Formal Indistinguishability extended to the Random Oracle Model

Cristian Ene, Yassine Lakhnech and Van Chan Ngo *

Université Grenoble 1, CNRS,Verimag

There are two main frameworks for analyzing cryptographic systems; the *symbolic framework*, originating from the work of Dolev and Yao, and the *computational approach*, growing out of the work of Goldwasser and Micali. A significant amount of effort has been made in order to link both approaches and profit from the advantages of each of them. Indeed, while the symbolic approach is more amenable to automated proof methods, the computation approach can be more realistic. Abadi and Rogaway were the first to prove a formal link between these two models. More precisely, they introduced an equivalence relation on terms and prove that equivalent terms correspond to indistinguishable distributions ensembles, when interpreted in the computational model. The work of Abadi and Rogaway has been extended to active adversaries and various cryptographic primitives.

Related works. A recently emerging branch of relating symbolic and computational models for passive adversaries is based on *static equivalence* from π-calculus, induced by an *equational theory*. Equational theories provide a framework to specify algebraic properties of the underlying signature, and hence, symbolic computations in a similar way as for abstract data types. That is, for a fixed equational theory, a term describes a computation in the symbolic model. Thus, an adversary can distinguish two frames (which roughly speaking are tuples of terms), if he is able to come up with two computations that yield the same result when applied to one frame, but different results when applied to the other frame. Such a pair of terms is called a *test*. Thus, a *static equivalence* relation is fully determined by the underlying equational theory, as two frames are *statically equivalent*, if there is no test that separates them. Baudet, Cortier and Kremer studied soundness and faithfulness of static equivalence for general equational theories and used their framework to prove soundness of exclusive or as well as certain symmetric encryptions. Abadi et al. used static equivalence to analyze guessing attacks.

Recently, Bana, Mohassel and Stegers argued that even though static equivalence works well to obtain soundness results for the equational theories mentioned above, it does not work well in other important cases. Consider for instance the Decisional Diffie Hellman assumption (DDH for short) that states that the tuples (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c), where a, b, c are randomly sampled, are indistinguishable. It does not seem to be obvious to come up with an equational theory for group exponentiation such that the induced static equivalence includes this pair of tuples without including others whose computational indistinguishability is not proved to be a consequence of the DDH assumption. The static equivalence induced by the standard equational theory for group exponentiation includes the pair (g, g^a, g^b, g^{a^2b}) and (g, g^a, g^b, g^c). It is unknown whether the computational indistinguishability of these two distributions can be proved under the DDH assumption. Therefore, Bana et al. propose an alternative approach to build symbolic indistinguishability relations: a *formal indistinguishability relation (FIR)* is defined as a closure of an initial set of equivalent frames with respect to simple operations

* Grenoble, email:name@imag.fr This work has been partially supported by the ANR projects SCALP, AVOTE and SFINCS

which correspond to steps in proofs by reduction. This leads to a exible symbolic equivalence relation. In order to prove soundness of a FIR it is enough to prove soundness of the initial set of equivalences. Moreover, static equivalence is one instance of a FIR.

Contributions. In this paper, we extend Bana et al.'s approach by introducing a notion of symbolic equivalence that allows us to prove computational security of encryption schemes symbolically. More specifically, we would like to be able to treat generic encryption schemes that transform one-way functions to IND-CPA secure encryption schemes. Therefore, three problems need to be solved. First, we need to cope with one-way functions. This is another example where static equivalence does not seem to be appropriate. It does not seem easy to come with a set of equations that capture the one-wayness of a function. Indeed, consider the term $f(a|b)$, where f is a one-way function and $|$ is bit-string concatenation. We know that we cannot easily compute $a|b$ given $f(a|b)$ for uniformly sampled a and b. However, nothing prevents us from being able to compute a for instance. Introducing equations that allow us to compute a from $f(a|b)$, e.g., $g(f(a|b)) = a$, may exclude some one-way functions and does not solve the problem. Nothing prevents us from computing a prefix of b, a prefix of the prefix, etc .... The second problem that needs to be solved is related to the fact that almost all practical provably secure encryption schemes are analyzed in the random oracle model. The random oracle model is an idealized model in which hash functions are randomly sampled functions. In this model, adversaries have oracle access to these functions. An important property is that if an adversary is unable to compute the value of an expression a and if $H(a)$ has not been leaked behore, then $H(a)$ looks like a uniformly sampled value. Thus, we need to be able to symbolically prove that a value of a given expression a cannot be computed by any adversary. This is sometimes called *weak secrecy* in contrast to indistinguishability based secrecy. To cope with this problem, our notion of symbolic indistinguishability comes along with a *non-derivability* symbolic relation. Thus in our approach, we start from an initial pair of a non-derivability relation and a frame equivalence relation. Then, we provide rules that define a closure of this pair of relations in the spirit of Bana et al.'s work. Also in our case, we prove that computational soundness of the obtained relations can be checked by checking computational soundness of the initial relations. The third problem is related to the fact that security notions for encryption schemes such IND-CPA and real-or-random indistinguishability of cipher-text under chosen plaintext involve *active* adversaries. Indeed, these security definitions correspond to two-phase games, where the adversary first computes a value, then a challenge is produced, then the adversary tries to solve the challenge. Static equivalence and FIR (as defined in by Bana et all.) consider only passive adversaries. To solve this problem we consider frames that include variables that correspond to adversaries. As frames are finite terms, we only have finitely many such variables. This is the reason why we only have a degenerate form of active adversaries which is enough to treat security of encryption schemes and digital signature, for instance. The advantage of defining non-deductibility as we did, and of considering FIR (instead of static equivalence) as the good abstraction of indistinguishability, is that first, we capture "just" what is supposed to be true in the computational setting, and second, if we add more equations to our abstract algebra in a coherent manner with respect to the initial computational assumptions, then our proofs still remain computationally sound. Moreover, the closure rules we propose in our framework are designed with the objective of minimizing the initial relations which depend on the underlying cryptographic primitives and assumptions. We illustrate our framework by proving IND-CPA security of the constructions of Bellare-Rogaway, Hash El Gamal and an encryption scheme proposed by Pointcheval.