Computational Soundness without Symbolic Length Function

Hubert Comon-Lundh
ENS Cachan, France

Masami Hagiya
University of Tokyo, Japan

Yusuke Kawamoto
INRIA & ENS Cachan, France

Hideki Sakurada
NTT Communication Science Laboratories, Japan

Starting with the seminal work of Abadi and Rogaway, there have been several results showing the *computational soundness* of symbolic models: we do not miss any attacks when considering a symbolic model, provided that the cryptographic primitives satisfy certain properties based on the computational complexity theory.

An attacker in the computational model can indeed distinguish two messages if they have different length. If we wish to establish a soundness result for indistinguishability properties, we need a way to ensure that the symbolic attacker has the same length distinguishing capabilities as the computational attacker. However the computational length of the messages depends on the security parameter, while the symbolic length must be independent of the security parameter. For instance, consider the two messages $\langle u, u\rangle$ and $\{u\}^{r}_{\mathsf{ek}(k)}$. The length of these two messages may coincide for some values of the security parameter and not for others. In that case, there is no way to define a computationally sound symbolic length function that maps each symbolic term to its symbolic length.

The previous soundness results require strong assumptions on message lengths. The solution adopted in Comon-Lundh and Cortier, consists in assuming that the length of any cryptographic primitive applied to some arguments is a homogeneous function of the lengths of its arguments. Typically, in case of a linear function, the length $|[\![\langle u, v\rangle]\!]_\eta|$ of the computational interpretation of a pair, with respect to the security parameter η must be $\alpha \times |[\![u]\!]_\eta| + \beta \times |[\![v]\!]_\eta| + \gamma \times \eta$. Then, by induction, we may factor out η from the length of the interpretation of any term and get equalities/inequalities on lengths, independently of η. This is a strong restriction on the implementation since, for instance, the pairing operation cannot have a constant overhead; it depends linearly on the security parameter.

In the present work, we show a computational soundness of the observational equivalence of (a fragment of) the applied pi-calculus without using a symbolic length function. In our calculus, honest processes have a label for each input that represents an expected length of the input. They wait for input until they receive a bit string of the expected length in the computational model. As regards encryption, each ciphertext term has a label that is used only in the symbolic model to distinguish the encryptions of the plaintexts of different expected lengths, but is ignored when we compute the computational interpretation of the term. These labels are assumed to satisfy that, for any security parameter, the computational interpretation of a labeled term has an expected length if every variable occurring in the term is substituted by an input bit string of expected length. This assumption is weaker than assuming a symbolic length function, as all terms are not necessarily labeled in our symbolic model.