Computational Soundness of Symbolic XOR in the Presence of Active Adversaries

(Abstract)

Hideki Sakurada\textsuperscript{1}, Yusuke Kawamoto\textsuperscript{*,2}, and Masami Hagiya\textsuperscript{2}
sakurada at theory.brl.ntt.co.jp, \{y.kwmt, hagiya\} at is.s.u-tokyo.ac.jp
\textsuperscript{1}NTT Communication Science Laboratories, NTT Corporation
\textsuperscript{2}Department of Computer Science, University of Tokyo, Japan

The applied pi calculus and the observational equivalence \cite{1} are used in many studies to define and analyze security of protocols.

Comon-Lundh and Cortier \cite{2} give the computational semantics of the calculus and prove the computational soundness of the observational equivalence. In their proof, computation trees that represent behaviors of processes and equivalence relation over the trees are used to bridge the observational equivalence and the computational indistinguishability. Comon-Lundh \textit{et al.} \cite{3} extend their result and prove the soundness without assuming a polynomial-time parsing function.

In this work, we apply the latter approach to the applied pi calculus extended with the XOR operator and compare it with the former approach from the viewpoint of the soundness result for the XOR operator.

References


*The author is supported by JSPS Research Fellowship.