Fachbereich
Computerwissenschaften

„Probabilistic Anonymity via Coalgebraic Simulations “

Ichiro Hasuo, Kyoto Univ., JP and Radboud Univ. Nijmegen, NL
http://www.cs.ru.nl/~ichiro

There is a growing concern on anonymity and privacy on the Internet, resulting in lots of work on formalization and verification of anonymity. Especially, importance of probabilistic aspect of anonymity is claimed recently by many authors. Among them are Bhargava and Palamidessi who present the definition of probabilistic anonymity for which, however, proof methods are not yet elaborated. In this paper we introduce a simulation-based proof method for probabilistic anonymity. It is a probabilistic adaptation of the method by Kawabe et al. for nondeterministic anonymity: anonymity of a protocol is proved by finding out a forward/backward simulation between certain automata. For the jump from non-determinism to probability we fully exploit a generic, coalgebraic theory of traces and simulations developed by Hasuo, Jacobs and Sokolova. In particular, an appropriate notion of probabilistic simulations is obtained by instantiating a generic definition with suitable parameters.

Wo Jakob-Haringer-Straße 2, HS T02
Wann Mittwoch, 16. Jänner 2007, 16:00 h Kontakt: Dr. Ana Sokolova