an equivalent relation (denoted as $=_E$) which is stable with respect to application of contexts and well-sorted substitutions of variables. We further require that E is stable under substitution of names. And all the equational theories that we consider here satisfy these properties. For instance, symmetric and deterministic encryption in modeled by the theory E_{enc} generated by the classical equation $E_{enc} = \{dec(enc(x, y) =_{E_{enc}} x\}$. Or a trapdoor one-way function in modeled by the theory E generated by the equation $E = \{g(e, f(x, y)) =_E (x, y)\}$, where g, f, e are the inverse function of f, trapdoor one-way function, extra information, respectively.

1.1.2 Frames, Deducibility, and Equivalence Relation

We use frames [2, 5] to represent sequences of information or the output observed by an attacker when the encryption scheme is revoked. Formally, we have the definition of a frame as follows:

Definition 2 (Frame) *A frame is an expression of the form* $\varphi = \nu\widetilde{n}.\{x_1 = T_1, ..., x_n = T_n\}$ *where* $\widetilde{n}$ *is a set of restricted names or bounded names, and for each* i*,* T_i *is a term of the same sort as* x_i *and the name of* φ *is the free name of all terms* T_i*.*

A frame is closed frame if and only if all terms are closed. In what follows, we use $names(\varphi), fnames(\varphi)$ and $bnames(\varphi)$ to represent the *names, free names*, and *bounded names* of the frame φ, respectively. And the size of a frame $\varphi = \nu\widetilde{n}.\{x_1 = T_1, ..., x_n = T_n\}$ is $|\varphi| = \sum_{i=1}^{n} |T_i|$.
For a frame $\varphi = \nu\widetilde{n}.\{x_1 = T_1, ..., x_n = T_n\}$, if φ' is another frame, let $\varphi\varphi'$ denote the frame $\nu\widetilde{n} \cup names(\varphi').\{x_1 = T_1\varphi', ..., x_n = T_n\varphi'\}$. For frames $\varphi_1, ..., \varphi_n$ with disjoint domains, let $\{\varphi_1|\varphi_2|...|\varphi_n\}$ be the frame corresponding to the combination of all the substitutions of $\varphi_1, ..., \varphi_n$. Given two frames $\varphi = \nu\widetilde{n}.\{x_1 = T_1, ..., x_n = T_n\}, \varphi' = \nu\widetilde{n}.\{x_1 = T'_1, ..., x_n = T'_n\}$, and the equational theory E, we say that $\varphi =_E \varphi'$ if and only if $T_i =_E T'_i$ for all i. Obviously, we can see properties following: $\varphi =_E \varphi'$ implies $\psi\varphi =_E \psi\varphi'$ such that $var(\psi) \subseteq dom(\varphi, \varphi')$, $\varphi =_E \varphi'$ implies $\tau(\varphi) =_E \tau(\varphi')$ for every renaming τ.
Given the cipertext or the output of an encryption scheme, we would like to represent the knowledge of an attacker about the plaintext or secret information or some parts of them. One of possible approaches is use the concept of deducibility. First, we need to consider the definition of an equational theory E and an equivalence respect to the equational theory.

Definition 3 (Equational Theory.) *An equational theory for a given signature is an equivalence relation* $E \subseteq \mathcal{T} \times \mathcal{T}$ *(written as* $=_E$ *in infix notation) on the set of terms such that*
(i) $T =_E T'$ *implies* $T\sigma =_E T'\sigma$ *for every substitution* σ
(ii) $T_1 =_E T_2$ *implies* $T\{x = T_1\} =_E T\{x = T_2\}$ *for every term* T *and every variable* x
(iii) $T_1 =_E T_2$ *implies* $\tau(T_1) =_E \tau(T_2)$ *for every renaming* τ*.*

That means an equational theory is an equivalence relation on terms that is stable under substitution of terms for variables, application of contexts, and renaming.

Definition 4 (Equivalent) *We say that two terms* M *and* N *are equal in a frame* φ *for an equational theory* E*, and write* $(M =_E N)\varphi$*, if and only if*

$\varphi = \nu\widetilde{n}.\sigma, M\sigma =_E N\sigma$, and $\widetilde{n} \cap (fnames(M) \cup fnames(N)) = \phi$ for some names $\widetilde{n}$ and substitution σ.

Definition 5 (Deducibility) *A (closed) term T is deducible from a frame φ in an equational theory E, written $\varphi \vdash T$, if and only if there exists a term M such that $var(M) \subseteq dom(\varphi), fnames(M) \cap bnames(\varphi) = \phi$ and $(M =_E T)_\varphi$.*

Axiomatized by the rules.

$$\begin{array}{rl}
\dfrac{}{\nu\widetilde{n'}.\sigma \vdash T} & \text{if } \exists x \in dom(\sigma) \text{ such that } x.\sigma = T \\
\dfrac{}{\nu\widetilde{n'}.\sigma \vdash s} & \text{if } s \notin \widetilde{n'} \\
\dfrac{\varphi \vdash T_1 \ldots \varphi \vdash T_k}{\varphi \vdash f(T_1, \ldots, T_k)} & \text{where } f \in F \\
\dfrac{\varphi \vdash T \;\; T =_E T'}{\varphi \vdash T'} &
\end{array}$$

Definition 6 (Non-Deducibility) *We say that the (closed) term T is not deducible from the frame φ in the equational theory E if there does not exist any term M such that $fnames(M) \cap bnames(\varphi) = \phi, var(M) \subseteq dom(\varphi)$ and $(M =_E T)_\varphi$, denoted as $\varphi \nvdash T$.*

For instance, we consider the equivalent theory E_{enc} and the frame $\varphi_1 = \nu k_1.k_2.k_3.k_4.\{x_1 = enc(k_1, k_2), x_2 = enc(k_4, k_3), x_3 = k_3\}$. Therefore, the name k_4 is deducible from φ_1 since $dec(x_2, x_3)\varphi_1 =_{E_{enc}} k_4$ but neither k_1 nor k_2 are deducible.

Deducibility is not always sufficient to account for the knowledge of an attacker. For instance, it lacks partial information on secrets. Indeed, if we consider a naive vote protocol where agents simply send their vote (0, or 1) encrypted with some key, the security problem is not whether an attacker can learn the values of 0, or 1, but rather whether the attacker can tell the difference between a message that contains the vote 0 and a message that contains the vote 1. That is why another classical notion in formal methods is *static equivalence.*

Definition 7 (Statically Equivalent) *Two frames φ_1 and φ_2 are statically equivalent in an equational theory E, written as $\varphi_1 \approx_E \varphi_2$, if and only if*

(i) *dom*$(\varphi_1) =$ *dom*(φ_2);
(ii) *for all terms* M *and* N *such that* $fnames(M, N) \cap bnames(\varphi_1, \varphi_2) = \phi$ *and* $var(M, N) \subseteq dom(\varphi_1)$, $M\varphi_1 =_E N\varphi_1$ *is equivalent to* $M\varphi_2 =_E N\varphi_2$.

For instance, the two frames $\nu k.\{x = enc(0, k)\}$ and $\nu k.\{x = enc(1, k)\}$ are statically equivalent with respect to E_{enc}. However the two frames
$\nu k.\{x = enc(0, k), y = k\}$ and $\nu k.\{x = enc(1, k), y = k\}$
are not (consider the test $dec(x, y) =^? 0$), although the set of terms that can be deduced from both frames is the same (0, 1 are two constants known by the adversary). Other example is covering the Diffie-Hellmann Assumption, the two frames $\nu g.a.b.\{x_1 = g, x_2 = g^a, x_3 = g^b, x_4 = g^{ab})$ and $\nu g.a.b.c.\{x_1 = g, x_2 = g^a, x_3 = g^b, x_4 = g^c)$ are statically equivalent.

1.1.3 Concrete Semantics

We now give terms and frames a random oracle model by an implementation of the primitives. Provided a set of sorts $\mathcal{S}$ and a set of symbols $\mathcal{F}$ as a set of function symbols, a $(\mathcal{S}, \mathcal{F})$ is called a *computational algebra.* A *computational algebra* A consists of

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

Based on the *computational model* above, we will create a distribution $(\psi) = [[\varphi]]_A$ which is associated to each closed frame $\varphi = \nu\widetilde{n}.\{x_1 = T_1, ..., x_k = T_k\}$ and of which each drawing $\hat{\psi} \leftarrow^R (\psi)$ as following:

- for each name a of sort s appearing in these terms $T_1, ..., T_k$, draw a value $\hat{a} \leftarrow^R [[s]]_A$;

– for each variable $x_i(1 \leq i \geq k)$ of sort s_i, compute $\hat{T}_i \in [[s_i]]_A$ recursively on the structure of terms: $\widehat{f(T'_1, ..., T'_m)} = [[f]]_A(\hat{T'_1}, ..., \hat{T'_m})$;

– return the value $\hat{\psi} = \{x_1 = \hat{T'_1}, ..., x_k = \hat{T'_k}\}$.

– for each call $h(\hat{a})$ if the value a in the hash table then return the corresponding hash value. Otherwise, return randomly a value.

Such values $\phi = \{x_1 = e_1, ..., x_n = e_n\}$ with $e_i \in [[s_i]]_A$ are called *concrete frames.* We extend the notation $[.]_A$ to (sets of) closed terms in the obvious way. We also generalize the notation to terms or frames with variables that means they are not closed, by specifying the concrete values for all of them: $[[.]]_A, \{x_1 = e_1, ...x_n = e_n\}$. 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.

We forcus on asymptotic notions of cryptographic security and consider families of computational model A_η indexed by a complexity parameter or security parameter $\eta \geq 0$. This parameter might be thought as the size of keys and other secret values. The concrete semantics of a frame φ is a family of distributions over concrete frame $[[\varphi]]_{A_\eta}$. We only consider the computational model such that each required operation on models is feasible by a polynomial-time algorithm in the complexity parameter η. That means that the concrete frame is efficiently computable.

Families of distributions (ensembles) over concrete frames benefit from the usual notion of cryptographic indistinguishability. Intuitively, two families of distributions (ψ_η) and (ψ'_η) are *indistinguishable*, written as $(\psi_\eta) \approx (\psi'_\eta)$, if and only if any probabilistic polynomial-time adversary $\mathcal{A}$ can not guess whether she is given a sample from (ψ_η) or (ψ'_η) with a probability significantly greater than $\frac{1}{2}$. Formally, we ask the advantage of $\mathcal{A}$,

$Adv^{IND}(\mathcal{A}, \eta, (\psi_\eta), (\psi'_\eta)) = P[\hat{\psi} \leftarrow^R (\psi_\eta) : \mathcal{A}(\eta, \hat{\psi}) = 1] - P[\hat{\psi} \leftarrow^R (\psi'_\eta) : \mathcal{A}(\eta, \hat{\psi}) = 1]$.

to be a *negligible function* of the security parameter η, that is, to remain eventually smaller than any $\eta^{-n}(n > 0)$ for sufficiently η. A family of distributions (ψ_η) is *collision-free* with respect to the family of congruences $=_{A_\eta}$ iff the probability of collision between two random elements from (ψ_η), that is $P[e_1, e_2 \leftarrow^R (\psi_\eta) : e_1 =_{A_\eta} e_2]$ is a negligible function of η. Note that, this is equivalent to asking that the probability of sampling any e_0

from $(\psi_\eta), P[e \leftarrow^R (\psi_\eta) : e =_{A_\eta} e_0]$, is uniformly bounded from above by a negligible function of η.

1.2 The Computational View of Asymmetric Encryption Schemes

1.2.1 Asymmetric Encryption Schemes

The computational modeling of encryption schemes provides a much more detailed description of a cryptographic protocol than the formal language that we present in the previous section. It captures the fact that key generation and encryption is probabilistic, and it includes the fact that computers have limits in their computational power. Here, key generation algorithms are represented by random variables, messages are bit strings of finite length, and algorithms, like encryption, decryption, key generation process, must be computable in polynomial-time relative to a parameter is called "security parameter".
The field of actions here is the set of strings $:= \{0,1\}^*$. A fixed subset, *plaintext* $\subseteq$ *strings* represents the messages that are allowed to be encrypted. We fix an element 0 in *plaintext*. Another subset, *keys* $\subseteq$ *strings* is chosen for the possible encrypting keys. In order to be able to build up messages from basic ingredients, we assume that an injective pairing function is given:
$[.,.]$: *strings* $\times$ *strings* $\rightarrow$ *strings*. The range of the pairing function will be called *pairs*. A asymmetric encryption scheme is given by a triple of algorithms, $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ (see the figure following), where

Security parameter. A security parameter η ranges over all natural values. Computationally, it is a finite string that contains only bit 1, as many as its value. The purpose of security parameter is to measure the difficulty of computation. Function, defined in term of η are tested if they are computable in the time interval no larger than some polynomial function of η. In some encryption scheme, security parameter can be the length of the keys.

$\mathcal{K}$, Keys generation algorithm. Keys for encryption are assumed to be randomly generated. The random generation must be computable in

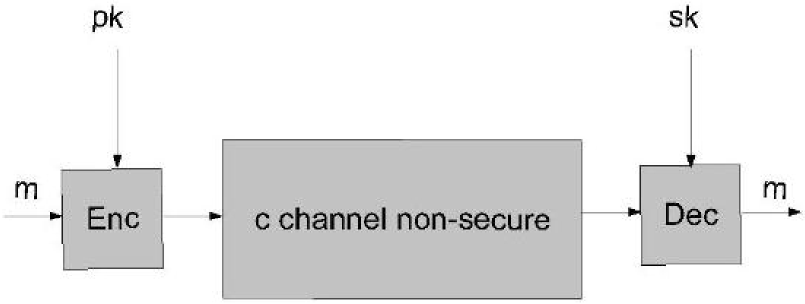

Figure 1.1: Asymmetric Encryption

polynomial-time with respect to the security parameter η. And returns randomly a pair (pk, sk) in the set $keys \times keys$, of matching public and secret keys.

$\mathcal{E}$, Encryption algorithm. is a probabilistic algorithm that takes a public key pk and a message x in *plaintext* to procedure a ciphertext y. The encryption of x using the public key pk as the encrypting key is a random variable over some discrete probability field. The values of this random variable are in *strings* and will be denoted as $\mathcal{E}_{pk}(x)$. We assume that this algorithm is polynomial-time computable in η whenever it is defined. And let $ciphers \subseteq strings$ is the set of all encryptions of $(x, pk) \subseteq plaintext \times keys$.

$\mathcal{D}$, Decryption algorithm. is a deterministic algorithm which takes a secret key sk and ciphertext y to produce either a message in *plaintext* or a special symbol *perp* to indicate that the ciphertext is invalid, and satisfying $\mathcal{D}_{sk}(\mathcal{E}_{pk}(x)) = x$ or $\perp$. Again $\mathcal{D}$ must be polynomial-time computable.

1.2.2 Definitions of Security

In the computational setting, we assume that an adversary has access to computers with limited computing power. The purpose of security is that an adversary should have very small probability of getting valuable information about encrypted messages, which is expressed mathematically as having little chance to tell different ciphers from apart. Namely, messages are random variables, since key generation and encryption is random; more exactly, they are sets of random variables (because of the security parameter), and the adversary is trying to distinguish these random sets. In order to express what it means to have little chance to distinguish two sets, we need the notion of *negligible function*:

Definition 8 (Negligible Function) *A function $\epsilon : \mathbf{N} \rightarrow \mathbf{R}$ is said to be negligible, if for any $c > 0$, there is a $n_c \in \mathbf{N}$ such that $\epsilon(\eta) \leq \eta^{-c}$ whenever $\eta \geq n_c$.*

This section provides formal definitions for the definitions of security of an asymmetric encryption discussed in previous section.

Experiments. We use standard notations and conventions for writing probabilistic algorithms and experiments. If A is a probabilistic algorithm, then $A(x_1, x_2, ...; r)$ is the result of running A on inputs $x_1, x_2, ...$ and coins r. We let $y \leftarrow A(x_1, x_2, ...)$ denote the experiment of picking r at random and letting y be $A(x_1, x_2, ...; r)$. If S is a finite set then $x \leftarrow S$ is the operation of picking an element uniformly from S. If α is neither an algorithm nor a set then $x \leftarrow \alpha$ is a simple assignment statement. We say that y *can be outputted by* $A(x_1, x_2, ...)$ if there is some r such that $A(x_1, x_2, ...; r) = y$. The formalizations that follow have a common framework that it may help to see at a high level first. In formalizing both indistinguishability and non-malleability we regard an adversary A as a pair of probabilistic algorithms, $A = (A_1, A_2)$. (We will say that A is polynomial-time if both A_1 and A_2 are.) This corresponds to A running in "‘two stages"’. The exact purpose of each stage depends on the particular adversarial goal, but for both goals the basic idea is that in the first stage the adversary, given the public key, seeks and outputs some test instance, and in the second stage the adversary is issued a challenge ciphertext y generated as a probabilistic function of the test instance, in a manner depending on the goal. (In addition A_1 can output some state information s that will be passed to A_2.) Adversary A is successful if she passes the challenge, with what "‘passes"’ means again depending on the goal. We consider three types of attacks under this setup. In a chosen-plaintext attack (CPA) the adversary can encrypt plaintexts of her choosing. Of course a CPA is unavoidable in the public-key setting: knowing the public key, an adversary can, on her own, compute a ciphertext for any plaintext she desires. So in formalizing definitions of security under CPA we do nothing beyond giving the adversary access to the public key; that's already enough to make a CPA implicit.

In a non-adaptive chosen-ciphertext attack (CCA1) we give A_1 (the public key) and access to a decryption oracle, but we do not allow A_2 access to a decryption oracle. This is sometimes called a non-adaptive chosen-ciphertext attack, in that the decryption oracle is used to generate the test instance, but taken away before the challenge appears.

In an adaptive chosen-ciphertext attack (CCA2) we continue to give A_1 (the public key) and access to a decryption oracle, but also give A_2 access to the same decryption oracle, with the only restriction that she cannot query the oracle on the challenge ciphertext y. This is an extremely strong attack model.

The number i in CCAi can be regarded as the number of adversarial stages during which she has access to a decryption oracle. Additionally, the bigger number corresponds to the stronger (and chronologically later) formalization. By the way: we do not bother to explicitly give A_2 the public key, because A_1 has the option of including it in s.

Indistinguishability of Encryptions. The classical goal of secure encryption is to preserve the privacy of messages: an adversary should not be able to learn from a ciphertext information about its plaintext beyond the length of that plaintext. We define a version of this notion, indistinguishability of encryption (IND), following, through a simple experiment. Algorithm A_1 is run on input the public key, pk. At the end of $A's$ execution she outputs a triple (x_0, x_1, s), the first two components being messages which we insist be of the same length, and the last being state information (possibly including pk) which she wants to preserve. A random one of x_0 and x_1 is now selected, say x_b. A challenge y is determined by encrypting x under pk. It is A_2's job to try to determine if y was selected as the encryption of x_0 or x_1 , namely to determine the bit b. To make this determination A_2 is given the saved state s and the challenge ciphertext y.

For concision and clarity we simultaneously define indistinguishability with respect to CPA, CCA1, and CCA2. The only difference lies in whether or not A_1 and A_2 are given decryption oracles. We let the string atk be instantiated by any of the formal symbols cpa, cca1, cca2, while ATK is then the corresponding formal symbol from CPA, CCA1, CCA2. When we say $\mathcal{O}_i = \epsilon$, where $i = 1, 2$, we mean $\mathcal{O}_i$ is the function which, on any input, returns the empty string, ϵ.

Definition 9 (IND-CPA, IND-CCA1, IND-CCA2) *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be an encryption scheme and let* $A = (A_1, A_2)$ *be an adversary. For atk in* $\{cpa, cca1, cca2\}$ *and* $k \in \mathbf{N}$ *let* $Adv^{ind-atk}_{A,\Pi}(k) =^{def} 2.Pr[(pk, sk) \leftarrow \mathcal{K}(1^\eta); (x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1}(pk); b \leftarrow \{0,1\}; y \leftarrow \mathcal{E}_{pk}(x_b) : A_2^{\mathcal{O}_2}(x_0, x_1, s, y) = b] - 1$
where
If $atk = cpa$ *then* $\mathcal{O}_1(.) = \epsilon$ *and* $\mathcal{O}_2(.) = \epsilon$
If $atk = cca1$ *then* $\mathcal{O}_1(.) = \mathcal{D}_{sk}(.)$ *and* $\mathcal{O}_2(.) = \epsilon$
If $atk = cca2$ *then* $\mathcal{O}_1(.) = \mathcal{D}_{sk}(.)$ *and* $\mathcal{O}_2(.) = \mathcal{D}_{sk}(.)$

We insist, above, that A_1 outputs x_0, x_1 with $|x_0| = |x_1|$. In the case of CCA2, we further insist that A_2 does not ask its oracle to decrypt y. We say that Π is secure in the sense of IND-ATK if A being polynomial-time implies that $Adv^{ind-atk}_{A,\Pi}(.)$ is negligible

1.3 Soundness and Faithfulness

The computational model of a cryptographic scheme is in a sense closer to reality than its formal representation by being a more detailed description. Therefore, the accuracy of a formal model can be characterized based on how close it is to the computational model. This is the reason that we introduce the notions of sound and faithful computational algebras with respect to the formal relations studied here: equality, static equivalence and deducibility. Let E be an equivalence theory and $R_1 \subseteq \mathcal{F}_c \times \mathcal{F}_c, R_2 \subseteq \mathcal{T}_c \times \mathcal{T}_c$, and $R_3 \subseteq \mathcal{F}_c \times \mathcal{T}_c$ are relations on closed frames, on closed terms, and relation on closed frames and terms, respectively. We denote R_1^c, R_2^c are the corresponding concrete relations. A family of computational algebras (A_η) is

- R_1-sound iff for every closed frames φ_1, φ_2 with the same domain such that $(\varphi_1, \varphi_2) \in R_1$ implies that for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is: $P[([[\varphi_1]]_{A_\eta}, [[\varphi_2]]_{A_\eta}) \in R_1^c]$ is non-negligible.

- R_1-faithful iff for every closed frames φ_1, φ_2 with the same domain such that $(\varphi_1, \varphi_2) \notin R_1$ implies that for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is: $P[([[\varphi_1]]_{A_\eta}, [[\varphi_2]]_{A_\eta}) \in R_1^c]$ is negligible.
- R_2-sound iff for every closed terms T_1, T_2 such that $(T_1, T_2) \in R_2$ implies that for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is: $P[\hat{e}_1, \hat{e}_2 \xleftarrow{R} [[T_1, T_2]]_{A_\eta} : (\hat{e}_1, \hat{e}_2)) \in R_2^c]$ is non-negligible.
- R_2-faithful iff for every closed terms T_1, T_2 such that $(T_1, T_2) \notin R_2$ implies that for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is: $P[\hat{e}_1, \hat{e}_2 \xleftarrow{R} [[T_1, T_2]]_{A_\eta} : (\hat{e}_1, \hat{e}_2)) \in R_2^c]$ is negligible.
- R_3-sound iff for every closed frame φ and term T such that $(\varphi, T) \in R_3$ implies that for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is: $P[\hat{\psi}, \hat{e} \xleftarrow{R} [[\varphi, T]]_{A_\eta} \hat{e}' \leftarrow \mathcal{A}(\eta, \hat{\psi}) : (\hat{e}', \hat{e})) \in R_2^c]$ is non-negligible.
- R_3-faithful iff for every closed frame φ and term T such that $(\varphi, T) \notin R_3$ implies that for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is: $P[\hat{\psi}, \hat{e} \xleftarrow{R} [[\varphi, T]]_{A_\eta} \hat{e}' \leftarrow \mathcal{A}(\eta, \hat{\psi}) : (\hat{e}', \hat{e})) \in R_2^c]$ is negligible.

Let E be the equivalence theory and a family of computational algebras (A_η) as above. The statements following are particular cases of the soundness and faithfulness as we have considered if we consider the concrete relations of $=_E$,$\approx_E$ and $\not\vdash$ in computational algebras (A_η) are $=_{A_\eta}, \approx$ and $\not\vdash_{A_\eta}$, respectively. The pair of concrete frame and term $(\hat{\psi}, \hat{e}) \in \not\vdash_{A_\eta}$ if there does not exist any concrete term $\hat{e}'$ of the term M' such that $fnames(M') \cap bnames(\varphi) = \phi; var(M') \subseteq dom(\varphi)$ and $\hat{e}' =_{A_\eta} \hat{e}$.

- $=_E$-sound iff for every frames φ_1, φ_2 with the same domain, $\varphi_1 =_E \varphi_2$ implies that $P[\hat{\psi}_1, \hat{\psi}_2 \xleftarrow{R} [[\varphi_1, \varphi_2]]_{A_\eta} : \hat{\psi}_1 =_{A_\eta} \hat{\psi}_2]$ is non-negligible;
- $=_E$-faithful iff for every frames φ_1, φ_2 with the same domain, $\varphi_1 \neq_E \varphi_2$ implies that $P[\hat{\psi}_1, \hat{\psi}_2 \xleftarrow{R} [[\varphi_1, \varphi_2]]_{A_\eta} : \hat{\psi}_1 =_{A_\eta} \hat{\psi}_2]$ is negligible;

The reason why we do not use adversaries in this definition. For example, would it not make more sense to define $=_E$-sound so that for each pair of closed frames φ_1 and φ_2 if $\varphi_1 =_E \varphi_2$ holds, then $[[\varphi_1]]_{A_\eta} \approx [[\varphi_2]]_{A_\eta}$, or for each pair of closed terms T_1 and T_2 if $T_1 =_E T_2$ holds, then $[[T_1, T_2]]_{A_\eta} \approx [[T_1, T_1]]_{A_\eta}$. However, using the fact that the advantage of an adversary trying to distinguish the two distributions cannot exceed the statical distance, it is easy to show that this definition would be equivalent to what is given above. These soundness definitions following are particular cases:

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

The soundness and faithfulness of formal non-deducibility relation and formal indistinguishability are introduced in next chapter.

Chapter 2

Formal Non-Deducibility and Formal Indistinguishability Relations

In this section, we propose a non-deducibility relation which is more flexible notion than non-deducibility that is defined in chapter 1. It is also necessary to fit a number of interesting cases for which non-deducibility is not appropriate. For instance, consider the property of a trapdoor one-way function. It is very difficult to capture its properties by using the deducibility. We can not find all the terms (about the argument) that an adversary can learn from the image of this function as $\nu a.b.\{x = f(a, b)\} \vdash a; \nu a.b.\{x = f(a, b)\} \vdash a \oplus c; \nu a.b.\{x = f(a, b)\} \vdash g(a, c)$ for any free symbol g and so on. Therefore, the use of non-deducibility is more suitable in the view of information security: non-deducibility represents the knowledge of an adversary that what he can not learn from the set of messages like $\nu a.\{x = f(a)\} \not\vdash a$. However, much more non-deducibility is allowed. For example, $\nu a.\{x = f(a)\} \not\vdash a; \nu a.\{x = f(a)\} \not\vdash a \oplus b$; and an infinitude of statements maybe not necessarily implies by the properties of a trapdoor one-way function. The analysis often goes in the other direction: the result is that not a given formal model has to be interpreted in a sound manner. We argue that a non-deducibility relation more useful is necessary. We call this type of relation is a formal non-deducibility relation (FNDR) which requires five properties from any FNDR, and through these properties an initial set of relations will generate a FNDR. Moreover, non-deducibility is one instance of FNDR. In order to test the sound property with respect to a computational interpretation, it is enough to check soundness on a set of relations that generate the FNDR in question. If soundness holds on the generating set of relations, then soundness holds in total. As in the work in [7, 6], the static equivalence does not work well in some important cases, and a more flexible notion is needed. For example, consider the Decisional Diffie-Hellman assumption. As Baudet et al. describe in [6], in an equivalent theory, 4-tuples (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c) are statically equivalent. Therefore, if the interpretation of the theory in certain computational group scheme is sound, then this scheme satisfies DDH assumption. However, formally much more is equivalent. For example, (g, g^a, g^b, ab) and (g, g^a, g^b, c) are also statically equivalent, and so on, an infinitude of statements not necessarily implied by the DDH assumption would be satisfied. Moreover, the analysis often goes in the other direction: not given formal model has to be interpreted in a sound manner, but for a given computational model we are looking for a formal theory that is simply, yet sound. That is how the formal indistinguishability relation (FIR) is formed. We require four properties from any FIR, and through these properties an initial set of relations will generate a FIR. In the similar way as the notion FNDR, to test soundness with respect to a computational interpretation, it is enough to check soundness on a set of relations that generate the FIR in question. If soundness holds on the generating set of relations, then soundness holds in total. And also statically equivalent is one instance of FIR.

2.1 Formal Non-Deducibility Relation

2.1.1 Weak Formal Non-Deducibility Relation

Definition 10 (wFNDR.) *A weak formal non-deducibility relation-wFNDR with respect to an equational theory E (written as $\nvDash_w$) is a relation on the set of closed frames and the set of closed terms such that for any closed frame φ and closed term M, if $\varphi \nvDash_w M$*

(i) Then $\tau(\varphi) \nvDash_w \tau(M)$, for any renaming τ;

(ii) And $M =_E N$ then $\varphi \nvDash_w N$;

(iii) And $\varphi =_E \varphi'$ then $\varphi' \nvDash_w M$;

(iv) for any frame φ_1 such that $var(\varphi_1) \subseteq dom(\varphi)$ and $names(\varphi_1) \cap bnames(\varphi) = \phi$ then $\varphi_1\varphi \not\models_w M$.

Remark 1 *Two frames $\varphi' = \nu\tilde{n}.\{x_i = T_i'\}, \varphi" = \nu\tilde{n}.\{x_i = T_i^{"}\}$, for all $i = 1, ..., k$, $\varphi' =_E \varphi"$ iff $T_i' =_E T_i^{"}, \forall i$. Note that we only consider two frames such that they have the same set of bound names. If φ_1, φ_2 are closed frames such that $dom(\varphi_1) \cap dom(\varphi_2) = \phi$, and $names(\varphi_2) \cap bnames(\varphi_1) = \phi$ and $\varphi_1 \not\models_w M, \varphi_2 \not\models_w M$, then $\{\varphi_1 | \varphi_2\} \not\models_w M$.*

The reason is following. If $dom(\varphi_1) = \{x_1, ..., x_k\}$, then let $\psi = \{x_1 = x_1, ..., x_k = x_k | \varphi_2\}$. Since $var(\psi) = \{x_1, ..., x_k\} \subseteq dom(\varphi_1); names(\psi) \cap bnames(\varphi_1) = names(\varphi_2) \cap bnames(\varphi_1) = \phi$. Using property *(iv)*, it follows that $\psi\varphi_1 = \{\varphi_1 | \varphi_2\} \not\models_w M$.

We propose here some useful propositions of a weak formal non-deducibility, the proposition of soundness is also proved.

Proposition 1 *Non-Deducibility relation $\nvdash$ is a weak formal non-deducibility relation $\not\models_w$ with respect to the equational theory E.*

Proof. We will show that $\nvdash$ satisfies the properties of a weak formal non-deducibility relation. First, we show that these properties *(i), (ii)*, and *(iii)* are satisfied by $\nvdash$. By the definition of non-deducibility, for every closed frame φ and closed term M such that $\varphi \nvdash M$, we have $\tau(\varphi) \nvdash \tau(M)$. For any frame φ and closed terms M and N such that $\varphi \nvdash M$ and $M =_E N$ then $\varphi \nvdash N$ duce to the transitive property of the equivalent theory E. And with any frames φ, φ' and closed terms M such that $\varphi \nvdash M$ and $\varphi =_E \varphi'$ then $\varphi' \nvdash M$ because for any term T if $T\varphi =_E M$ then $T\varphi' =_E M$.
Let frames φ, φ_1 and a closed term M as in *(iv)*. We have to show that if $\varphi_1 \nvdash M$ then $\varphi\varphi_1 \nvdash M$. Assume that $\varphi\varphi_1 \vdash M$, so by the definition of deducibility relation, there exists a term T such that $var(T) \subseteq dom(\varphi\varphi_1)$ and $fnames(T) \cap bnames(\varphi\varphi_1) = fnames(T) \cap (bnames(\varphi) \cup names(\varphi_1)) = \phi$. This implies $fnames(T) \cap bnames(\varphi_1) = \phi$. And $T(\varphi\varphi_1) =_E M$. Consider term $T\varphi$, we have $fnames(T\varphi) \cap bnames(\varphi_1) = (fnames(T) \cup names(\varphi)) \cap bnames(\varphi_1) = \phi; var(T\varphi) \subseteq var(\varphi) \subseteq dom(\varphi_1)$. And $T(\varphi\varphi_1) =_E (T\varphi)\varphi_1 =_E M$. Therefore, $\varphi_1 \vdash M$. Contradiction. Therefore, $\varphi\varphi_1 \nvdash M$. That means $\nvdash$ satisfies the property (iv).

□

Proposition 2 *The intersection of an arbitrary number of weak formal non-deducibility relations with respect to the same equational theory E is a weak formal non-deducibility relation.*

Proof. Let $(\not\models_{w,i})_{i \in I}$, where I is some indexing set, be a sequence of weak formal non-deducibility relations with respect to the same equational theory E, and let $(\not\models_w)$ be their intersection. We will show that $(\not\models_w)$ satisfies the properties *(iv)*. Let φ, φ_1 be as in *(iv)*. Because $(\varphi_1, M) \in (\not\models_{w,i})$, so $\varphi_1 \not\models_{w,i} M; \varphi\varphi_1 \not\models_{w,i} M$ for all i, then $\varphi_1 \not\models_w M; \varphi\varphi_1 \not\models_w M$. In the similar way, we can prove that $(\not\models_w)$ satisfies also the other properties.

□

Proposition 3 *Consider a set $\tilde{S} \subseteq \mathcal{F}_c \times \mathcal{T}_c$. If $S \subseteq \tilde{S}$ is a relation on a closed frame and a term. Then there is a unique smallest subset $\langle S \rangle_{wFNDR} \subseteq \tilde{S}$ containing S, such that $\langle S \rangle_{wFNDR}$ is a weak formal non-deducibility relation with respect to the equivalent theory E. We can generate the $\langle S \rangle_{wFNDR}$ like that. Let*

$$\langle S \rangle_{wFNDR} := \begin{cases} (\varphi', M') \in \mathcal{F}_c \times \mathcal{T}_c \mid \exists \varphi, \psi, M \textit{ such that } (\varphi, M) \in S, \\ \varphi' =_E \tau(\psi\varphi), M' =_E \tau(M) \textit{ where} \\ names(\psi) \cap bnames(\varphi) = \phi, var(\psi) \subseteq dom(\varphi) \end{cases}$$

For instance, we consider an example to show how a frame ψ is constructed such that $var(\psi) \subseteq dom(\varphi)$ and $names(\psi) \cap bnames(\varphi) = \phi$. This frame can be constructed from the closed frames in the set S. For example, assume that $(\varphi_2, M) \in S$ such that $names(\varphi_1) \cap names(\varphi_2) = \phi$. Then we can construct $\psi = \{\varphi_1 | x_1, ..., x_k\}$, where $\{x_1, ..., x_k\} = dom(\varphi_2)$. Therefore, $(\varphi' = \psi\varphi_2, M) \in \langle S \rangle_{wFNDR}$. That means $(\{\varphi_1 | \varphi_2\}, M) \in \langle S \rangle_{wFNDR}$.

Proof. For the first statement, we will show the existence of the smallest set. We call the set $S' = \{S" \mid S \subseteq S"$ with $S"$ is a wFNDR$\}$. Then the smallest set $\hat{S}$ is the intersection of all the sets in S'. By the proposition 2, $\hat{S}$ is a wFNDR. By the definition of the construction of $\langle S \rangle_{wFNDR}$, it is clear that $S \subseteq \langle S \rangle_{wFNDR}$. We will show that $\langle S \rangle_{wFNDR}$ is a $wFNDR$.

That means we have to show that $\langle S\rangle_{wFNDR}$ satisfies all the properties of a *wFNDR*. By the generation of $\langle S\rangle_{wFNDR}$, we can see that it satisfies the properties *(i), (ii), (iii)* of a weak formal non-deducibility relation. So we have to show that it will satisfy the property *(iv).* Let φ is a frame such that $var(\varphi) \subseteq dom(\varphi_1), names(\varphi) \cap bnames(\varphi_1) = \phi$, and (φ_1, M) in $\langle S\rangle_{wFNDR}$ then we show that $(\varphi\varphi_1, M)$ also in $\langle S\rangle_{wFNDR}$. Because (φ_1, M) in $\langle S\rangle wFNDR$, the form is $\varphi_1 =_E \tau(\psi\varphi')$ and $M =_E \tau(M')$ such that (φ', M') in S with the conditions $var(\psi) \subseteq dom(\varphi')$ and $names(\psi) \cap bnames(\varphi') = \phi$. We can see that $names(\varphi) \cap bnames(\varphi') = \phi$, because $bnames(\varphi_1) = bnames(\psi) \cup bnames(\varphi')$. Consider the frame $\varphi\psi$, we have $names(\varphi\psi) \cap bnames(\varphi') \subseteq [names(\varphi) \cup names(\psi)] \cap bnames(\varphi') = \phi$. By the condition of the frame φ, $var(\varphi) \subseteq dom(\varphi_1)$ and $dom(\varphi_1) = dom(\psi)$, so $var(\varphi\psi) \subseteq var(\psi)$. Moreover, $var(\psi) \subseteq dom(\varphi')$. That means $var(\varphi\psi) \subseteq dom(\varphi')$. The pair of a closed frame and a term $(\varphi\varphi_1 =_E (\varphi\psi)\varphi', M =_E M')$ with the pair of closed frame and term (φ', M') in S. Therefore, $(\varphi\varphi_1, M)$ also in $\langle S\rangle_{wFNDR}$. Therefore, $\hat{S} \subseteq \langle S\rangle_{wFNDR}$. Consider any pair of closed frame and term $(\varphi', M') \in \langle S\rangle_{wFNDR}$, by the generation, we see that $\forall S" \subseteq S', (\varphi', M') \in S"$. That implies $\langle S\rangle_{wFNDR} \subseteq \hat{S}$.

□

Proposition 4 *Let a computational algebra that is $=_E -$sound. Let $S \subseteq \tilde{S}$ is a relation on closed frames and terms such that S is sound. Then the weak formal non-deducibility relation $\langle S\rangle_{wFNDR}$ is sound with respect to the equational theory E.*

First, we consider the definition of the soundness of $\langle S\rangle_{wFNDR}$. This definition is a particular case of the soundness definition in the section soundness and faithfulness in the chapter 1.

Definition 11 *$\langle S\rangle_{wFNDR}$-sound if and only if for every pair of a closed frame and a term (φ, M) in $\langle S\rangle_{wFNDR}$ implies that for every probabilistic polynomial-time adversary $\mathcal{B}$, its advantage $P[\hat{\phi}, \hat{e} \xleftarrow{R} [[\varphi, M]]_{A_\eta}; \hat{e'} \xleftarrow{R} \mathcal{B}(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$ is negligible.*

Proof. To show $\langle S\rangle_{wFNDR}$-sound, we will show that all pairs of a closed frame and term implies for any probabilistic polynomial-time adversary whose advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, M]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{A}(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$ is negligible. Let (φ', M') is any pair of a closed frame and term in $\langle S \rangle_{wFNDR}$. By the definition of the generation there exists a pair $(\varphi, M) \in S$ and a term ψ with $names(\psi) \cap bnames(\varphi) = \phi; var(\psi) \subseteq dom(\varphi)$, $\varphi' =_E \tau(\psi\varphi), M' =_E \tau(M)$. Because two families of distributions $[[\psi\varphi]]_{A_\eta}$ and $[[\tau(\psi\varphi)]]_{A_\eta}$ are the same. And the soundness of $=_E$. Therefore, to show (φ', M') is sound equivalent to show that $(\psi\varphi, M)$ is sound. We will show that for any frame φ_1, closed term M and any frame φ such that $var(\varphi) \subseteq dom(\varphi_1); names(\varphi) \cap bnames(\varphi_1) = \phi$. For any probabilistic polynomial-time adversary $\mathcal{A}$ whose advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_1, M]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{A}(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$ is negligible implies $P[\hat{\phi'}, \hat{e} \leftarrow^R [[\varphi\varphi_1, M]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}(\eta, \hat{\phi'}) : \hat{e'} =_{A_\eta} \hat{e}]$ is negligible for any probabilistic polynomial-time adversary $\mathcal{B}$. Suppose that $\mathcal{B}$ can deduce the closed term M from the frame $\varphi\varphi_1$ with the advantage $P[\hat{\phi'}, \hat{e} \leftarrow^R [[\varphi\varphi_1, M]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}(\eta, \hat{\phi'}) : \hat{e'} =_{A_\eta} \hat{e}]$ is non-negligible. This gives the adversary $\mathcal{A}$ can deduce the closed term M from φ_1 in a polynomial-time algorithm: Given the concrete frame $\hat{\phi}, \hat{e}$ are sampled from the family distribution $[[\varphi_1, M]]_{A_\eta}$. The adversary $\mathcal{A}$ interprets the frame φ using the values, specified by $\hat{\phi}$ for the variables in φ. All these variables are assigned a unique values of $\hat{\phi}$ is sampled from φ_1 since $var(\varphi) \subseteq dom(\varphi_1)$. $\mathcal{A}$ constructs a concrete frame $\hat{\sigma}$ and runs $\mathcal{B}(\eta, \hat{\sigma})$. Then the output is $\mathcal{B}$'s output. The family of distribution of $\hat{\sigma}$ is exactly the family of distribution $[[\varphi\varphi_1]]_{A_\eta}$. Therefore, the advantage of $\mathcal{A}$ equals the advantage of $\mathcal{B}$, which is non-negligible. In addition, $\mathcal{A}$ runs in probabilistic polynomial-time since the size of encoding of φ is constant in η, so the concrete frame $\hat{\sigma}$ can computed in probabilistic polynomial-time. Contradiction. Therefore, $P[\hat{\phi'}, \hat{e} \leftarrow^R [[\varphi\varphi_1, M]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}(\eta, \hat{\phi'}) : \hat{e'} =_{A_\eta} \hat{e}]$ is negligible for any probabilistic polynomial-time adversary $\mathcal{B}$.

□

2.1.2 Formal Non-Deducibility Relation

Definition 12 (FNDR.) *A formal non-deducibility relation-FNDR with respect to an equational theory E (written as $\not\models$) is a relation on the set of pairs of a closed frame and a closed term such that $\not\models$ is a wFNDR and satisfies (v) for any free symbol g and $\varphi \not\models g(T_1, ..., T_k)$ then there exists some terms*

T_i, with $i \in \{1, ..., k\}$ such that $\varphi \not\models T_i$.

Proposition 5 *Let the set pairs of closed frames and terms S is a wFNDR, and $\langle S\rangle^{(v)}$ is the set of all the possible extensions R on S with respect to the property: if $(\varphi, g(T_1, ..., T_k)) \in R$, where g is any free symbol in $\mathcal{F}$, then $(\varphi, T_i) \in R$ for some subterms T_i. These extensions are formal non-deducibility relations. If S is sound then there exist some extension r in $\langle S\rangle^{(v)}$ on S which is sound.*

For instance, we will consider an example of the extensions, let S is a *wFNDR*:
$S = \{(\varphi, a), (\varphi_1, b), (\varphi_2, g(g_1(c, d), e))\}$
Then the extensions on S with respect to the property above are:
$\{S \cup \{(\varphi_2, g_1(c, d)), (\varphi_2, c)\}\}$;
$\{S \cup \{(\varphi_2, g_1(c, d)), (\varphi_2, d)\}\}$;
$\{S \cup \{(\varphi_2, g_1(c, d)), (\varphi_2, c), (\varphi_2, d)\}\}$;
$\{S \cup \{(\varphi_2, e\}\}$;
$\{S \cup \{(\varphi_2, g_1(c, d)), (\varphi_2, c), (\varphi_2, e)\}\}$;
$\{S \cup \{(\varphi_2, g_1(c, d)), (\varphi_2, d), (\varphi_2, e)\}\}$;
$\{S \cup \{(\varphi_2, g_1(c, d)), (\varphi_2, c), (\varphi_2, d), (\varphi_2, e)\}\}$.
And there is at least one of these extensions is sound if the wFNDR S is sound.

Lemma 1 *Let S is a wFNDR such that there is one pair $(\varphi, g(a_1, ..., a_k)) \in S$, where g is any free symbol in $\mathcal{F}$, and we make extensions in the same way as in the proposition. Then there exists some extension which is sound.*

Proof. For the first statement, the extensions are formal non-deducibility relations: The extensions satisfy the properties *(i),(ii),(iii),(iv)* because the set S is a wFNDR. And by the definition of the extensions, it is obviously to see that they satisfy the property *(v)*. To prove the second statement, first, we prove the lemma above. The reason is that: if we assume that all of the extensions are not sound. That means every pairs of closed frames and terms (φ, a_i) in each extensions satisfies, $(\varphi \not\models a_i)$ implies that there is a polynomial-time adversary A_i whose advantage is $P[\hat{\phi}, \hat{e} \xleftarrow{R} [[\varphi, a_i]]_{A_\eta}; \hat{e'} \xleftarrow{R} A_i(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$ is non-negligible. We construct an adversary B who can deduce all subterms a_i with the advantage of B is non-negligible: Given the concrete

frame $\hat{\phi}$ of φ, and η, B runs $A_i(\eta, \hat{\phi}), i = 1, ..., k$ and the output is $a_1, ..., a_k$(we assume that the number of subterms which are names is no larger than some polynomial function of security parameter η). Otherwise, the function g is computable in polynomial-time algorithm, so in polynomial-time algorithm, the adversary B can construct the term $g(a_1, ..., a_k)$ with his advantage is non-negligible. Contradiction, that means there exists some extensions which is sound. If we apply this lemma to the set S consisting pairs of closed frames and terms. These pairs have form $(\varphi, g(T_1, ..., T_k))$. We can obtain what we want to prove.
Now, we show that these extensions are formal non-deducibility relation. By the generation of this extension, it is obviously to see that it satisfies the properties $(i), (ii), (iii), (iv)$ because the set S is a *wFNDR*. We have to show that these extensions satisfy the property (v). For any pair $(\varphi, g(T_1, ..., T_k))$ in each of these extensions, then there are some pairs $(\varphi, T_i), i \in \{1, ..., k\}$ with (φ, T_i) in this extension. That is what we want to prove.

□

These useful propositions following are also reserved for formal non-deducibility relation.

Proposition 6 *Deducibility relation $\nvdash$ is a formal non-deducibility relation $\not\models$ with respect to the equational theory E.*

Proof. We will show that $\nvdash$ satisfies the properties of a formal non-deducibility relation. First, we show that these properties *(i), (ii), (iii), (iv)* are satisfied by $\nvdash$ (see the proof in the section of weak formal non-deducibility relation). Only the property *(iv)* remain. Assume that $\varphi \nvdash g(T_1, ..., T_k)$, then there exists some subterms T_i such that $\varphi \nvdash T_i$. We assume that there is not any subterms such that $\varphi \nvdash T_i$, duce to the free symbols g in $\mathcal{F}$ is computable, hence $\varphi \vdash g(T_1, ..., T_k)$. Contradiction.

□

2.2 Formal Indistinguishability Relation

As Gergei Bana, Payman Mohassel, and Till Stegers mention in [8], the statically equivalent relation does not work well in some importance cases, and a more flexible notion is needed. They argue that an equivalence relation finer than static equivalence is necessary to fit a number of interesting cases for which static equivalence is not suitable. We will call this type of equivalence relation a formal indistinguishability relation. This equivalence relation is defined as follows:

2.2.1 Definition

Definition 13 *A formal indistinguishability relation with respect to an equational theory E is an equivalence relation $\cong$ on the set of closed frames such that*
(i) $\varphi_1 \cong \varphi_2$ if $dom(\varphi_1) = dom(\varphi_2)$;
(ii) for any frame φ, if φ_2 are closed frames such that $var(\varphi) \subseteq dom(\varphi_i)$, $names(\varphi) \cap bnames(\varphi_i) = \phi$ and $\varphi_1 \cong \varphi_2$ then $\varphi\varphi_1 \cong \varphi\varphi_2$;
(iii) for any two frames $\varphi' = \{x_i = T'_i\}_{i=1,...n}$ and $\varphi" = \{x_i = T"_i\}_{i=1,...n}$, if $T'_i =_E T"_i$ for all i, then $\varphi' \cong \varphi"$; moreover, $\varphi' \not\approx_E \varphi"$ implies $\varphi' \ncong \varphi"$;
(iv) for any renaming $\tau, \tau(\varphi) \cong \varphi$.

Remark 2 *Corresponding sections of equivalent frames are equivalent. That is, for example, if $\varphi_1 = \nu\widetilde{n}.\{x_i = T_i\}_{i=1,...,4} \cong \varphi_2 = \nu\widetilde{n}.\{x_i = T'_i\}_{i=1,...,4}$ then $\{x_2 = T_2, x_4 = T_4\} \cong \{x_2 = T'_2, x_4 = T'_4\}$. This follows from (ii) by setting $\varphi = \nu\theta.\{x_2 = x_2, x_4 = x_4\}$.*
If $\varphi_1, \varphi_2, \varphi'_1, \varphi'_2$ are frames such that $dom(\varphi_1) \cap dom(\varphi_2) = \phi, dom(\varphi'_1) \cap dom(\varphi'_2) = \phi, names(\varphi_2) \cap bnames(\varphi_1) = \phi, names(\varphi'_2) \cap bnames(\varphi'_1) = \phi$ and $\varphi_i \cong \varphi'_i$, then $\{\varphi_1|\varphi_2\} \cong \{\varphi'_1|\varphi'_2\}$. The reason is the following: Choose a renaming τ such that $\tau(\varphi_1) = \varphi_1, \tau(\varphi'_1) = \varphi'_1, \tau(\varphi'_2) = \varphi'_2$ and $names(\tau(\varphi_2)) \cap bnames(\varphi_1) = names(\tau(\varphi_2)) \cap bnames(\varphi'_1) = \phi$. This can be done because we assumed that there are infinitely many names of each sort. Using (iv) we see that $\{\varphi_1|\varphi_2\} \cong \tau(\{\varphi_1|\varphi_2\}) = \{\varphi_1|\tau(\varphi_2)\}$. If $dom(\varphi_1) = dom(\varphi'_1) = \{x_1, ..., x_k\}$, then let $\psi = \{x_1 = x_1, ..., x_k = x_k|\tau(\varphi_2)\}$. Using (ii), it follows that $\{\varphi_1|\tau(\varphi_2)\} = \psi\varphi_1 \cong \psi\varphi'_1 = \{\varphi'_1|\tau(\varphi_2)\}$. Since by (iv) again $\tau(\varphi_2) \cong \varphi_2$ and $\varphi_2 \cong \varphi'_2$ by assumption, $\tau(\varphi_2) \cong \varphi'_2$ holds , and applying (ii) in a similar fashion as above, we obtain $\{\varphi'_1|\tau(\varphi_2)\} \cong \{\varphi'_1|\varphi'_2\}$. Putting all these together, $\{\varphi_1|\varphi_2\} \cong \{\varphi'_1|\varphi'_2\}$

2.2.2 Useful Propositions on FIR

The following useful proposition on FIR are introduced in [8].

Proposition 7 *Static equivalence $\approx_E$ is a formal indistinguishability relation with respect to the equational theory E.*

Proof. *See the appendix.*

Proposition 8 *The intersection of an arbitrary number of formal indistinguishability relations (with respect to the same equational theory E) is a formal indistinguishability relation.*

Proof. *See the appendix*

Proposition 9 *Consider static equivalence as a subset $\tilde{E} \subseteq \mathcal{F}_c \times \mathcal{F}_c$. If $S \subseteq \tilde{E}$, then there is an unique smallest $\langle S \rangle_{\cong} \subseteq \tilde{E}$ is a formal indistinguishability relation with respect to the equivalent theory E. $\langle S \rangle_{\cong}$ can be generated in the following way: Let*

$$S' := \begin{cases} (\varphi', \varphi") \in \mathcal{F}_c \times \mathcal{F}_c | \varphi' = \varphi\{\varphi_1^{'}|...|\varphi_n^{'}\}, \varphi" = \varphi\{\varphi_1^{"}|...|\varphi_n^{"}\} \\ such\ that\, bnames(\varphi) = \phi\ and\ for\ all\, i = 1, ..., n, \\ (\varphi', \varphi") \in S,\ or(\varphi", \varphi') \in S,\ or\varphi" =_E \tau_i(\varphi') for\ some\ renaming\, \tau_i. \end{cases}$$

and $\langle S \rangle_{\cong}$ is the transitive closure of S'.

Proof. *See the appendix.*

The computational model of a cryptographic scheme is in a sense closer to reality than its formal representation by being more detailed description. Therefore the accuracy of a formal model can be characterized based on how close it is to the computational model. More specifically, how formal and computational indistinguishability relate to each other via the interpretation. The most important concepts to describe this are given in the following definition.

Definition 14 *Let A be a computation algebra, and let $\cong$ be a formal indistinguishability relation on the set of frames, and let $F \subseteq \mathcal{F}_c$. We say that the computational algebra A is $\cong$-sound on F if for every closed pair* *of frames $\varphi_1, \varphi_2 \in F, \varphi_1 \cong \varphi_2$ implies that $[[\varphi_1]]_{A_\eta} \approx [[\varphi_2]]_{A_\eta}$. A is $\cong$-complete on F if for every closed pair of frames $\varphi_1, \varphi_2 \in F, \varphi_1 \ncong \varphi_2$ implies that $[[\varphi_1]]_{A_\eta} \not\approx [[\varphi_2]]_{A_\eta}$. A is $\cong$-faithful on F if for every closed pair of frames $\varphi_1, \varphi_2 \in F, \varphi_1 \ncong \varphi_2$ implies that the statistical distance is not negligible and there is a probabilistic polynomial-time adversary $\mathcal{A}$ such that $|Adv_\eta^{\mathcal{A}}([[\varphi_1]]_{A_\eta}, [[\varphi_2]]_{A_\eta}) - \Delta([[\varphi_1]]_{A_\eta}, [[\varphi_2]]_{A_\eta})|$ is negligible. For all three notions, we adopt the convention that if no such set F is mentioned, it is assumed that $F = \mathcal{F}_c$.*

Proposition 10 *Let A be a computational algebra that is $=_E$-sound. Suppose $S \subseteq \widetilde{E}$ is a binary relation on closed frames such that $(\varphi, \psi) \in S$ implies $[[\varphi]]_{A_\eta} \approx [[\psi]]_{A_\eta}$. Then $[[\varphi]]_{A_\eta} \approx [[\psi]]_{A_\eta}$whenever $\varphi \cong \psi$. That is, A is $\cong$-sound.*

Proof. *See the appendix.*

Chapter 3

Useful Propositions, Axioms for Encryption primitives

We prove here some useful propositions of *deducibility relation, non-deducibility* and *static equivalence relation.* These propositions allow us see that non-deducibility and statically equivalent relations are formal non-deducibility and formal indistinguishability relations, respectively. Moreover, assume that we have a set of pairs of closed frames and terms such that each pairs in this set satisfies $\varphi \nvdash T$ then we apply these propositions to extend this set. These useful propositions ensure that the result is a formal non-deducibility relation (FNDR). In the similar way, assume that we have a set of pairs of frames such that every pairs of frames satisfies $\varphi_1 \approx_E \varphi_2$ then after applying these useful propositions to extend this set. These useful propositions ensure that the result is a formal indistinguishability relation (FIR). Finally, we introduce some basic axioms for general encryption primitives and show that these axioms are sound.

3.1 Useful Propositions

3.1.1 Useful Propositions on Deducibility Relation

Proposition 11 *Let a closed frame and term such that $\varphi \vdash T$. For any renaming $\tau, \tau(\varphi) \vdash \tau(T)$.*

Proof. We have $\varphi \vdash T$, by the definition of the deduction concept, there exists a term M such that: $var(M) \subseteq dom(\varphi)$; $fnames(M) \cap bnames(\varphi) = \phi$; $(M =_E T)_\varphi$. Since $\tau(M\varphi) =_E \tau(T); fnames(\tau(M)) \cap bnames(\tau(\varphi)) = \phi$ and $var(M) \subseteq dom(\varphi)$. So we can conclude that $\tau(\varphi) \vdash \tau(T)$.

□

Proposition 12 *Let a closed frame and term such that $\varphi \vdash T$. For any renaming closed term $T' =_E T, \varphi \vdash T'$.*

Proof. We have $\varphi \vdash T$, by the definition of the deduction concept, there exists a term M such that: $var(M) \subseteq dom(\varphi)$; $fnames(M) \cap bnames(\varphi) = \phi$; $(M =_E T)_\varphi$. Since $M\varphi =_E T =_E T'; fnames(M)) \cap bnames(\varphi) = \phi$ and $var(M) \subseteq dom(\varphi)$. So we can conclude that $\varphi \vdash T'$.

□

Proposition 13 *Let two frames φ_1 and φ_2 such that $\varphi_1 =_E \varphi_2$. For any (closed) term T. If $\varphi_1 \vdash T$ then $\varphi_2 \vdash T$.*

Proof. We have $\varphi_1 \vdash T$, by the definition of the deduction concept, there exists a term M such that: $var(M) \subseteq dom(\varphi_1)$; $fnames(M) \cap bnames(\varphi_1) = \phi$; $(M =_E T)_{\varphi_1}$. Since $\varphi_1 =_E \varphi_2; fnames(M) \cap bnames(\varphi_2) = \phi$ and $var(M) \subseteq dom(\varphi_2)$. Therefore,$(M =_E T)_{\varphi_1}$ implies $(M =_E T)_{\varphi_2}$. So we can conclude that $\varphi_2 \vdash T$.

□

Proposition 14 *Let two frames φ and closed frame φ_1 such that $var(\varphi) \subseteq dom(\varphi_1); bnames(\varphi_1) \cap names(\varphi) = \phi$. For any (closed) term T. If $\varphi_1 \vdash T$ then $\varphi\varphi_1 \vdash T$.*

Proof. We have to show that if $\varphi_1 \vdash T$ then $\varphi\varphi_1 \vdash T$. Since $\varphi_1 \vdash T$, so by the definition of deducibility relation, there exists a term M such that $var(M) \subseteq dom(\varphi_1)$ and $fnames(M) \cap bnames(\varphi_1) = \phi$. And $M(\varphi_1) =_E T$. Consider term $M\varphi$, we have $fnames(M\varphi) \cap bnames(\varphi_1) = (fnames(M) \cup names(\varphi)) \cap bnames(\varphi_1) = \phi; var(M\varphi) \subseteq var(\varphi) \subseteq dom(\varphi_1)$. And $M(\varphi\varphi_1) = (M\varphi)\varphi_1 =_E T$. So, $\varphi\varphi_1 \vdash T$.

□

Proposition 15 *Let two frames φ_1 and φ_2. For any (closed) term T. If $\varphi_1 \vdash T; dom(\varphi_1) \cap dom(\varphi_2) = \phi; bnames(\varphi_1) \cap names(\varphi_2) = \phi$ then $\{\varphi_1 | \varphi_2\} \vdash T$.*

Proof. Let M be a term such that $var(M) \subseteq dom(\{\varphi_1|\varphi_2\}); fnames(M) \cap (bnames(\varphi_1) \cup bnames(\varphi_2) = \phi$, we will prove that $(M =_E T)\{\varphi_1|\varphi_2\}$. We have $dom(\{\varphi_1|\varphi_2\}) = dom(\varphi_1) \cup dom(\varphi_2)$, implies $var(M) \subseteq (dom(\varphi_1) \cup dom(\varphi_2))$ and $dom(\varphi_1) \cap dom(\varphi_2) = \phi$, so

$$\begin{aligned} M\{\varphi_1|\varphi_2\} &= (M\varphi_1)\varphi_2 \\ &= (M\varphi_2)\varphi_1 \\ &= (M\{x_i = T_i\})\varphi_1 \end{aligned}$$

Let a term $M_1 = M\{x_i = T_i\}$. That means we replace all the variables x_i of the term M such that $x_i \in var(\varphi_2)$. Because $bnames(\varphi_1) \cap names(\varphi_2) = \phi$, so $fnames(M_1) = (fnames(M) \cup names(\varphi_2)) \cap bnames(\varphi_1) = \phi$. The term M_1 satisfies: $var(M_1) \subseteq dom(\varphi_1)$; $fnames(M_1) \cap bnames(\varphi_1) = (fnames(M) \cup names(\varphi_2)) \cap bnames(\varphi_1) = \phi$; $M\{\varphi_1|\varphi_2\} =_E T$. And T is a closed term, $T\{\varphi_1|\varphi_2\} = T$. That means $M\{\varphi_1|\varphi_2\} = T\{\varphi_1|\varphi_2\}$. We can conclude that $\{\varphi_1|\varphi_2\} \vdash T$.

□

Proposition 16 *Let two frames φ_1 and φ_2 such that $dom(\varphi_1) \cap dom(\varphi_2) = \phi$ and $names(\varphi_2) \cap bnames(\varphi_1) = \phi$. For any (closed) term T. If $\{\varphi_1|\varphi_2\} \vdash T$; then $\varphi_1 \vdash T$ or $\varphi_2 \vdash T$.*

Proof. There exists a term M such that: $var(M) \subseteq (dom(\varphi_1) \cup dom(\varphi_2))$; $fnames(M) \cap (bnames(\varphi_1) \cup bnamse(\varphi_2)) = \phi$; $M\{\varphi_1|\varphi_2\} =_E T$. We consider three cases following:

(i) $var(M) \subseteq dom(\varphi_1)$

Consider $M\{\varphi_1|\varphi_2\} =_E (M\varphi_1)\varphi_2 =_E M\varphi_1$ duce to $dom(\varphi_1) \cap dom(\varphi_2) = \phi$ and $var(M) \subseteq dom(\varphi_1)$ As the properties of the term M above, we have: $var(M) \subseteq dom(\varphi_1)$; $fnames(M) \cap bnames(\varphi_1) = \phi$; $M\varphi_1 =_E T$. That means $\varphi_1 \vdash T$.

(ii) $var(M) \subseteq dom(\varphi_2)$

In the similar way, we have $M\{\varphi_1|\varphi_2\} =_E (M\varphi_2)\varphi_1 =_E M\varphi_2$ and the term M satisfies:
$var(M) \subseteq dom(\varphi_2)$; $fnames(M) \cap bnames(\varphi_2) = \phi$; $M\varphi_2 =_E T$. This implies $\varphi_2 \vdash T$.
(iii) $dom(\varphi_i) \subset var(M) \subseteq (dom(\varphi_1 \cup dom(\varphi_2))$
$M\{\varphi_1|\varphi_2\} =_E T \leftrightarrow (M\{x_i = T_i\})\varphi_1 =_E T$. $M\{x_i = T_i\}$ means that we replace all variables x_i of the term M such that $x_i \in var(\varphi_2)$ by the substitution of the frame φ_2. If we choose $M_1 = M\{x_i = T_i\}$,so $var(M_1) \subseteq dom(\varphi_1)$ and $fnames(M_1) \cap bnames(\varphi_1) = \phi$ since $fnames(M) \cap bnames(\varphi_1) = \phi$ and $names(\varphi_2) \cap bnames(\varphi_1) = \phi$. The term M_1 satisfies:
$var(M_1) \subseteq dom(\varphi_1)$; $fnames(M_1) \cap bnames(\varphi_1) = \phi$; $M_1\varphi_1 =_E T$. This implies $\varphi_1 \vdash T$.

□

Proposition 17 *Let a closed frame and term such that $\varphi \not\vdash T$. For any renaming $\tau, \tau(\varphi) \not\vdash \tau(T)$.*

Proof. Duce to renaming is bijection so if we assume that $\tau(\varphi) \vdash \tau(T)$, then apply the proposition 11, this implies $\varphi \vdash T$. Contradiction.

□

Proposition 18 *Let a closed frame and term such that $\varphi \not\vdash T$. For any closed term $T' =_E T, \varphi \not\vdash T'$.*

Proof. We assume that $\varphi \vdash T'$, by applying the proposition 12, this implies $\varphi \vdash T$. Contradiction.

□

Proposition 19 *Let two frames φ_1 and φ_2 such that $\varphi_1 =_E \varphi_2$. For any (closed) term T. If $\varphi_1 \not\vdash T$ then $\varphi_2 \not\vdash T$.*

Proof. We assume that $\varphi_2 \vdash T$. By the definition of deduction, there exists a term M such that:
$fnames(M) \cap bnames(\varphi_2) = \phi$; $var(M) \subseteq dom(\varphi_2)$; $(M =_E T)\varphi_2$. Since $\varphi_1 =_E \varphi_2$. This implies that:

$var(M) \subseteq dom(\varphi_1)$; $fnames(M) \cap bnames(\varphi_1) = \phi$; $(M =_E T)\varphi_1$. That is $\varphi_1 \vdash T$. Contradiction, therefore,we have $\varphi_2 \nvdash T$

□

Proposition 20 *Let two frames φ and closed frame φ_1 such that $var(\varphi) \subseteq dom(\varphi_1); bnames(\varphi_1) \cap names(\varphi) = \phi$. For any (closed) term T. If $\varphi_1 \nvdash T$ then $\varphi\varphi_1 \nvdash T$.*

Proof. We have to show that if $\varphi_1 \nvdash T$ then $\varphi\varphi_1 \nvdash T$. Assume that $\varphi\varphi_1 \vdash T$, so by the definition of deducibility relation, there exists a term M such that $var(M) \subseteq dom(\varphi\varphi_1)$ and $fnames(M) \cap bnames(\varphi\varphi_1) = fnames(M) \cap (bnames(\varphi) \cup names(\varphi_1)) = \phi$. This implies $fnames(M) \cap bnames(\varphi_1) = \phi$. And $M(\varphi\varphi_1) =_E T$. Consider term $M\varphi$, we have $fnames(M\varphi) \cap bnames(\varphi_1) = (fnames(M) \cup names(\varphi)) \cap bnames(\varphi_1) = \phi; var(M\varphi) \subseteq var(\varphi) \subseteq dom(\varphi_1)$. And $M(\varphi\varphi_1) = (M\varphi)\varphi_1 =_E T$. Therefore, $\varphi_1 \vdash T$. Contradiction, so, $\varphi\varphi_1 \nvdash T$.

□

Proposition 21 *Let two frames φ_1 and φ_2 such that $dom(\varphi_1) \cap dom(\varphi_2) = \phi$ and $names(\varphi_2) \cap bnames(\varphi_1) = \phi$. For any (closed) term T. If $\varphi_1 \nvdash T; \varphi_2 \nvdash T$ then $\{\varphi_1|\varphi_2\} \nvdash T$.*

Proof. We assume that $\{\varphi_1|\varphi_2\} \vdash T$. As the proposition 16 above, we have $\varphi_1 \vdash T$ or $\varphi_2 \vdash T$. Contradiction, therefore, $\{\varphi_1|\varphi_2\} \nvdash T$.

□

Proposition 22 *Let two frames φ_1 and φ_2. For any (closed) term T. If $\varphi_1 \nvdash T, \varphi_2 \nvdash T$ and there exists a frame φ_3 such that $\varphi_2 =_E \varphi_3$ with then $\{\varphi_1|\varphi_2\} \nvdash T$.*

Proof. This proposition is the lemma of proposition 13, proposition 21 and the lemma following

Let four frames $\varphi_1, \varphi_1^{'}, \varphi_2, \varphi_2^{'}$. If $\varphi_1 =_E \varphi_1^{'}, \varphi_2 =_E \varphi_2^{'}$ then $\{\varphi_1|\varphi_2\} =_E \{\varphi_1^{'}|\varphi_2^{'}\}$.

Apply the proposition 21 for these frames φ_1 and φ_3, the result is $\{\varphi_1|\varphi_3\} \nvdash$

T. Then we apply the proposition 27 for these frames φ_1, φ_2 and φ_3, we have two frames $\{\varphi_1|\varphi_2\} =_E \{\varphi_1|\varphi_3\}$. Finally, applying the proposition 19 for two frames $\{\varphi_1|\varphi_2\}$ and $\{\varphi_1|\varphi_3\}$, and the result is exactly what we had to prove to see that $\{\varphi_1|\varphi_2\} \not\vdash T$.

□

Proposition 23 *Let two frames φ_1 and φ_2 with $dom(\varphi_1) \cap dom(\varphi_2) = \phi; names(\varphi_1) \cap names(\varphi_2) = \phi$. For any (closed) term T. If $\{\varphi_1|\varphi_2\} \not\vdash T$ then $\varphi_1 \not\vdash T$ and $\varphi_2 \not\vdash T$.*

Proof. We assume that $\varphi_1 \vdash T$ or $\varphi_2 \vdash T$. By the proposition 15, we can have $\{\varphi_1|\varphi_2\} \vdash T$. Contradiction, therefore, we can conclude that $\varphi_1 \not\vdash T$ and $\varphi_2 \not\vdash T$.

□

3.1.2 Useful Propositions on Equivalent Relation

Proposition 24 *Static equivalence $\approx_E$ is a equivalent relation $R \subseteq F_c \times F_c$ with respect to an equational theory E. That is $\approx_E$ satisfies three properties: reflexity, symmetry, and transitivity.*

Proof. We will prove that $\approx_E$ relation satisfies three properties above
(i) Reflexity
For any frame φ, with every two terms M and N such that $var(M) \subseteq dom(\varphi), var(N) \subseteq dom(\varphi), fnames(M, N) \cap bnames(\varphi) = \phi$. It is obviously that $(M =_E N)\varphi$ is equivalent to $(M =_E N)\varphi$. This implies $\varphi \approx_E \varphi$.
(ii) Symmetry
For any two frames φ_1 and φ_2, such that $\varphi_1 \approx_E \varphi_2$. Duce to $\varphi_1 \approx_E \varphi_2$, so with every two terms *M, N*,
$var(M) \subseteq dom(\varphi_i), i = 1, 2$; $var(N) \subseteq dom(\varphi_i), i = 1, 2$; $fnames(M, N) \cap (bnames(\varphi_1 \cup bnames(\varphi_2)) = \phi$; $dom(\varphi_1) = dom(\varphi_2)$; $(M =_E N)\varphi_1 \leftrightarrow (M =_E N)\varphi_2$. Therefore, with the property of the equivalent relation, for every two term *M, N*, it satisfies $(M =_E N)\varphi_2 \leftrightarrow (M =_E N)\varphi_1$ or $\varphi_2 \approx_E \varphi_1$.
(iii) Transitivity
Let φ_1, φ_2 and φ_3 be three frames such that $\varphi_1 \approx_E \varphi_2$ and $\varphi_2 \approx_E \varphi_3$. We

will prove that $\varphi_1 \approx_E \varphi_3$. For every frames M, N be two frames such that:
$var(M,N) \subseteq dom(\varphi_i), i = 1,2,3$
$fnames(M,N) \cap (bnames(\varphi_1) \cup bnames(\varphi_2) \cup bnames(\varphi_3)) = \phi$.
Since we have $\varphi_1 \approx_E \varphi_2$ so $(M =_E N)\varphi_1$ is equivalent $(M =_E N)\varphi_2$ and $\varphi_2 \approx_E \varphi_3$ implies $(M =_E N)\varphi_2$ is equivalent $(M =_E N)\varphi_3$. This is obviously to see that $(M =_E N)\varphi_1$ is equivalent $(M =_E N)\varphi_3$. And that is exactly what we want to prove, that is $\varphi_1 \approx_E \varphi_3$.

□

Proposition 25 *Let τ is an any renaming function. For every frame φ, then $\tau(\varphi) \approx_E \varphi$.*

Proof. To prove this proposition, we construct another renaming τ' in the following: On the $bnames(\varphi)$, let τ' be equal τ, and on N $(bnames(\varphi) \cup \tau(bnames(\varphi))$, let τ' be the identity map. We will have to define τ' on the domain $\tau(bnames(\varphi)) \backslash bnames(\varphi)$. Since τ is a sort-preserving bijection, the number of elements in the domain $\tau(bnames(\varphi))$ $bnames(\varphi)$ is the same as the number of elements in $bnames(\varphi)$ $\tau(bnames(\varphi))$ for each sort s. Both are $|bnames(\varphi)| - |bnames(\varphi) \cap \tau(bnames(\varphi))|$, which equals $|\tau(bnames(\varphi))| - |bnames(\varphi) \cap \tau(bnames(\varphi))|$. So on the domain $\tau(bnames(\varphi)) \setminus bnames(\varphi)$ choose τ' to be any bijection to the domain $bnames(\varphi) \setminus \tau(bnames(\varphi))$. It is then easy to see that τ' is a sort-preserving bijection on N, and that $\tau'(\varphi) = \tau(\varphi)$ for the frame φ. Moreover, for any term M that shares no names with φ and $\tau(\varphi), \tau'(M) = M$, and therefore $M\tau(\varphi) = M\tau'(\varphi) = \tau'(M\varphi)$ holds. Hence, for any two terms M and N such that $fnames(M,N) \cap (bnames(\varphi) \cup bnames(\tau(\varphi))) = \phi$, $M\tau(\varphi) =_E N\tau(\varphi)$ if and only if $\tau'(M\varphi) =_E \tau'(N\varphi)$ which happends. Since τ' is a bijection - if and only if $M\varphi =_E N\varphi$, and $\tau(\varphi) approx_E \varphi$ follows.

□

Proposition 26 *Let two frames φ_1 and φ_2. And φ is a (closed) frame with $var(\varphi) \subseteq dom(\varphi_i) = \phi, i = 1,2$ and $names(\varphi) \cap bnames(\varphi_i) = \phi$. And if $\varphi_1 \approx_E \varphi_2$ then $\varphi\varphi_1 \approx_E \varphi\varphi_2$.*

Proof. Let M, N be terms whose variables are included in $dom(\varphi\varphi_1)$, duce to $var(\varphi) \subseteq dom(\varphi_i), i = 1, 2$ so $dom(\varphi\varphi_1) = dom(\varphi\varphi_2)$, that is $var(M, N) \subseteq dom(\varphi\varphi_2)$. And M, N have no names in common with $\varphi\varphi_i, i = 1, 2$. Then $fnames(M\varphi) = fnames(M) \cup names(\varphi)$, and $fnames(M) \cup names(\varphi)$ is disjoint from $bnames(\varphi_i)$ by the assumption on M and condition of the proposition. Therefore, $fnames(M\varphi)$ and $bnames(\varphi_i)$ are disjoint (and likewise for N).

If $\varphi_1 \approx_E \varphi_2$ holds, then by the definition of static equivalence, $(M\varphi)\varphi_1 =_E (N\varphi)\varphi_1$ if and only if $(M\varphi)\varphi_2 =_E (N\varphi)\varphi_2$. Therefore, $M(\varphi\varphi_1) =_E N(\varphi\varphi_1)$ if and only if $M(\varphi\varphi_2) =_E N(\varphi\varphi_2)$, and that is exactly what we want to prove to see that $\varphi\varphi_1 \approx_E \varphi\varphi_2$.

□

Proposition 27 *Let four frames $\varphi_1, \varphi_1^{'}, \varphi_2$ and $\varphi_2^{'}$ such that $dom(\varphi_1) \cap dom(\varphi_2) = \phi, dom(\varphi_1^{'}) \cap dom(\varphi_2^{'}) = \phi, names(\varphi_1) \cap names(\varphi_2) = \phi$ and $names(\varphi_1^{'}) \cap names(\varphi_2^{'}) = \phi$. If $\varphi_1 \approx_E \varphi_1^{'}$ and $\varphi_2 \approx_E \varphi_2^{'}$ then $\{\varphi_1|\varphi_2\} \approx_E \{\varphi_1^{'}|\varphi_2^{'}\}$.*

Lemma 2 *Let 3 frames $\varphi, \varphi_1, \varphi_2$ such that $dom(\varphi) \cap dom(\varphi_1) = \phi; dom(\varphi) \cap dom(\varphi_2) = \phi; names(\varphi) \cap names(\varphi_1) = \phi; names(\varphi) \cap names(\varphi_2) = \phi$. If $\varphi_1 \approx_E \varphi_2$, then $\{\varphi|\varphi_1\} \approx_E \{\varphi|\varphi_2\}$.*

Proof. Choose a renaming τ such that $\tau(\varphi_1) = \varphi_1; \tau(\varphi_1^{'}) = \varphi_1^{'}; \tau(\varphi_2^{'}) = \varphi_2^{'}; \tau(\varphi_2)$ and $names(\tau(\varphi_2)) \cap names(\varphi_1) = names(\tau(\varphi_2)) \cap names(\varphi_1^{'}) = \phi$. This can be done because we assumed that there are infinitely many names of each sort.

Using the proposition 25, we see that $\{\varphi_1|\varphi_2\} \approx_E \tau(\{\varphi_1|\varphi_2\}) = \{\varphi_1|\tau(\varphi_2)\}$. Duce to $\varphi_1 \approx_E \varphi_1^{'}$ so $dom(\varphi_1) = dom(\varphi_1^{'}) = \{x_1, ..., x_k\}$, then let the frame $\psi = \{x_1 = x_1, ..., x_k = x_k|\tau(\varphi_2)\}$. We see that $var(\psi) \subseteq dom(\varphi_1), dom(\varphi_1^{'})$ and $names(\psi) \cap (names(\varphi_1) \cup names(\varphi_1^{'})) = names(\tau(\varphi_2)) \cap (names(\varphi_1) \cup names(\varphi_1^{'}) = \phi$,then using the proposition 26 for three frames $\psi, \varphi_1, \varphi_1^{'}$, it follows that $\{\varphi_1|\tau(\varphi_2)\} = \psi\varphi_1 \approx_E \psi\varphi_1^{'} = \{\varphi_1^{'}|\tau(\varphi_2)\}$.

Since $\varphi_2 \approx_E \varphi_2^{'}$ and $\varphi_2 \approx_E \tau(\varphi_2)$, therefore, $\tau(\varphi_2) \approx_E \varphi_2^{'}$. Due to $\tau(\varphi_2) \approx_E \varphi_2^{'}$ so $dom(\varphi_2) = dom(\varphi_2^{'}) = \{x_1, ..., x_t\}$, then let the frame $\psi' = \{x_1 = x_1, ..., x_t = x_t|\varphi_1^{'}\}$. It is easy to see that:

$var(\psi') \subseteq dom(\tau(\varphi_2)), dom(\varphi_2^{'}); names(\psi') \cap (names\tau(\varphi_2) \cup names(\varphi_2^{'})) =$

$names(\varphi_1^{'}) \cap names\tau(\varphi_2) \cup names(\varphi_2^{'})) = \phi$
Then using the proposition 26 again for three frames $\psi', \tau(\varphi_2)$ and $\varphi_2^{'}$, it results that $\{\varphi_1^{'}|\tau(\varphi_2)\} = \psi'\tau(\varphi_2) \approx_E \psi'\varphi_2^{'} = \{\varphi_1^{'}|\varphi_2^{'}\}$. Putting all these together, $\{\varphi_1|\varphi_2\} \approx_E \{\varphi_1^{'}|\varphi_2^{'}\}$.

□

3.2 Basic Axioms on Encryption Primitives

In this section,we will show basic axioms on encryption primitives such that *random assignment, xor function, concatenation function, hash function*, and *trapdoor one-way permutation function* [11, 10, 9, 18], the proofs are put in the appendix. These axioms present a general set of pairs of frames or frames and closed terms whose frames and closed terms under an equivalent theory E. And then, we show that these axioms are FNDR and FIR, sound under the condition that the equivalent theory E is sound. Based on these axioms and applying of the propositions and lemmas in the section of formal indistinguishability and non-deducibility relations, we can verify asymmetric encryption schemes automatically. We first establish an equivalent theory E.
Consider the signature $\Sigma = (\mathcal{S}, \mathcal{F})$ consists of the set of sorts and the set of free symbols:
$\mathcal{S} = \{A, G, Hash, Img, Cipher, Key, Data\}$
$\mathcal{F} = \{0, 1, 1_G, 1_A, +, -, ., *, exp, \oplus, cons, head, tail, nil, h, f, g\}$.
To establish the equivalent theory E, we concentrate on abelian groups G with exponents taken over a commutative ring A. Consider the following equational theory to model a commutative group with exponentiation (as in [6]). Let A and G be sorts, and let $\mathcal{F}$ contains the following function symbols:

$* : G \times G \to G$	$- : A \to A$
$1_G : G$	$. : A \times A \to A$
$+ : A \times A \to A$	$1_A : A$
$0 : A$	$exp : G \times A \to G$

To simplify the notation, we write U^V for $exp(U, V)$. And the formal model consists of term algebras over these sets of sorts and function symbols and equipped with the equational theory who is generated from the set of equations as follows:

$u + v = v + u$

$u + (v + w) = (u + v) + w$

$u + 0_A = u$

$u + (-u) = 0_A$

$u.v = v.u$

$u.(v.w) = (u.v).w$

$u.1_A = u$

$(u + v).w = u.w + v.w$

To model the exclusive or function. Let $Data$ be a sort and we consider the infix symbol in $\mathcal{F}$ $\oplus : Data \times Data \rightarrow Data$ and two constants $0, 1 : Data$. And the equations following are equipped with the equational theory E:

$(x \oplus y) \oplus z = x \oplus (y \oplus z) \quad x \oplus y = y \oplus x$

$x \oplus x = 0 \quad x \oplus 0 = x$

And the computational algebras $A_\eta, \eta \geq 0$:

- the concrete domain $[[s]]_{A_\eta}$ is the set of bit-string of length $\eta, \{0, 1\}^\eta$ with the uniform distribution;

- $\oplus$ is interpreted by the usual XOR function over $\{0, 1\}^\eta$;

- $[[0]]_{A_\eta} = 0^\eta$ and $[[1]]_{A_\eta} = 1^\eta$

Then to model the concatenation function. Let $Key, Cipher$ be sorts such that $Key, Cipher \leq_{\mathcal{S}} Data$, and the following function symbols:

$\vert\vert : Data \times Data \rightarrow Data$	pairing constructor
$head : Data \rightarrow Data$	head of a pair
$tail : Data \rightarrow Data$	tail of a pair
$nil : List_0$	empty Data
$0, 1 : Data$	constants

The set of equations following are equipped with the equational theory E:

$dec(enc(x, y), y) = x \quad enc(nil, x) = nil$

$enc(dec(x, y), y) = x \quad dec(nil, x) = nil$

$head(||(x, y)) = x \quad tail(x) = nil$

$tail(||(x, y)) = y \quad ||(head(x), tail(x)) = x$

And the concrete meaning of sorts end function symbols is given by the computational algebras A defined as follows:

- the carrier sets are $[[Data]]_{A_\eta} = \{0, 1\}^k$ equipped with the uniform distribution and the usual equational relation
- enc, dec are implemented by a cipher for data of the particular size and keys of the size k

- $[[nil]]_{A_\eta}$ is the empty bit-string, $[[const]]_{A_\eta}$ is the usual concatenation, $[[0]]_{A_\eta} = 0^k, [[1]]_{A_\eta} = 1^k, [[head]]_{A_\eta}$ returns the first k digits of bit-strings, whereas $[[tail]]_{A_\eta}$ returns the last k digits.

To model the hash and trapdoor one-way permutation function symbols. Let $Hash, Img$ be sorts such that $Hash, Img \leq_{\mathcal{S}} Data$. And the function symbols following are in the set $\mathcal{F}$:

$h : Data \rightarrow Hash$	hash function
$f : Data \rightarrow Img$	trapdoor one-way permutation
$f : Data \times Data \rightarrow Img$	partially trapdoor one-way permutation
$g : Keys \times Img \rightarrow Data$	(partially) invert trapdoor one-way permutation

And the equations following are equipped with the equational theory E:

$$g(f(x)) = x \quad g(f(x, y)) = x$$

And the concrete meaning of sorts end function symbols is given by the computational algebras A defined as follows:

- g are implemented by a cipher for data of the particular size and keys of the size k
- $[[Hash]]_{A_\eta}, [[Img]]_{A_\eta} = \{0, 1\}^k \leq_{\mathcal{S}} Data$ are equipped with the uniform distribution and usual equational relation.
- $[[h]]_{A_\eta}, [[f]]_{A_\eta}, [[g]]_{A_\eta}$ are the usual hash, trapdoor one-way permutation and its invert.

Observe that we did not include the symbol for the invert hash function in the language. The reason is that computing a from $h(a)$ is not feasible for any adversary. One the set of sorts is set, the set of function symbols and the computational group scheme is set, the computational interpretation of this signature is straightforward.

3.2.1 Random generation

We consider a *random assignment* like this νa, in π - calculus that means creating a fresh name a. It is that it declares a new unique name a, distinct from all external names, for use in the process. Based on the propositions above, we propose a set of specific axioms following which are sound:

(RD1) $\nu a.\theta \not\models a.$

(RE1) $\nu a.\{x = a\} \cong \nu r.\{x = r\}.$

3.2.2 Xor function

The following basic axioms are sound for *xor function*:

(XD1) $\nu\widetilde{n}.\sigma \not\models T$, then $\nu\widetilde{n}.\nu a.\{\sigma|x = a \oplus T\} \not\models T$, such that $a \notin (\widetilde{n} \cup fnames(T))$.

(XE1) $\nu\widetilde{n}.a.\{\sigma|x = a \oplus T\} \cong \nu\widetilde{n}.r.\{\sigma|x = r\}$, such that $a \notin (\widetilde{n} \cup fnames(T))$.

3.2.3 Concatenation function

The following basic axioms are served for *concatenation function* and sound:

(CD1) $\varphi \not\models T$, then $\varphi \not\models T \parallel T', \forall T' \in \mathcal{T}_c$.

(CE1) $\nu a.b.\{x = a \parallel b\} \cong \nu r.\{x = r\}$.

3.2.4 Hash function

The following basic axioms are of *hash function* are sound:

(HD1) $\varphi \not\models T$, $\{\varphi|x = h(T)\} \not\models T$ such that $h(T)$ does not appear in φ.

(HE1) $\varphi \not\models T$, $\{\varphi|x = h(T)\} \cong \{\varphi|\nu r.\{x = r\}\}$ such that $h(T)$ does not appear in φ.

3.2.5 One-way function

The following basic axioms are sound and served for *one-way permutation function*:

(OD1) $\nu a.\{x = f(a)\} \not\models a$.

(OE1) $\nu a.\{x = f(a)\} \cong \nu r.\{x = r\}$.

If f is a partially one-way permutation function, then these basic axioms are sound:

(OD1') $\nu a.b.\{x = f(a||b)\} \not\models a$.

(OE1') $\nu a.b.\{x = f(a||b)\} \cong \nu r.\{x = r\}$.

The following rules are consequent:

(OD2) $\nu\widetilde{n}.\sigma \not\models T$, then $\nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\} \not\models a$.

(OE2) $\nu\widetilde{n}.\sigma \not\models T$, then $\nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\} \cong \nu\widetilde{n}.\nu r.\{\sigma|x = r\}$.

Chapter 4

Applications

Now, we apply the framework that developed in chapter 2 and the axioms for encryption primitives in chapter 3 to prove automatically the secure properties (indistinguishability chosen plaintext attack - IND-CPA) of some asymmetric encryption schemes. To do this we propose the general framework as follows: Let two sets S_d, S_e, where the first one consists pairs of closed frames and terms such that every pair (φ, T) such that $fnames(T) \subseteq names(\varphi)$, is sound that means it implies for any probabilistic polynomial-time adversary $\mathcal{B}$, its advantage $P[\hat{\phi}, \hat{e} \xleftarrow{R} [[\varphi, T]]_{A_\eta}; \hat{e'} \xleftarrow{R} \mathcal{B}(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$ is negligible. And the second one consists pairs of closed frames such that every pair (φ_1, φ_2) such that $dom(\varphi_1) = dom(\varphi_2)$, is sound that means it implies for any probabilistic polynomial-time adversary $\mathcal{B}$, its probability that distinguishes two frames is negligible. To create these sets we consider these axioms for encryption primitive. And then, we apply the propositions in chapter 2 to generate a formal non-deducibility relation and a formal indistinguishability relation to show the secure properties of an asymmetric encryption scheme (see the figure following). In these schemes, we consider these function H and G as hash functions, both assumed to be ideal random functions [14], and the function f as trapdoor one-way permutation function or partially trapdoor one-way permutation function, where k is a security parameter
$H : \{0,1\}^k \rightarrow Y; G : X \rightarrow \{0,1\}^k$

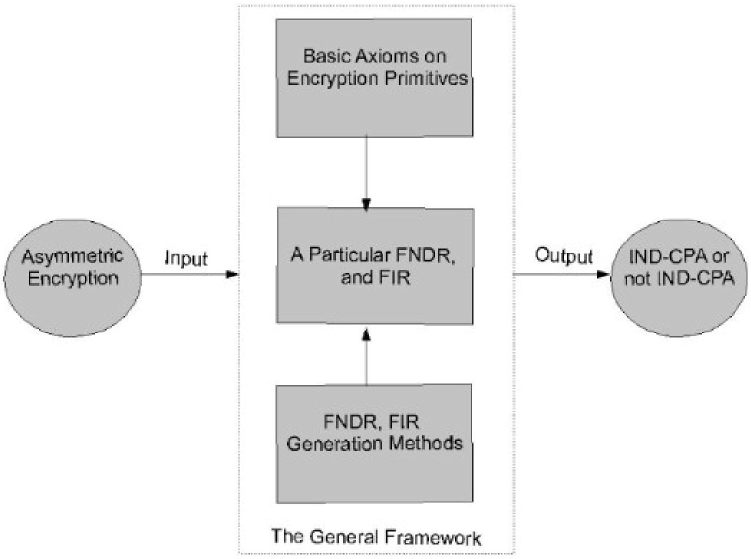
Basic Axioms on Encryption Primitives
A Particular FNDR, and FIR
FNDR, FIR Generation Methods
Asymmetric Encryption
Input
Output
IND-CPA or not IND-CPA
The General Framework

Figure 4.1: The General Framework for Verification

4.1 Bellare and Rogaway'93

[12] Let us consider such a trapdoor one-way permutation function $f : X \rightarrow Z$ and we denote g its invert:
Encryption of $m \in M = \{0,1\}^{k_0} \rightarrow (a||b||c)$, $r \in X$ is randomly chosen.
$a = f(r)$;
$b = m \oplus G(r)$;
$c = H(m \parallel r), (a||b||c) \rightarrow$ is the ciphertext.
Decryption of $(a||b||c)$, given $a \in Z; b \in \{0,1\}^k; c \in Y$, compute:
$r = g(a)$;
$m = b \oplus G(r)$.
If $c = H(m||r)$ then m is the plaintext, otherwise 'Reject': invalid ciphertext.
First, we can represent the output of this encryption scheme as output $=$ $f(r)||m \oplus G(r)||H(m \parallel r)$ as the frame following:
$\varphi = \nu r.\{x_a = f(r), x_b = m \oplus G(r), x_c = H(m \parallel r)\}$
Apply the basic axioms on the encryption primitives in chapter 3, we have this set of pairs of closed frames and terms such that every pair (φ, M)

implies that every probabilistic polynomial-time adversary $\mathcal{B}$ with the advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, M]]_{A_\eta}; \hat{e}' \leftarrow \mathcal{B}(\eta, \hat{\phi}) : \hat{e}' =_{A_\eta} \hat{e}]$ is negligible.
$S_d = \{$
$(\nu r.\{x_a = f(r)\}, r);$
$(\nu r.\{x_a = f(r)\}, m||r);$
$(\nu r.\{x_a = f(r), x_b = G(r)\}, r);$
$(\nu r.\{x_a = f(r), x_b = G(r)\}, m||r);$
$(\nu r.\{x_a = f(r), x_c = H(m||r)\}, m||r)\}.$
Apply the generation of a formal non-deducibility relation-FNDR in the previous chapter, we have the pairs of closed frames and terms following are in $\langle S_d \rangle_{\not\models}$:
$(\nu r.\{x_a = f(r), x_b = m \oplus G(r)\}, m||r);$
(by $(\varphi\varphi_1, m||r);$
$\varphi = \nu r.\{x_a = x_a, x_b = m \oplus x_b\},$
$(\varphi_1 = \nu r.\{x_a = f(r), x_b = G(r)\}, m||r) \in S_d)$
$(\nu r.r_2.\{x_a = f(r), x_b = r_2\}, m||r);$
(by $(\varphi\varphi_1, m||r);$
$\varphi = \nu r_2.\{x_a = x_a, x_b = r_2\}, (\varphi_1 = \nu r.\{x_a = f(r)\}, m||r) \in S_d)$
$(\nu r.r_3.\{x_a = f(r), x_c = r_3\}, r)$
(by $(\varphi\varphi_1, m||r);$
$\varphi = \nu r_3.\{x_a = x_a, x_c = r_3\}, (\varphi_1 = \nu r.\{x_a = f(r)\}, m||r) \in S_d)$

Form the pairs in $\langle S_d \rangle_{\not\models}$ and by applying the basic axioms on encryption primitives, we have the set S_e such that every pairs of closed frames (φ_1, φ_2) implies that every probabilistic polynomial-time adversary $\mathcal{B}$ with the advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_1]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1] - P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_2]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1]$ is negligible.:
$S_e = \{$
$(\nu r.\{x_a = f(r)\}, \nu r_1.\{x_a = r_1\});$
$(\nu r.\{x_a = f(r), x_b = G(r)\},$
$\nu r.r_2.\{x_a = f(r), x_b = r_2\});$
$(\nu r.\{x_a = f(r), x_c = H(m||r)\},$
$\nu r.r_3.\{x_a = f(r), x_c = r_3\});$
$(\nu r.\{x_a = f(r), x_b = m \oplus G(r), x_c = H(m||r)\},$
$\nu r.r_3.\{x_a = f(r), x_b = m \oplus G(r), x_c = r_3\});$

$(\nu r.r_2.\{x_a = f(r), x_b = r_2, x_c = H(m||r)\},$
$\nu r.r_2.r_3.\{x_a = f(r), x_b = r_2, x_c = r_3\});$
$(\nu r.r_2.r_3.\{x_a = f(r), x_b = m \oplus r_2, x_c = r_3\},$
$\nu r.r_2.r_3.\{x_a = f(r), x_b = r_2, x_c = r_3\})\}.$
Apply the generation of a formal indistinguishability relation-FIR in the previous chapter, we have the pairs of closed frames and terms following are in $\langle S_e \rangle_{\cong}$:
$(\nu r.\{x_a = f(r), x_b = m \oplus G(r)\}, \nu r.r_2.\{x_a = f(r), x_b = m \oplus r_2\});$
(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"_1|\varphi"_2\});$
$\varphi = \{x_a = x_a, x_b = x'_b \oplus x_b, x_c = x_c\};$
$(\varphi'_1 = \nu r.\{x_a = f(r), x_b = G(r)\},$
$\varphi"_1 = \nu r.r_2.\{x_a = f(r), x_b = r_2\}) \in S_e;$
$(\varphi'_2 = \{x'_b = m\} =_E \tau(\{x'_b = m\}) = \varphi"_2)$ for the identified renaming)
$(\nu r.r_3.\{x_a = f(r), x_b = m \oplus G(r), x_c = r_3\},$
$\nu r.r_2.r_3.\{x_a = f(r), x_b = m \oplus r_2, x_c = r_3\});$
(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"_1|\varphi"_2\});$
$\varphi = \{x_a = x_a, x_b = x'_b \oplus x_b, x_c = x_c\},$
$(\varphi'_1 = \nu r.\{x_a = f(r), x_b = G(r)\},$
$\varphi"_1 = \nu r.r_2.\{x_a = f(r), x_b = r_2\}) \in S_e,$
$(\varphi'_2 = \nu r_3.\{x'_b = m, x_c = r_3\} =_E \tau(\nu r_3.\{x'_b = m, x_c = r_3\}) = \varphi"_2)$
for the identified renaming)
$(\nu r.\{x_a = f(r), x_b = m \oplus G(r), x_c = H(m||r)\},$
$\nu r.r_2.r_3.\{x_a = f(r), x_b = r_2, x_c = r_3\});$
(the transitive property)
$(\nu r.r_2.r_3.\{x_a = f(r), x_b = r_2, x_c = r_3\},$
$\nu r_1.r_2.r_3.\{x_a = r_1, x_b = r_2, x_c = r_3\};$
(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"'_1|\varphi"'_2\});$
$\varphi = \{x_a = x_a, x_b = x_b, x_c = x_c\},$
$(\varphi'_1 = \nu r.\{x_a = f(r)\}, \varphi"_1 = \nu r_1.\{x_a = r_1\}) \in S_e,$
$(\varphi'_2 = \nu r_2.r_3.\{x_b = r_2, x_c = r_3\} =_E \varphi"_2 = \tau(\nu r_2.r_3.\{x_b = r_2, x_c = r_3\}))$
(for the identified renaming)
$(\nu r.\{x_a = f(r), x_b = m \oplus G(r), x_c = H(m \parallel r)\},$
$\nu r_1.r_2.r_3.\{x_a = r_1, x_b = r_2, x_c = r_3\})\}.$
(the transitive property)
That means this encryption schemes is semantic security (IND-CPA) or an

adversary can not distinguish the frame φ and the frame with random value.

4.2 REACT

[13] Let us consider such a partially trapdoor one-way permutation function $f : X \times X \rightarrow Z$ and we denote g its partial invert:
Encryption of $m \in M = \{0,1\}^{k_0} \rightarrow (a||b||c)$.
$R \in X, r \in X$ are randomly chosen.
$a = f(R||r)$;
$b = m \oplus G(R)$;
$c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R))), (a||b||c) \rightarrow$ is the ciphertext.
Decryption of $(a||b||c)$, given $a \in Z; b \in \{0,1\}^k; c \in Y$, compute:
$R = g(a)$;
$m = b \oplus G(R)$.
If $c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))$ then m is the plaintext, otherwise 'Reject': invalid ciphertext.
First, we can represent the output of this encryption scheme as output $= f(R||r)||m \oplus G(R)||H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))$ as the frame following:
$\varphi = \nu R.r.\{x_a = f(R||r), x_b = m \oplus G(R), x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\}$
Apply the basic axioms on the encryption primitives in chapter 3, we have this set of pairs of closed frames and terms such that every pair (φ, M) implies that every probabilistic polynomial-time adversary $\mathcal{B}$ with the advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, M]]_{A_\eta}; \hat{e}' \leftarrow \mathcal{B}(\eta, \hat{\phi}) : \hat{e}' =_{A_\eta} \hat{e}]$ is negligible.
$S_d = \{$
$(\nu R.r.\{x_a = f(R||r)\}, R)$;
$(\nu R.r.\{x_a = f(R||r)\}, R||m||f(R||r)||(m \oplus G(R)))$;
$(\nu R.r.\{x_a = f(R||r), x_b = G(R)\}, R)$;
$(\nu R.r.\{x_a = f(R||r), x_b = G(R)\}, R||m||f(R||r)||(m \oplus G(R)))$;
$(\nu R.r.\{x_a = f(R||r), x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\},$
$R||m||f(R||r)||(m \oplus G(R)))\}$.
Apply the generation of a formal non-deducibility relation-FNDR in the previous chapter, we have the pairs of closed frames and terms following are in $\langle S_d \rangle_{\not\models}$:

$(\nu R.r.\{x_a = f(R||r), x_b = m \oplus G(R)\}, R||m||f(R||r)||(m \oplus G(R)));$
(by $(\varphi\varphi_1, R||m||f(R||r)||(m \oplus G(R)));$
$\varphi = \nu r.\{x_a = x_a, x_b = m \oplus x_b\},$
$(\varphi_1 = \nu r.\{x_a = f(R||r), x_b = G(R)\}, R||m||f(R||r)||(m \oplus G(R))) \in S_d)$
$(\nu R.r.r_2.\{x_a = f(R||r), x_b = r_2\}, R||m||f(R||r)||(m \oplus G(R)));$
(by $(\varphi\varphi_1, R||m||f(R||r)||(m \oplus G(R)));$
$\varphi = \nu r_2.\{x_a = x_a, x_b = r_2\},$
$(\varphi_1 = \nu r.\{x_a = f(R||r)\}, R||m||f(R||r)||(m \oplus G(R))) \in S_d)$
$(\nu R.r.r_3.\{x_a = f(R||r), x_c = r_3\}, R).$
(by $(\varphi\varphi_1, R);$
$\varphi = \nu r_3.\{x_a = x_a, x_c = r_3\}$
$(\varphi_1 = \nu r.\{x_a = f(R||r)\}, R) \in S_d)$

Form the pairs in $\langle S_d \rangle_{\not\models}$ and by applying the basic axioms on encryption primitives, we have the set S_e such that every pairs of closed frames (φ_1, φ_2) implies that every probabilistic polynomial-time adversary $\mathcal{B}$ with the advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_1]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1] - P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_2]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1]$ is negligible:
$S_e = \{$
$(\nu R.r.\{x_a = f(R||r)\}, \nu r_1.\{x_a = r_1\});$
$(\nu R.r.\{x_a = f(R||r), x_b = G(R)\},$
$\nu R.r.r_2.\{x_a = f(R||r), x_b = r_2\});$
$(\nu R.r.\{x_a = f(R||r), x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\},$
$\nu R.r.r_3.\{x_a = f(R||r), x_c = r_3\});$
$(\nu R.r.r_2.\{x_a = f(R||r), x_b = r_2, x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\},$
$\nu R.r.r_2.r_3.\{x_a = f(R||r), x_b = r_2, x_c = r_3\});$
$(\nu R.r.\{x_a = f(R||r), x_b = m \oplus G(R), x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\},$
$\nu R.r.r_3.\{x_a = f(R||r), x_b = m \oplus G(R), x_c = r_3\})(\nu R.r.r_2.r_3.\{x_a = f(R||r), x_b = m \oplus r_2, x_c = r_3\},$
$\nu R.r.r_2.r_3.\{x_a = f(R||r), x_b = r_2, x_c = r_3\})\}.$
Apply the generation of a formal indistinguishability relation-FIR in the previous chapter, we have the pairs of closed frames and terms following are in $\langle S_e \rangle_{\cong}$:
$(\nu R.r.\{x_a = f(R||r), x_b = m \oplus G(R)\}, \nu R.r.r_2.\{x_a = f(R||r), x_b = m \oplus r_2\});$

(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"_1|\varphi"_2\})$;
$\varphi = \{x_a = x_a, x_b = x'_b \oplus x_b, x_c = x_c\}$;
$(\varphi'_1 = \nu R.r.\{x_a = f(R||r), x_b = G(R)\}$,
$\varphi"_1 = \nu R.r.r_2.\{x_a = f(R||r), x_b = r_2\}) \in S_e$;
$(\varphi'_2 = \{x'_b = m\} =_E \tau(\{x'_b = m\}) = \varphi"_2)$ for the identified renaming)
$(\nu R.r.r_3.\{x_a = f(R||r), x_b = m \oplus G(R), x_c = r_3\}$,
$\nu R.r.r_2.r_3.\{x_a = f(R||r), x_b = m \oplus r_2, x_c = r_3\})$;
(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"_1|\varphi"_2\})$;
$\varphi = \{x_a = x_a, x_b = x'_b \oplus x_b, x_c = x_c\}$,
$(\varphi'_1 = \nu R.r.\{x_a = f(R||r), x_b = G(R)\}$,
$\varphi"_1 = \nu R.r.r_2.\{x_a = f(R||r), x_b = r_2\}) \in S_e$,
$(\varphi'_2 = \nu r_3.\{x'_b = m, x_c = r_3\} =_E \tau(\nu r_3.\{x'_b = m, x_c = r_3\}) = \varphi"_2)$
for the identified renaming)
$(\nu R.r.\{x_a = f(R||r), x_b = m \oplus G(R), x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\}$,
$\nu R.r.r_2.r_3.\{x_a = f(R||r), x_b = r_2, x_c = r_3\})$;
(the transitive property)
$(\nu R.r.r_2.r_3.\{x_a = f(R||r), x_b = r_2, x_c = r_3\}$,
$\nu r_1.r_2.r_3.\{x_a = r_1, x_b = r_2, x_c = r_3\}$;
(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"'_1|\varphi"'_2\})$;
$\varphi = \{x_a = x_a, x_b = x_b, x_c = x_c\}$,
$(\varphi'_1 = \nu R.r.\{x_a = f(R||r)\}, \varphi"_1 = \nu r_1.\{x_a = r_1\}) \in S_e$,
$(\varphi'_2 = \nu r_2.r_3.\{x_b = r_2, x_c = r_3\} =_E \varphi"_2 = \tau(\nu r_2.r_3.\{x_b = r_2, x_c = r_3\}))$
for the identified renaming)
$(\nu R.r.\{x_a = f(R||r), x_b = m \oplus G(R), x_c = H(R \parallel m \parallel f(R||r) \parallel (m \oplus G(R)))\}$,
$\nu r_1.r_2.r_3.\{x_a = r_1, x_b = r_2, x_c = r_3\})\}$.
(the transitive property)
That means this encryption schemes is semantic security (IND-CPA) or an adversary can not distinguish the frame φ and the frame with random value.

4.3 Pointcheval's Transformer

[9] Let us consider such a partially trapdoor one-way permutation function $f : X \times Y \to Z$ and we denote g its invert:

Encryption of $m \in M = \{0,1\}^{k_0} \rightarrow (a||b)$, $r \in X, s \in \{0,1\}^{k_0}$ are randomly chosen.
$a = f(r||H(m||s))$;
$b = (m||s) \oplus G(r), (a||b) \rightarrow$ is the ciphertext.
Decryption of $(a||b)$, given $a \in Z; b \in \{0,1\}^k$, compute:
$r = g(a)$;
$M = b \oplus G(r)$.
If $a = f(r||H(M)$ then $m = [M]_{k_0}$ is the plaintext, otherwise 'Reject': invalid ciphertext.
First, we can represent the output of this encryption scheme as output $= f(r||H(m||s))||((m||s) \oplus G(r))$ as the frame following:
$\varphi = \nu r.s.\{x_a = f(r||H(m||s)), x_b = ((m||s) \oplus G(r))\}$
Apply the basic axioms on the encryption primitives in chapter 3, we have this set of pairs of closed frames and terms such that every pair (φ, M) implies that every probabilistic polynomial-time adversary $\mathcal{B}$ with the advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, M]]_{A_\eta}; \hat{e}' \leftarrow \mathcal{B}(\eta, \hat{\phi}) : \hat{e}' =_{A_\eta} \hat{e}]$ is negligible.
$S_d = \{$
$(\nu r.s.\{x_a = f(r||H(m||s))\}, r)$;
$(\nu r.s.\{x_a = f(r||H(m||s)), x_b = G(r)\}, r)\}$;
$(\nu s.\{x_a = H(m||s)\}, m||s)$.
Apply the generation of a formal non-deducibility relation-FNDR in the previous chapter, we have the pairs of closed frames and terms following are in $\langle S_d \rangle_{\not\models}$:
$(\nu s.\{x_a = f(r||H(m||s))\}, m||s)$
(by $(\varphi\varphi_1, m||s)$;
$\varphi = \{x_a = f(r||x_a)\}, (\varphi_1 = \nu s.\{x_a = H(m||s)\}, m||s) \in S_d)$.
Form the pairs in $\langle S_d \rangle_{\not\models}$ and by applying the basic axioms on encryption primitives, we have the set S_e such that every pairs of closed frames (φ_1, φ_2) implies that every probabilistic polynomial-time adversary $\mathcal{B}$ with the advantage: $P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_1]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1] - P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi_2]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1]$ is negligible:
$S_e = \{$
$(\nu r.\{x_b = G(r)\}, \nu r_2.\{x_b = r_2\})$;
$(\nu r.s.\{x_a = f(r||H(m||s))\}, \nu r_1.\{x_a = r_1\})$;
$(\nu r.s.\{x_a = f(r||H(m||s)), x_b = G(r)\}, \nu r.s.r_2.\{x_a = f(r||H(m||s)), x_b =$

$r_2\});$
$(\nu r.s.\{x_a = f(r||H(m||s)), x_b = (m||s)\oplus G(r)\}, \nu r.s.r_2.\{x_a = f(r||H(m||s)), x_b = r_2\})\}.$
Apply the generation of a formal indistinguishability relation-FIR in the previous chapter, we have the pairs of closed frames and terms following are in $\langle S_e\rangle_{\cong}$:
$(\nu r.s.r_2.\{x_a = f(r||H(m||s)), x_b = r_2\}, \nu r_1.r_2.\{x_a = r_1, x_b = r_2\})$
(by $(\varphi\{\varphi'_1|\varphi'_2\}, \varphi\{\varphi"_1|\varphi"_2\});$
$\varphi = \{x_a = x_a, x_b = x_b\},$
$(\varphi'_1 = \nu r.s.\{x_a = f(r||H(m||s))\}, \varphi"_1 = \nu r_1.\{x_a = r_1\}) \in S_e$
$(\varphi'_2 = \nu r_2, \{x_b = r_2\} =_E \tau(\nu r_2, \{x_b = r_2\}) = \varphi"_2)$
for the identified renaming τ That means this encryption schemes is semantic security (IND-CPA) or an adversary can not distinguish the frame φ and the frame with random value.

Conclusions and Future Work

In this thesis we developed a general framework for verifying the property security of an asymmetric encryption scheme. These are the result on abstract models with equational theories. We also define a new formal non-deducibility relation - FNDR beside the formal indistinguishability relation - FIR. Then we define the soundness and faithfulness of cryptographic implementations with respect to abstract models. This is the approach to bridge two views of cryptography: formal and computational. These definitions allow us to ensure that a term is not deducible in an abstract model from a frame implies that the part of information is also can not be deduced from the ciphertext in computational model. Also two frames are not distinguishable in an abstract model implies that these they can not be distinguished in computational model. Finally, to generate the general framework, we propose the basic axioms on encryption primitives and the useful propositions to generate a FNDR and FIR from a set of pairs of closed frames and term a set of pairs of closed frames, respectively. We also propose the propositions to guarantee soundness property of a FNDR and a FIR.

A direction for further work is to study the other basic axioms on encryption primitives. Also include the probabilistic encryptions, for example how to find basic axioms to represent the polynomials multiplication operation. Study the concrete security and how to automate this method. Another direction is to extend the capability of the general framework for verifying more property security of an asymmetric encryption like IND-CCA1, IND-CCA2, NM-CCA1, NM-CCA2 not only the property security IND-CPA.

Bibliography

[1] M. Abadi, and A. D. Gordon *A calculus for cryptographic protocols, the Spi calculus*, In Proc. 4th ACM Conference on Computer and Communications Security (CCS'97), pages 36-47, 1997.

[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, M. Burrows, B. Lampson, and G. Plotkin *A calculus for access control in distributed systems*, ACM Transactions on Programming Languages and Systems, 15(4):706-734, 1993.

[4] 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. Relations.

[5] 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.

[6] M. Baudet, V. Cortier, and S. Kremer *Computationally sound implementations of equqtional theories against passive adversaries*, In Proc. 32st International Colloquium on Automata, Languages and Programming (ICALP'05), volume 3580 of LNCS, pages 652-663, 2005.

[7] M. Abadi, M. Baudet, and B. Warinschi *Guessing attacks and computational soundness of static equivalence*, In L. Aceto and A. Ingolfsdottir, editors, Proceedings. 9th International Conference on Foundations of Software Science and Computational Structures(FoSSa '06), volume 3921 of LNCS, pages 398-412, 2006.

[8] G. Bana, P. Mohassel, and T. Stegers *Computational soundness of formal indistinguishability and static equivalence*, In Proceedings. ASIAN 2006, Lecture Notes in Computer Science, Springer-Verlag, 2007.

[9] David Pointcheval *Chosen-Ciphertext security for any One-way cryptosystem*, In Proceedings. Lecture Notes in Computer Science, Springer-Verlag, 2000.

[10] 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.

[11] 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.

[12] M. Bellare and P. Rogaway *Optimal asymmetric encryption*, In Alfredo De Santis, editor, EURO-CRYPT, volume 950 of LNCS, pages 92-111, 1994.

[13] T. Okamoto and D. Pointcheval *React: Rapid enhanced-security asymmetric cryptosystem transform*, In CT-RSA 2001: Proceeding of the 2001 Conference on Topics in Cryptography, pages 159-175, London, UK, 2001.

[14] M. Bellare and P. Rogaway *Random oracles are practical: a paradigm for designing efficient protocols*, In Procs of the 1st CCS, pages 62-73, ACM Press, NewYork, 1993.

[15] M. Abadi, M. Baudet and B. Warinschi *Guessing attacks and the computational soundness of static equivalences*, In Procs of the 9th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'06), volume 3921 of LNCS, pages 398-412, 2006.

[16] P. Adao, G. Bana and A. Scedov *Computational and information-theoric soundness and completeness of formal encryption*, In Procs of the 18th IEEE Computer Security Foundations Workshop (CSFW'05), pages 170-184, 2005.

[17] M. Backes and B. Pfitzmann *Symmetric encryption in a simulatable Dolev-Yao style cryptographic library*, In Procs of the 17th IEEE Computer Security Foundations Workshop (CSFW'04), pages 204-218, 2004.

[18] V. Cortier S. Delaune and P. Lafourcade *A survey of algebraic properties used in cryptographic protocols*, Journal of Computer Security, To appear, 2005.

[19] D. Dolev and A. C. Yao *On the security of public key protocols*, IEEE Transactions on Information Theory, IT-29(12):198-208, 1983.

[20] S. Goldwasser and S. Micali *Probabilistic encryption*, Journal of Computer and System Sciences, 28:270-299, 1984.

[21] M. Burrows, M. Abadi and R. Needham *A logic of authentication*, Proceedings of the Royal Society, Series A, 426(1871):233-271, 1989. Also appeard as SRC Research Report 39 and, in a shortened form, in ACM Transactions on Computer Systems 8, 1 (February 1990), 18-36.

[22] R. A. Kemmerer *Analyzing encryption protocols using formal verification techniques*, IEEE Journal on Selected Areas in Communications, 7(4):448-457, May 1989.

[23] M. Bellare, J. Killian and P. Rogaway *The security of cipher block chaining*, In Y. Desmedt, editor, Advances in Cryptology - CRYPTO'94, 14th Annual International Cryptology Conference, volume 839 of LNCS, pages 341-358, Santa Barbara, California, USA, August 1994.

[24] S. Goldwasser, S. Micali and A. Wigderson *Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems*, Journal of the ACM, 38(1):691-729, 1991.

Appendix

Proposition 7. *Static equivalence $\approx_E$ is a formal indistinguishability relation with respect to the equational theory E.*

Proof. Items (i) and (iii) are trivially satisfied by $\approx_E$. Consider frames $\varphi, \varphi_1, \varphi_2$ as in (ii). Let M, N be terms whose variables are included in $\mathit{dom}(\varphi\varphi_1) = \mathit{dom}(\varphi\varphi_2) = \mathit{dom}(\varphi)$ and that have no names in common with $\varphi\varphi_i, i = 1, 2$. Then $fnames(M\varphi) = fnames(M) \cup names(\varphi)$, and $fnames(M) \cup names(\varphi)$ is disjoint from $names(\varphi_i)$ by the assumption on M and condition (ii). Therefore $fnames(M\varphi)$ and $bnames(\varphi_i)$ are disjoint (and likewise for N). If $\varphi_1 \approx_E \varphi_2$ holds, then by the definition of static equivalence, $(M\varphi)\varphi_1 =_E (N\varphi)\varphi_1$ if and only if $(M\varphi)\varphi_2 =_E (N\varphi)\varphi_2$. Therefore, $M(\varphi\varphi_1) =_E N(\varphi\varphi_1)$ if and only if $M(\varphi\varphi_2) =_E N(\varphi\varphi_2)$, and that is exactly what we had to prove.

To see (iv), we construct another renaming τ' in the following: On the $bnames(\varphi)$, let τ' be equal τ, and on N $(bnames(\varphi) \cup \tau(bnames(\varphi))$, let τ' be the identity map. We will have to define τ' on the domain $\tau(bnames(\varphi)) \setminus bnames(\varphi)$. Since τ is a sort-preserving bijection, the number of elements in the domain $\tau(bnames(\varphi))$ $bnames(\varphi)$ is the same as the number of elements in $bnames(\varphi)$ $\tau(bnames(\varphi))$ for each sort s. Both are $|bnames(\varphi)| - |bnames(\varphi) \cap \tau(bnames(\varphi))|$, which equals $|\tau(bnames(\varphi))| - |bnames(\varphi) \cap \tau(bnames(\varphi))|$. So on the domain $\tau(bnames(\varphi)) \setminus bnames(\varphi)$ choose τ' to be any bijection to the domain $bnames(\varphi) \setminus \tau(bnames(\varphi))$. It is then easy to see that τ' is a sort-preserving bijection on N, and that $\tau'(\varphi) = \tau(\varphi)$ for the frame φ. Moreover, for any term M that shares no names with φ and $\tau(\varphi), \tau'(M) = M$, and therefore $M\tau(\varphi) = M\tau'(\varphi) = \tau'(M\varphi)$ holds. Hence, for any two terms M and N such that $fnames(M, N) \cap (bnames(\varphi) \cup bnames(\tau(\varphi))) = \phi$, $M\tau(\varphi) =_E N\tau(\varphi)$ if and only if $\tau'(M\varphi) =_E \tau'(N\varphi)$

which happends. Since τ' is a bijection - if and only if $M\varphi =_E N\varphi$, and $\tau(\varphi) \approx_E \varphi$ follows.

□

Proposition 8. *The intersection of an arbitrary number of formal indistinguishability relations (with respect to the same equational theory E) is a formal indistinguishability relation.*

Proof. Let $(\cong_i)_{i \in I}$, where I is some indexing set, be a sequence of weak formal indistinguishability relations with respect to the same equational theory E, and let $\cong$ be their intersection. Clearly, $\cong$ is equivalence relation and satisfies the properties (i),(iii). We will show that $\cong$ also satisfies the properties (ii), (iv). Let $\varphi, \varphi_1, \varphi_2$ be as in (ii). Because $(\varphi\varphi_1) \cong_i \varphi\varphi_2$ for all $i \in I$, hence $\varphi\varphi_1 \cong \varphi\varphi_2$. Likewise, since every $\cong_i$ is preserved by the renaming of variables, $\cong$ is preserved also. Therefore (ii),(iv) are also satisfied by $\cong$.

□

Proposition 9. *Consider static equivalence as a subset $\tilde{E} \subseteq \mathcal{F}_c \times \mathcal{F}_c$. If $S \subseteq \tilde{E}$, then there is an unique smallest $\langle S \rangle_{\cong} \subseteq \tilde{E}$ is a formal indistinguishability relation with respect to the equivalent theory E. $\langle S \rangle_{\cong}$ can be generated in the following way: Let*

$$S' := \begin{cases} (\varphi', \varphi") \in \mathcal{F}_c \times \mathcal{F}_c | \varphi' = \varphi\{\varphi_1^{'}|...|\varphi_n^{'}\}, \varphi" = \varphi\{\varphi_1^{"}|...|\varphi_n^{"}\} \\ \text{such that } bnames(\varphi) = \phi \text{ and for all } i = 1, ..., n, \\ (\varphi', \varphi") \in S, \text{ or}(\varphi", \varphi') \in S, \text{ or}\varphi" =_E \tau_i(\varphi')\text{for some renaming } \tau_i. \end{cases}$$

and $\langle S \rangle_{\cong}$ is the transitive closure of S'.

Proof. We see that the existence of the smallest subset is clear. Then to prove the statement about how to construct $\langle S \rangle_{\cong}$, consider the transitive closure $\hat{S}$ of S'.It is clear from the definition of S' that $\hat{S}$ is symmetric, reflexive and transitive, hence an equivalence relation. Also clear that S, S' in $\hat{S}$. Therefore, we only need to show that $\hat{S}$ is a formal indistinguishability relation.

By the generation of $\hat{S}$, we can see that it satisfies the properties (i),(iii) and (iv) of a formal indistinguishability relation. So we have to show that it will satisfy the property (ii). Let φ be as in (ii). Suppose that $(\varphi_1, \varphi_2) \in \hat{S}$, so there are frames $\psi_1, ..., \psi_n$ such that $\varphi_1 = \psi_1$ and $\varphi_2 = \psi_n$, and the pair $(\psi_i, \psi_{i+1}, i = 2, ..., n$, are all in S'. Without loss of generality, we can assume that $names(\varphi) \cap bnames(\psi_i) = \phi$, because otherwise the names can be remove away via renaming, the result pairs of frames will still be in S'. If we can show that $(\varphi\psi_i, \varphi\psi_{i+1}) \in S'$, then the transitivity ensures that $(\varphi\varphi_1, \varphi\varphi_2) \in \hat{S}$. Let us fix the value i. Since $(\psi_i, \psi_{i+1}) \in S'$ so the frame ψ_i has form $\psi_i = \psi\{\psi'_1|...|\psi'_m\}$ and $\psi_{i+1} = \psi\{\psi"'_1|...|\psi"'_m\}$ such that for all $j = 1, ..., m$, $(\psi'_j, \psi"'_j) \in S$, or $(\psi"'_j, \psi'_j) \in S$ or $\psi"'_j = \tau_j(\psi'_j)$ for some renaming τ_j and $names(\psi) = \phi$. If $[names(\{\psi'_1|...|\psi'_m\}) \setminus names(\psi_i)] \cap names(\varphi) \neq \phi$, then replace those names with fresh ones in $\{\psi'_1|...|\psi'_m\}$ this can be done because they don't show up in ψ. Similarly for ψ_{i+1}. Let $a_1, ..., a_l$ be the names occurring in φ, and let $y_1, ..., y_l$ be the fresh variables. For $1 \leq k \geq l$, replace every occurrence of a_k in φ by the variable y_k, obtaining a frame ζ such that $names(\zeta) = \phi$ and $(\varphi\psi_i = (\zeta\psi\{\psi'_1|...|\psi'_m|y_1 = a_1|...|y_l = a_l\}$ and $(\varphi\psi_{i+1} = (\zeta\psi\{\psi"'_1|...|\psi"'_m|y_1 = a_1|...|y_l = a_l\}$. By assumption, $names(\psi) = \phi$, so $names(\zeta\psi) = \phi$, and therefore, $(\varphi\psi_i, \varphi\psi_{i+1}) \in S'$.

□

Proposition 10. *Let A be a computational algebra that is $=_E$-sound. Suppose $S \subseteq \widetilde{E}$ is a binary relation on closed frames such that $(\varphi, \psi) \in S$ implies $[[\varphi]]_{A_\eta} \approx [[\psi]]_{A_\eta}$. Then $[[\varphi]]_{A_\eta} \approx [[\psi]]_{A_\eta}$ whenever $\varphi \cong \psi$. That is, A is $\cong$-sound.*

Proof. As a consequence of proposition above, it is sufficient to verify that those production rules preserve the computational indistinguishability of the frames. For the reflexivity, transitivity, and symmetry, this is implied by the fact that computational indistinguishability is an equivalence relation. By the definition of the interpretation of a frame, it is also clear that if ψ is any frame and τ is a renaming, then $[[\psi]]_{A_\eta} \approx [[\tau(\psi)]]_{A_\eta}$.
We will show that for any frame $\varphi_1, \varphi_2, \varphi$ are as in proposition above, then $[[\varphi_1]]_{A_\eta} \approx [[\varphi_2]]_{A_\eta}$ implies $[[\varphi\varphi_1]]_{A_\eta} \approx [[\varphi\varphi_2]]_{A_\eta}$. Suppose that there is a probabilistic polynomial-time adversary $\mathcal{A}$ whose advantage:
$|P[\mathcal{A}(\eta, [[\varphi\varphi_1]]_{A_\eta}) = 1] - P[\mathcal{A}(\eta, [[\varphi\varphi_2]]_{A_\eta}) = 1]|$ is non-negligible. This

gives an adversary $\mathcal{B}$ that distinguishes φ_1, φ_2 with non-negligible advantage. Given the concrete frame $\hat{\psi}$ are the sampled elements of $[[\varphi_1]]_{A_\eta}$ or $[[\varphi_2]]_{A_\eta}$. The adversary $\mathcal{B}$ simply interprets the frame φ using the values specified by $\hat{\psi}$ for the variables occurring in φ. All these variables are assigned a unique values if $\hat{\psi}$ is sampled from $[[\varphi_i]]_{A_\eta}$ since $var(\varphi) \subseteq dom(\varphi_i).\mathcal{B}$ constructs a concrete frame $\hat{\sigma_i}$ and runs $\mathcal{A}(\hat{\sigma_i})$. Then the output is $\mathcal{A}'s$ output. Therefore, the advantage of $\mathcal{B}$ equals the advantage of A, which is non-negligible because the distribution of $\hat{\sigma_i}$ is exactly $[[\varphi\varphi_i]]_{A_\eta}$. In addition, $\mathcal{B}$ runs in probabilistic polynomial-time since the size of encoding of φ is constant in η, so the concrete frame $\hat{\sigma_i}$ can computed in probabilistic polynomial-time. Contradiction.

□

Random generation

We consider a *random assignment* like this νa, in π - calculus that means creating a fresh name a. It is that it declares a new unique name a, distinct from all external names, for use in the process. Based on the propositions above, we propose a set of specific axioms following which are sound:
(RD1) $\nu a.\theta \not\models a$.
(RE1) $\nu a.\{x = a\} \cong \nu r.\{x = r\}$.

Proof. For the axiom $(RD)1$, we assume that a has the sort s. Consider a polynomial-time adversary B, its advantage is:
$P[\hat{\epsilon}, \hat{e} \leftarrow^R [[\nu a.\theta, a]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}(\eta, \hat{\epsilon}) : \hat{e'} =_{A_\eta} \hat{e}]$
$= P[\hat{e} \leftarrow^R [[s]]_{A_\eta}; \hat{e}' \leftarrow \mathcal{B}(\eta, \hat{\epsilon}) : \hat{e} =_{A_\eta} \hat{e}']$
is negligible because of the *collision-free* property of the distribution.
For the axiom $(RE1)$, we have to show that this implies $[[\nu a.\{x = a\}]]_{A_\eta} \approx [[\nu r.\{x = r\}]]_{A_\eta}$. Assume that a and r have the same sort s. Consider a probabilistic polynomial-time adversary $\mathcal{B}$, its advantage is:
$P[\hat{\phi} \leftarrow^R [[\nu a.\{x = a\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1] - P[\hat{\phi} \leftarrow^R [[\nu r.\{x = r\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1]$.
Because r and a have the same sort, so two families of distributions over the concrete frames $\phi_i = \{x = e\}, e \in [[s]]_{A_\eta}, i = 1, 2$ are the same. Therefore, the advantage of $\mathcal{B}$ is negligible.

Xor function

The following basic axioms are served for *xor function*:
(XD1) $\nu\widetilde{n}.\sigma \not\models T$, then $\nu\widetilde{n}.\nu a.\{\sigma|x = a \oplus T\} \not\models T$, such that $a \notin (\widetilde{n} \cup fnames(T))$.
(XE1) $\nu\widetilde{n}.a.\{\sigma|x = a\oplus T\} \cong \nu\widetilde{n}.r.\{\sigma|x = r\}$, such that $a \notin (\widetilde{n}\cup fnames(T))$.

Proof. $(XD1)$ We call $\varphi = \nu\widetilde{n}.\sigma; \varphi_1 = \nu\widetilde{n}.\nu a.\{\sigma|x = a \oplus T\}$. Suppose that there is a probabilistic polynomial-time adversary $\mathcal{B}_1$ able to deduce the closed term T from φ_1 correctly with non-negligible probability of success. That means the advantage:
$P[\hat{\phi_1}, \hat{e} \leftarrow^R [[\varphi_1, T]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \hat{\phi_1}) : \hat{e'} =_{A_\eta} \hat{e}]$
is non-negligible. Consider the concrete frame $\hat{\phi}, \hat{e}$ from the family distribution $[[\varphi, T]]_{A_\eta}$. Then we construct an adversary $\mathcal{B}_2$ to deduce the closed term T from the frame φ as follows: $\mathcal{B}_2$ construct the concrete frame $\hat{\phi'} = \{\hat{\phi}|x = \hat{a}\}$ from the family of distribution $[[\nu a.\{x = a\}\}]]_{A_\eta}$, and the concrete frame $\hat{\phi}$, and runs $\mathcal{B}_1(\eta, \hat{\phi'})$ and output the output of the adversary $\mathcal{B}_1$. Because as we show that the distributions $[[x = a \oplus T]]_{A_\eta}, [[x = a]]_{A_\eta}$ are the same (see the reason following), so the families of distributions of $\hat{\phi}$ and $\hat{\phi'}$ are exactly the same. Therefore, the advantage of $\mathcal{B}_2$ is the advantage of the adversary $\mathcal{B}_1$.
$P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, T]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_2(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$
$= P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, T]]_{A_\eta}; \hat{a} \leftarrow^R [[s]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \{\hat{\phi}|x = \hat{a}\} : \hat{e'} =_{A_\eta} \hat{e}]$
$= P[\hat{\phi_1}, \hat{e} \leftarrow^R [[\varphi_1, T]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \hat{\phi_1}) : \hat{e'} =_{A_\eta} \hat{e}]$
is non-negligible. Otherwise, $\mathcal{B}_2$ runs in the probabilistic polynomial-time algorithm. Contradiction.
$(XE1)$ Assume that $a \oplus T$ and $x = a$ are the same sort *Data*. Because the distribution of $[[Data]]_{A_\eta}$ is uniform and the property of xor function. Therefore, given the concrete term $T : Data$, $\forall \hat{a}_0, P[\hat{a} \leftarrow^R [[x = a \oplus T]]_{A_\eta} : \hat{a} =_{A_\eta} \hat{a}_0] = P[\hat{a} \leftarrow^R [[x = a]]_{A_\eta} : \hat{a} =_{A_\eta} \hat{a}_0] = \frac{1}{|D|}$, where D is the size of domain of sort *Data*. That means the distributions are the same. The advantage of every probabilistic polynomial-time adversary $\mathcal{B}_1$ is:
$P[\hat{\phi}_1 \leftarrow^R [[\varphi_1]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}_1) = 1] - P[\hat{\phi}_2 \leftarrow^R [[\varphi_2]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}_2) = 1]$ is 0.

Concatenation function

The following basic axioms are served for *concatenation function* and sound:
(CD1) $\varphi \not\models T$, then $\varphi \not\models T \parallel T', \forall T' \in \mathcal{T}_c$.
(CE1) $\nu a.b.\{x = a \parallel b\} \cong \nu r.\{x = r\}$.

Proof. $(CD1)$ Suppose that there is a probabilistic polynomial-time $\mathcal{B}_1$ who can deduce the closed term $T \parallel T'$ from the closed frame φ. Its advantage:
$P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, T \parallel T']]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$.
is non-negligible. We build an adversary $\mathcal{B}_2$ as follows: Given the $\hat{e'} = \hat{T} \parallel \hat{T'}$ be the answer of $\mathcal{B}_1$ and the concrete frame $\hat{\phi}$, the adversary $\mathcal{B}_2$ runs $\mathcal{B}(\eta, \hat{\phi})$ returns $head(\hat{e'})$ and the result is exactly $\hat{T}$. Otherwise, $\mathcal{B}_2$ runs in a probabilistic polynomial-time. Contradiction.
$(CE1)$ Consider the concrete frames $\hat{\phi}$ is sampled from the families distributions $[[\nu a.b.\{x = a \parallel b\}]]_{A_\eta}$ or $[[\nu r.\{x = r\}]]_{A_\eta}$. Assume that $a \parallel b; r$ are the same sort $Data$, so $\forall \hat{a}_0, P[\hat{r} \leftarrow^R [[x = r]]_{A_\eta} : \hat{r} =_{A_\eta} \hat{a}_0] = P[\hat{e} \leftarrow^R [[x = a \parallel b]]_{A_\eta} : \hat{e} =_{A_\eta} \hat{a}_0] = \frac{1}{|D|}$, where D is the size of domain of sort $Data$. That means the distributions are the same. Therefore, the advantage:
$P[\hat{\phi} \leftarrow^R [[\nu a.b.\{x = a \parallel b\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1] - P[\hat{\phi} \leftarrow^R [[\nu r.\{x = r\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi}) = 1]$.
is negligible.

Hash function

The following basic axioms of a *hash function* are sound:
(HD1) $\varphi \not\models T$, $\{\varphi | x = h(T)\} \not\models T$ such that $h(T)$ does not appear in φ.
(HE1) $\varphi \not\models T$, $\{\varphi | x = h(T)\} \cong \{\varphi | \nu r.\{x = r\}\}$ such that $h(T)$ does not appear in φ.

Proof. $(HD1)$ We assume that there is an adversary $\mathcal{B}_1$ who can deduce the closed term T from the closed frame $\varphi_1 = \{\varphi | \{x = h(T)\}\}$ in the probabilistic polynomial-time algorithm. Its advantage is:
$P[\hat{\phi_1}, \hat{e} \leftarrow^R [[\varphi_1, T]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \hat{\phi_1}) : \hat{e'} =_{A_\eta} \hat{e}]$.
is non-negligible. Consider the concrete frame $\hat{\phi}$ from the family of distribution $[[\varphi]]_{A_\eta}$. We construct an adversary $\mathcal{B}_2$ who deduces the closed

term T from the closed frame φ as follows: $\mathcal{B}_2$ constructs a concrete frame $\hat{\phi}' = \{\hat{\phi}|x = [[h]]_{A_\eta}(\hat{a})\}$ from the concrete frame $\hat{\phi}_1$ and the concrete term $\hat{a}$ be the concrete term from $[[Data]]_{A_\eta}$ (we assume that the sort of term T is $Data$), runs $\mathcal{B}_1(\eta, \hat{\phi}')$ and outputs the output of $\mathcal{B}_1$. Duce to the property of the hash function like a random oracle model, x is drawn from the distribution ($\leftarrow^R [[Hash]]_{A_\eta}$) independently from $\hat{a}$ and $h(T)$ does not appear in φ. Hence, the distribution of $\hat{\phi}'$ and $\hat{\phi}_1$ are exactly the same, the advantage of the adversary $\mathcal{B}_2$ is:
$P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, T]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_2(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{e}]$
$= P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, T]]_{A_\eta}; \hat{a} \leftarrow^R [[Data]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \{\hat{\phi}|x = [[h]]_{A_\eta}(\hat{a})\}) : \hat{e'} =_{A_\eta} \hat{e}]$.
$= P[\hat{\phi}, \hat{e} \leftarrow^R [[\varphi, T]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \hat{\phi}_1) : \hat{e'} =_{A_\eta} \hat{e}]$.
is non-negligible. Contradiction.
$(HE1)$ Assume that there is a probabilistic polynomial-time adversary $\mathcal{B}_1$. He can distinguish two closed frames $\{\varphi|x = h(T)\}$ and $\{\varphi|\nu r.\{x = r\}\}$. Let $\hat{\phi}'$ is a sample from $[[\varphi_0 = \{\varphi|x = h(T)\}]]_{A_\eta}$ or $[[\varphi_1 = \{\varphi|\nu r.\{x = r\}]]_{A_\eta}$ to be analyzed. $\mathcal{B}_1$ must produce a term has form $[[h]]_{A_\eta}(\hat{e'})$. $\mathcal{B}_1$ returns 1 if $x\hat{\phi}' =_{A_\eta} [[h]]_{A_\eta}(\hat{e'})$, otherwise it returns 0. Duce to the collision-free property of hash function, so $\hat{e'} =_{A_\eta} \hat{T}$. By the definition the advantage of $\mathcal{B}_1$ is:
$P[\hat{\phi}' \leftarrow^R [[\varphi_0]]_{A_\eta} : \mathcal{B}_1(\eta, \hat{\phi}') = 1] - P[\hat{\phi}' \leftarrow^R [[\varphi_1]]_{A_\eta} : \mathcal{B}_1(\eta, \hat{\phi}') = 0]$
$= P[\hat{\phi}', \hat{e} \leftarrow^R [[\varphi_0, T]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{B}_1(\eta, \hat{\phi}'|_{dom(\varphi)}) : [[h]]_{A_\eta}(\hat{e'}) =_{A_\eta} [[h]]_{A_\eta}(\hat{e})] -$
$P[\hat{\phi}', \hat{e} \leftarrow^R [[\varphi_1, T]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{B}_1(\eta, \hat{\phi}'|_{dom(\varphi)}) : x\hat{\phi}' =_{A_\eta} = [[h]]_{A_\eta}(\hat{e})]$
$\geq P[\hat{\phi}', \hat{e} \leftarrow^R [[\varphi_0, T]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{B}_1(\eta, \hat{\phi}'|_{dom(\varphi)}) : \hat{e'} =_{A_\eta} = \hat{e}] - P[\hat{\phi}', \hat{e} \leftarrow^R [[\varphi_1, T]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{B}_1(\eta, \hat{\phi}'|_{dom(\varphi)}) : x\hat{\phi}' =_{A_\eta} [[h]]_{A_\eta}(\hat{e})]$.
is non-negligible. In the last probability expression is negligible, because $x\hat{\phi}'$ is drawn from the distribution ($\leftarrow^R [[Hash]]_{A_\eta}$) independently from $\hat{e}$. And the hash function is considered as a random oracle model. Therefore, $P[\hat{\phi}', \hat{e} \leftarrow^R [[\varphi_0, T]]_{A_\eta}; \hat{e'} \leftarrow^R \mathcal{B}_1(\eta, \hat{\phi}'|_{dom(\varphi)}) : \hat{e'} =_{A_\eta} = \hat{e}]$ is non-negligible. That means there is a probabilistic polynomial-time who can deduce the closed term T form φ with the advantage is non-negligible. Contradiction.

One-way function

The following basic axioms are sound and served for *one-way permutation function*:
(OD1) $\nu a.\{x = f(a)\} \not\models a$.

(OE1) $\nu a.\{x = f(a)\} \cong \nu r.\{x = r\}$.

If f is a partially one-way permutation function, then these basic axioms are sound:

(OD1') $\nu a.b.\{x = f(a||b)\} \not\models a$.

(OE1') $\nu a.b.\{x = f(a||b)\} \cong \nu r.\{x = r\}$.

The following rules are consequent:

(OD2) $\nu\widetilde{n}.\sigma \not\models T$, then $\nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\} \not\models a$.

(OE2) $\nu\widetilde{n}.\sigma \not\models T$, then $\nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\} \cong \nu\widetilde{n}.\nu r.\{\sigma|x = r\}$.

Proof. $(OD1)$ Consider any adversary $\mathcal{B}_1$ who want to deduce the closed term a from the closed frame $\varphi = \nu a.\{x = f(a)\}$. The advantage of $\mathcal{B}_1$ is:

$P[\hat{\phi}, \hat{a} \leftarrow^R [[\varphi, a]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{a}]$.

$= P[[[f]]_{A_\eta}(\hat{a}), \hat{a} \leftarrow^R [[\varphi, a]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, [[f]]_{A_\eta}(\hat{a})) : [[f]]_{A_\eta}(\hat{e'}) =_{A_\eta} [[f]]_{A_\eta}(\hat{a})]$.

is negligible duce to the property of trap-door one-way permutation function, $P[f(\mathcal{A}(f(x))) = f(x)]$ is negligible for all polynomial-time adversary $\mathcal{A}$.

$(OE1)$ We assume that the sort of r and the domain of the trapdoor one-way permutation function f are the same, we call it $Img(f)$. It is obviously to see that two families of distributions $[[f(a)]]_{A_\eta}; [[Img(f)]]_{A_\eta}$ are the same. Therefore, we have the advantage of any adversary who want to distinguish two closed frames is:

$P[\hat{\phi_1} \leftarrow^R [[\nu a.\{x = f(a)\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi_1}) = 1] - P[\hat{\phi_2} \leftarrow^R [[\nu r.\{x = r\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi_2}) = 1]$.

is negligible.

$(OD1')$ Consider any adversary $\mathcal{B}_1$ who want to deduce the closed term a from the closed frame $\varphi = \nu a.b.\{x = f(a||b)\}$. The advantage of $\mathcal{B}_1$ is:

$P[\hat{\phi}, \hat{a} \leftarrow^R [[\varphi, a]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{a}]$.

$= P[[[f]]_{A_\eta}(\hat{a}||\hat{b}), \hat{a} \leftarrow^R [[\varphi, a]]_{A_\eta}; \exists\hat{b'}; \hat{e'} \leftarrow \mathcal{B}_1(\eta, [[f]]_{A_\eta}(\hat{a}||\hat{b})) : [[f]]_{A_\eta}(\hat{e'}||\hat{b'}) =_{A_\eta} [[f]]_{A_\eta}(\hat{a}||\hat{b'})]$.

is negligible duce to the property of partially trap-door one-way permutation function, $P[\exists y'; f(x'||y') = f(x||y) : x' = \mathcal{A}(f(x||y))]$ is negligible for all polynomial-time adversary $\mathcal{A}$.

$(OE1')$ We assume that the sort of r and the domain of the partially trapdoor one-way permutation function f are the same, we call it $Img(f)$. It is obviously to see that two families of distributions $[[f(a||b)]]_{A_\eta}; [[Img(f)]]_{A_\eta}$ are the same. Therefore, we have the advantage of any adversary who want

to distinguish two closed frames is:
$P[\hat{\phi_1} \leftarrow^R [[\nu a.b.\{x = f(a||b)\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi_1}) = 1] - P[\hat{\phi_2} \leftarrow^R [[\nu r.\{x = r\}]]_{A_\eta} : \mathcal{B}(\eta, \hat{\phi_2}) = 1]$.
is negligible.
$(OD2)$ For any adversary $\mathcal{B}$ who want to deduce the closed term a from the closed frame $\varphi = \nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\}$ in a probabilistic polynomial-time, then its advantage is:
$P[\hat{\phi}, \hat{a} \leftarrow^R [[\varphi, a]]_{A_\eta}; \hat{e'} \leftarrow \mathcal{B}(\eta, \hat{\phi}) : \hat{e'} =_{A_\eta} \hat{a}]$
$= P[\hat{\phi}, \hat{a} \leftarrow^R [[\varphi, a]]_{A_\eta}; \exists\hat{b'}; \hat{e'} \leftarrow \mathcal{B}(\eta, x\hat{\phi}) : [[f]]_{A_\eta}(\hat{e'}||\hat{b'}) =_{A_\eta} [[f]]_{A_\eta}(\hat{a}||\hat{b'})]$.
is negligible duce to the property of partially trap-door one-way permutation function, $P[\exists y'; f(x', y') = f(x, y) : x' = \mathcal{A}(f(x, y))]$ is negligible for all polynomial-time adversary $\mathcal{A}$.
$(OE2)$ Let S be the set consisting of these pairs:
$(\nu\widetilde{n}.\sigma, \nu\widetilde{n}.\sigma)$;
$(\nu a.\{x = a\}, \nu b.\{x = b\})$;
$(\nu a.b.\{x = f(a||b)\}, \nu r.\{x = r\})$;
$(\nu\widetilde{n}.\{\sigma|x = h(T)\}, \nu\widetilde{n}.r.\{\sigma|x = r\})$ (with $\nu\widetilde{n}.\sigma \not\models T$).
Then, by the axioms above, we have $\langle S\rangle_{\cong}$-sound. In this model, $\langle S\rangle_{\cong}$ will make exactly those frames equivalent for which equivalence necessarily follows from the pairs in the set S. From $(\nu a.b.\{x = f(a, b)\}, \nu r.\{x = r\}); (\nu\widetilde{n}.\sigma, \nu\widetilde{n}.\sigma)$, we have this frames in $\langle S\rangle_{\cong}$:
$(\nu\widetilde{n}.a.b.\{\sigma|x = f(a||b)\}, \nu\widetilde{n}.r.\{\sigma|x = r\})$. And from $(\nu a.\{x = a\}, \nu b.\{x = b\}); (\nu\widetilde{n}.\{\sigma|x = h(T)\}, \nu\widetilde{n}.r.\{\sigma|x = r\})$, the frame:
$(\nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\}, \nu\widetilde{n}.a.b.\{\sigma|x = f(a||b)\}) \in \langle S\rangle_{\cong}$.
Therefore, $\nu\widetilde{n}.a.\{\sigma|x = f(a||h(T))\}, \nu\widetilde{n}.r.\{\sigma|x = r\} \in \langle S\rangle_{\cong}$. That is what we have to prove.