Synchronized Chaos for Authentication and Communication

William Langford
wlangfor@uoguelph.ca
University of Guelph

A "chaotic" dynamical system has trajectories which never repeat themselves, and appear to have random behaviour, even though they remain completely deterministic. Locally, nearby trajectories separate exponentially in time. Yet, Pecora and Carroll (1990) showed that two chaotic dynamical systems can be synchronized with a scalar signal. This inspired several proposals to use "synchronized chaos" as a masking scheme for secure communication. In each case, mathematical analysis led to algorithms for unmasking the signal, based on the underlying deterministic property. In this work, we exploit the deterministic property of a chaotic dynamical system to present an authentication and communication scheme, which works through a modular arithmetic filter. This filter removes the information exploited by existing unmasking algorithms. A receiver possessing the secret "key" is still able to synchronize with the sender. (Joint work with Steven Sladewski.)