Formal Aspects of Anonymity

Robert Morelli

UUCS-02-006

School of Computing
University of Utah
Salt Lake City, UT 84112 USA

January 15, 2002

Abstract

We present a formal definition of anonymity in the context of concurrent processes. The definition is given in category theoretic terms. Moreover, the concept of a split cofibration is shown to both simplify the analysis of anonymity as well as to increase the framework's expressiveness. Because of its categorical nature, our definition is largely independent of any specific model of concurrency. We instantiate the theory to two specific models, Hoare trace languages and probabilistic transition systems. By providing a semantics for CSP, the former model endows CSP with a definition of anonymity that applies to every CSP process simulation. The latter model, probabilistic transition systems, provides a definition of anonymity applicable to probabilistic processes. This seems to be the first general such definition.