YASSINE LAKHNECH, University of Grenoble, CNRS - VERIMAG
Computational Indistinguishability Logic

Computational Indistinguishability Logic is a logic for reasoning about cryptographic primitives in computational models. It captures reasoning patterns that are common in provable security, such as simulations and reductions. CIL is sound for the standard model, but also supports reasoning in the random oracle and other idealized models. We illustrate the benefits of CIL by discussing several case studies.