Contribution ID: **126** Type: **poster**

ARC4 stream cipher as a nonlinear mixing dynamical system

Due to outspread of WiFi technology, which utilized stream ciphers, ARC4 has once become the most widespread stream cipher in the world. The idea of the cypher is to use a deterministic dynamics, with strong mixing properties in order to produce a pseudorandom trajectory of symbols, identically distributed, with minimal correlations. A pair of ARC4 sharing common initial condition (secret key) is used to produce the same trajectory on the encrypting and decrypting side.

The aim of this contribution is to show a few results, which may be obtained if we apply standard techniques of nonlinear dynamics to a trajectory generated by some cryptographic system.

The first effect we show is a relation between Renyi entropy distribution of the pseudorandom string and the quality of the key. Various strategies for key selection introduce variability in the minimum and the peak of entropy distribution.

The second effect we show is the nonuniform distribution of sum of two consecutive samples (a digraph). Families of digraphs revealing certain anomalies were known before, but application of the return map, shows a nonuniform probability certain area of phase space in Takens reconstruction. Hence, the generator is distinguishable from random, although the timeseries look completely random.

Some successful attacks upon RC4 have relied on a fact, quite nonlinear in spirit, that within the transient phase, the system did not loose information about its initial conditions fast enough, which produced correlations, which were utilized to reveal the key, and decipher the message. A lack of standard nonlinear operation: i.e. omission of transients led to compromitation of the whole WiFi technology (WEP). Current findings confirm that application of nonlinear techniques in cryptology may provide interesting results.

Primary author: BUCHNER, Teodor (Faculty of Physics, Warsaw University of Technology)

Presenter: BUCHNER, Teodor (Faculty of Physics, Warsaw University of Technology)