Abstract Submitted
for the DFD19 Meeting of
The American Physical Society

Cryptographic analysis of chaotic fluid flows[1] WILLIAM GILPIN, Harvard Quantitative Biology Initiative — In computer science, hash functions are elementary operators that convert arbitrary-length inputs into finite-length outputs. We describe a direct analogy between these functions and the motion of particles advected by fluid flows, and we show that, when the governing flow is chaotic, hydrodynamic hash functions exhibit statistical properties typically associated with hash functions used for digital cryptography. These include non-invertibility, sensitivity to initial input, and avoidance of collisions, in which two similar inputs produce the same output. We show that this analogy originates from the tendency of certain chaotic flows to braid together particle trajectories across space in time in an irreducible manner, and we describe how techniques used to probe the properties of digital hash functions may be used to characterize the properties of flows when only limited observational data is available. Our findings have potential applications as microfluidic proof-of-work systems, as well as for characterizing large-scale transport by ocean flows and biological microswimmers.

[1]Harvard Quantitative Biology Initiative, NDSEG Fellowship

William Gilpin
Stanford University

Date submitted: 30 Jul 2019 Electronic form version 1.4