Computational soundness of observational equivalence*

Hubert Comon-Lundh† Véronique Cortier ‡

In [7], R. Canetti and J. Herzog consider (composable) security proofs for key exchange protocols. One of the main features of their work is to consider also a security property that is not a trace property: it requires indistinguishability between two versions of the protocol. They first rely on a composition theorem, showing that the security for an arbitrary number of sessions is implied by a one-session security. Then they design symbolic properties, corresponding to the computational ones and show that the symbolic abstraction of the protocol is sound w.r.t. these properties, for one session of the protocol. This allows to automate the security proofs, as described in [6] for instance.

Our work also aims at compositional computational security proofs through a symbolic abstraction. We claim to improve over [7] in the following respects:

1. We consider any indistinguishability property and prove that it is soundly abstracted by observational equivalence. This allows to consider many more security properties, such as for instance anonymity. In addition, this is a uniform way of abstracting properties. We do not need to introduce symbolic functionalities: we simply replace indistinguishability with observational equivalence.

2. We consider an arbitrary number of sessions: processes may be replicated. This is useful since we do not need to prove that one session security implies many-sessions security, while keeping the core of universal composability: observational equivalence of processes implies their security in any environment. In other words, our result allows to prove that a protocol is secure in any environment, without having to prove universal composability.

3. The secrets may be shared at any level: they can be local to a session, shared by one or more participants over sessions or even re-used in different protocols. This is specified at the symbolic level by the scope of the name generation.

To the best of our knowledge, the only general result relating observational equivalence and computational indistinguishability in an active attacker setting is [2], in which, however, cryptographic primitives are not part of the syntax.

We prove our result for symmetric encryption, relying on standard cryptographic assumptions (IND-CPA and INT-CTXT), but the same techniques can be applied to other security primitives such as signatures and public-key encryption. The proof requires the introduction of the concept of *tree soundness* in the case of passive attackers and the use of intermediate structures, which we called *computation trees*. These techniques are general and can be reused in other settings. A complete version of the result with full proofs can be found at [8].

Other related works include results for passive adversaries [1, 5, 12, 11] and for active adversaries, but for dedicated security properties: either trace properties [3, 7, 9, 10] or a special indistinguishability property [4, 7].

*This work has been partially supported by the grants ARA FormaCrypt and ANR AVOTÉ.
†ENS Cachan and Research Center for Information Security (RCIS), AIST, Tokyo
‡LORIA, CNRS & INRIA project Cassis

References

[1] M. Abadi, M. Baudet, and B. Warinschi. Guessing attacks and the computational soundness of static equivalence. In *Foundations of Software Science and Computation Structure (FoSSaCS'06)*, volume 3921 of *LNCS*, pages 398–412, 2006.

[2] P. Adão and C. Fournet. Cryptographically sound implementations for communicating processes. In *International Colloquium on Algorithms, Languages and Programming (ICALP'06)*, 2006.

[3] M. Backes and B. Pfitzmann. Symmetric encryption in a simulatable Dolev-Yao style cryptographic library. In *Computer Security Foundations Workshop (CSFW'04)*, 2004.

[4] M. Backes and B. Pfitzmann. Relating cryptographic und symbolic key secrecy. In *Symp. on Security and Privacy (SSP'05)*, pages 171–182, 2005.

[5] M. Baudet, V. Cortier, and S. Kremer. Computation- ally sound implementations of equational theories against passive adversaries. In *Proc. ICALP'05*, volume 3580 of *LNCS*, 2005.

[6] B. Blanchet, M. Abadi, and C. Fournet. Automated verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 75(1):3–51, 2008.

[7] R. Canetti and J. Herzog. Universally composable symbolic analysis of cryptographic protocols. In *Theory of Cryptography Conference (TCC'06)*, 2006.

[8] H. Comon-Lundh and V. Cortier. Computational soundness of observational equivalence. Research Report 6508, INRIA, 04 2008.

[9] V. Cortier and B. Warinschi. Computationally sound, automated proofs for security protocols. In *European Symposium on Programming (ESOP'05)*, volume 3444 of *LNCS*, pages 157–171, 2005.

[10] P. Laud. Symmetric encryption in automatic analyses for confidentiality against active adversaries. In *Symp. on Security and Privacy (SSP'04)*, pages 71–85, 2004.

[11] D. Micciancio and S. Panjwani. Adaptive security of symbolic encryption. In *Theory of cryptography Conference (TCC 05)*, volume 3378 of *LNCS*, pages 169–187, 2005.

[12] D. Micciancio and B. Warinschi. Completeness theorems for the Abadi-Rogaway language of encrypted expressions. *Journal of Computer Security*, 2004.