Hamilton Institute

Information Theory, Security and Privacy

Flavio du Pin Calmon
Research Laboratory of Electronics, MIT

Tuesday, July 30, 2013

Abstract

In this talk we discuss a few of our recent results on using information-theoretic tools to design and analyze security and privacy systems. In the first part of the talk, we present a new information-theoretic definition of security and associated results, based on list decoding in a source coding setting. We begin by presenting list-source codes, which naturally map a key length (entropy) to a list size. We then show that such codes can be analyzed in the context of a novel information-theoretic metric, namely epsilon-symbol secrecy, that encompasses both the one-time pad and traditional rate-based asymptotic metrics. We derive fundamental bounds for epsion-symbol secrecy and demonstrate how these bounds can be achieved with MDS codes when the source is uniformly distributed.

In the second part of the talk, we discuss a general statistical inference framework to capture the privacy threat incurred by a user who releases data to a passive but curious adversary given utility constraints. We show that applying this general framework to the setting where the adversary uses the self-information cost function naturally leads to a non-asymptotic information-theoretic approach for characterizing the best achievable privacy subject to utility constraints. Based on these results we introduce two privacy metrics, namely average information leakage and maximum information leakage. We prove that under both metrics the resulting design problem of finding the optimal mapping from the user's data to a privacy-preserving output can be cast as a modified rate-distortion problem which, in turn, can be formulated as a convex program.

Venue: Seminar Room, Hamilton Institute, Science Building, NUI Maynooth

Time: 2.00 - 3.00pm

Travel directions are available at www.hamilton.ie

IEEE
CC Ireland Chapter