Interactive Information Flow
(Invited Talk)

Catuscia Palamidessi[1], Mário S. Alvim[1], and Miguel E. Andrés[2]

[1] INRIA and LIX, École Polytechnique Palaiseau, France
[2] Institute for Computing and Information Sciences, The Netherlands

Abstract. In recent years, there has been a growing interest in considering the quantitative aspects of Information Flow, partly because often the a priori knowledge of the secret information can be represented by a probability distribution, and partly because the mechanisms to protect the information may use randomization to obfuscate the relation between the secrets and the observables.

We consider the problem of defining a measure of information leakage in interactive systems. We show that the information-theoretic approach which interprets such systems as (simple) noisy channels is not valid anymore when the secrets and the observables can alternate during the computation, and influence each other. However, the principle can be retrieved if we consider more complicated types of channels, that in Information Theory are known as channels with memory and feedback. We show that there is a complete correspondence between interactive systems and such kind of channels. Furthermore, the proposed framework has good topological properties which allow to reason compositionally about the worst-case leakage in these systems.

References

1. Andrés, M.E., Palamidessi, C., van Rossum, P., Smith, G.: Computing the leakage of information-hiding systems. In: Proc. of TACAS (2010) (to appear)
2. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: Anonymity protocols as noisy channels. Inf. and Comp. 206(2-4), 378–401 (2008)
3. Clark, D., Hunt, S., Malacaria, P.: Quantified interference for a while language. In: Proc. of QAPL 2004. ENTCS, vol. 112, pp. 149–166. Elsevier, Amsterdam (2005)
4. Desharnais, J., Jagadeesan, R., Gupta, V., Panangaden, P.: The metric analogue of weak bisimulation for probabilistic processes. In: Proc. of LICS, pp. 413–422 (2002)
5. Malacaria, P.: Assessing security threats of looping constructs. In: Proc. of POPL, pp. 225–235. ACM, New York (2007)
6. James, M.: Causality, feedback and directed information. In: Proc. of the International Symposium on Information Theory and its Applications, Honolulu (1990)
7. Smith, G.: On the foundations of quantitative information flow. In: de Alfaro, L. (ed.) FOSSACS 2009. LNCS, vol. 5504, pp. 288–302. Springer, Heidelberg (2009)
8. Tatikonda, S., Mitter, S.K.: The capacity of channels with feedback. IEEE Transactions on Information Theory 55(1), 323–349 (2009)

A. Armando and G. Lowe (Eds.): ARSPA-WITS 2010, LNCS 6186, p. 111, 2010.