Abstract channels, gain functions and the information order

CC Morgan[1] and G Smith[2]

[1] School of Computer Science and Engineering, UNSW, Australia
[2] School of Computing and Inf. Sciences, Florida International University, USA

In [1] a partial order was proposed for information channels, and given a formulation based both on testing (using gain functions) and structure (channel composition). These two formulations were almost shown to be equivalent, and the not-quite-proved portion was named the "Coriaceous Conjecture."

In [2] a denotational semantics was proposed for probabilistic programs with non-interference-style security, including a partial *program-refinement* order "is at least as secure as" suitable for it.

The two groups [1, 2] discovered their common goals in November 2012 [3], in particular that their two independently formulated orders agreed in their intentions. As a result, later that month [4] the Coriaceous Conjecture was shown to hold [5] — the two orders are indeed isomorphic.

This order, in its structural formulation, appears nicely to generalise the *Lattice of Information* order [6] from its original qualitative formulation to a quantitative formulation, as required when probabilities are taken into account; and the new order has many interesting properties, e.g. related to completeness (of the partial order), and to probability measures. It does not however seem to be a lattice.

The talk we will give at FCS, based on work with all our colleagues [1, 2], will describe how this order arose, the domain of "abstract channels" a.k.a. "hyper-distributions" that it synthesises, will speculate on what the order's significance might be, and will give a sketch of why we do not think it is a lattice.

Is that a challenge, or an opportunity?

References

1. M. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith. Measuring information leakage using generalized gain functions. *Proc. 25th IEEE CSF* pp265–279. 2012.
2. A. McIver, L. Meinicke, and C. Morgan. Compositional closure for Bayes Risk in probabilistic noninterference. *Proc. ICALP*, LNCS 6199 pp223–35. Springer, 2010.
3. A. McIver. Shonan meeting on *Quantitative methods in security- and safety-critical applications.* November 2012.
   `www.nii.ac.jp/shonan/blog/2012/03/08/`
   `/quantitative-methods-in-security-and-safety-critical-applications/`
4. B. Köpf, P. Malacaria, C. Palamidessi. Dagstuhl seminar 12481 *Quantitative Security Analysis.* November 2012.
   `//www.dagstuhl.de/en/program/calendar/semhp/?semnr=12481`
5. A. McIver, L. Meinicke, and C. Morgan. Draft proof of the Coriaceous Conjecture.
   `www.dagstuhl.de/mat/index.en.phtml?12481`
6. J. Landauer and T. Redmond. A lattice of information. CSFW 1993, pp65–70.