

# Modular Soundness Proofs via Deduction Games (work in progress)

Hubert Comon-Lundh, Steve Kremer, and Joe-Kai Tsay

LSV, ENS Cachan & CNRS & INRIA

Currently, proofs of computational soundness of different equational theories cannot be easily composed; adding a cryptographic primitive to a given framework typically requires the construction of the soundness proof from the bottom up. Our long term aim is to present a framework which eases the combination of soundness proofs of equational theories under active attacks.

We present work in progress on a general security definition, which we call *deducibility game*. It is formulated as a game, in which a PPT attacker may either query bitstrings or terms to an oracle. Roughly, if the attacker submits a bitstring then the oracle returns a fresh name which is from now on associated to this bitstring. If the attacker submits a term, then the oracle generates the corresponding concrete instantiation. The symbolic names and terms that are sent during a game execution are recorded in a frame  $\varphi$ . The aim of the attacker is to produce a bitstring  $bs$  and a test  $\psi$  such that  $bs$  computationally satisfies  $\psi$ , but there is no term  $t$  which is deducible from  $\varphi$  and satisfies  $\psi$ .

Protocols are modelled in a general way as transition systems for which we define symbolic and computational protocol executions. For this model we formulate a trace mapping property, which is also the main ingredient to the soundness proofs for trace properties of, e.g., [4,3,2]. Intuitively, the trace property states that any computational trace corresponds to a symbolic trace, up to a negligible probability. In a first result we show that satisfying the deducibility game criterion implies trace mapping.

A notable difference of our trace mapping result, compared to [4,3,2], is that we do not rely on a parsing assumption for bitstrings. This allows us to study the computational soundness equational theories such as exclusive OR.

Similarly to [1], our work is directed at reducing the effort for proving soundness of different equational theories under active attacks. However, we are currently not working on embedding other calculi into our framework, instead our deducibility criterion should simplify the combination of soundness proofs for multiple equational theories.

In order to indicate the usefulness of the deducibility criterion, we show for the equational theory of public-key encryption that, if the implementation of the encryption scheme is IND-CCA2 secure, then an adversary's success probability in winning the deducibility game is negligible. We are currently investigating the soundness of the equational theory of exclusive OR, and how one can combine the proofs of different equational theory with respect to the deducibility criterion. In other future work, we would like to explore in how far the deducibility criterion can be used in combination with other criteria in order to obtain computational soundness of observational equivalence.

## References

1. Michael Backes, Dennis Hofheinz, and Dominique Unruh. Cosp: A general framework for computational soundness proofs. In *ACM CCS 2009*, pages 66–78, November 2009. Preprint on IACR ePrint 2009/080.
2. Véronique Cortier, Steve Kremer, Ralf Küsters, and Bogdan Warinschi. Computationally sound symbolic secrecy in the presence of hash functions. In Naveen Garg and S. Arun-Kumar, editors, *Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06)*, volume 4337 of *Lecture Notes in Computer Science*, pages 176–187, Kolkata, India, December 2006. Springer.
3. Véronique Cortier and Bogdan Warinschi. Computationally sound, automated proofs for security protocols. In *14th European Symposium on Programming Languages ESOP 2005*, pages 157–171, July 2005.
4. Daniele Micciancio and Bogdan Warinschi. Soundness of formal encryption in the presence of active adversaries. In *Theory of cryptography conference - Proceedings of TCC 2004*, pages 133–151, January 2004.