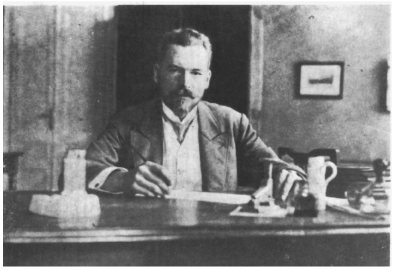

Contribution ID: **45** Type: **poster**

Weak initial conditions of RC4 pseudorandom number generator

Thursday, 6 September 2018 15:00 (3 hours)

Phase space of cryptographic systems, such as RC4 stream cipher is an interesting object, to which statistical physics may be applied. Entropy of a trajectory and of a state space, transient phase, coexisting attractors, 1/f noise and complexity measures are just a few examples of physical ideas, that may be applied to cryptographic systems, which opens the possibility of many new research subjects. The basis for this interdisciplinary research is the fact, that pseudorandom number generators, which form a core of many cryptographic systems, are just strongly mixing deterministic nonlinear systems in a chaotic state. And the main difference lays in the fact, that basic operations in cryptography, such as XOR operator are in space of integer numbers (as in Bernoulli shift).

In this contribution we expose a weakness of RC4 cipher: that apparently strong cryptographic keys of high entropy can lead to weak initial condition for the pseudorandom number generator. These weak initial conditions lead to poor mixing in the long transient part of a pseudorandom trajectory. This allows to mount a successful attack on this cipher, e.g. using known plaintext attack. We show this by numerical analysis of the space of initial conditions of a simplified version of RC4. We show, that central limit theorem may be applied to this system, and due to this fact many families of weak cryptographic keys may be determined. Basing on these results it is possible to calculate the average weakness of space of all cryptographic keys, which shows an inherent security flaw, built in the structure of priming phase of the RC4 cipher. Current findings confirm that application of nonlinear techniques in cryptology may provide interesting results.

Primary author: Mr KUBAŃ, Aleksander (Faculty of Physics, Warsaw University of Technology)

Co-author: Dr BUCHNER, Teodor (Faculty of Physics, Warsaw University of Technology)

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

Session Classification: Poster session