Practical Realization of a Return Map Immune Chaotic Stream Cipher in Circuitry

D.R. Brown D. Materassi

October 13, 2016

Abstract

The chaotic Lorenz attractor system has a unique property that allows it to self-synchronize with a like system through a single shared state. Using a plain text binary message a single system parameter can be modulated to mask this message and transmit it securely through the single shared state. The most simple methods of this encryption technique are, however, vulnerable to the return map attack. Using a time-scaling factor to further obfuscate the modulation process, a return map attack immunity is gained. We report on the progress towards a realization of this process in real-time analog circuitry using off-the-shelf components and minimal processing power.