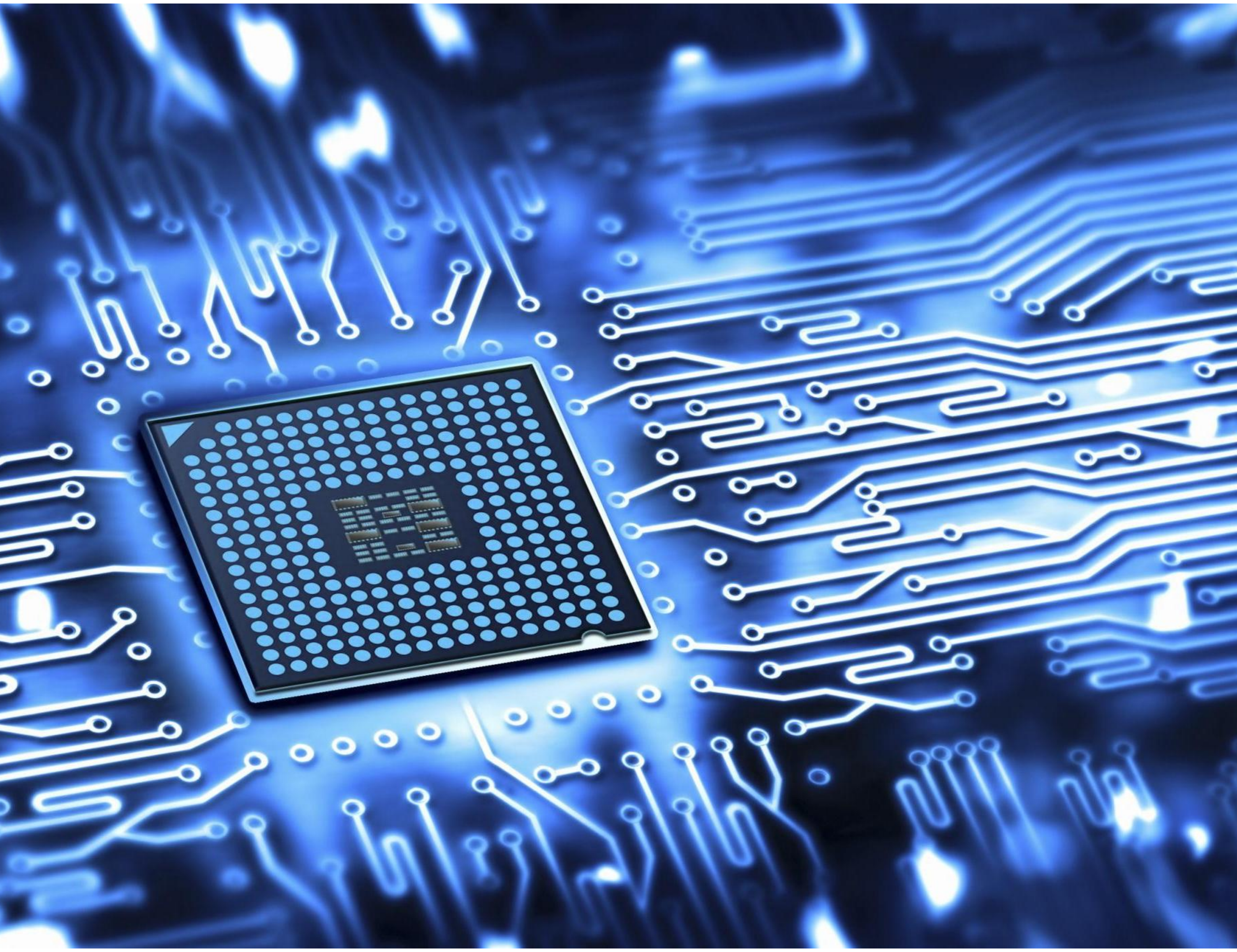
Integrated & Embedded Systems Laboratory



Chaos Based Cryptography

Poznan 2016

Chaos-based cryptography

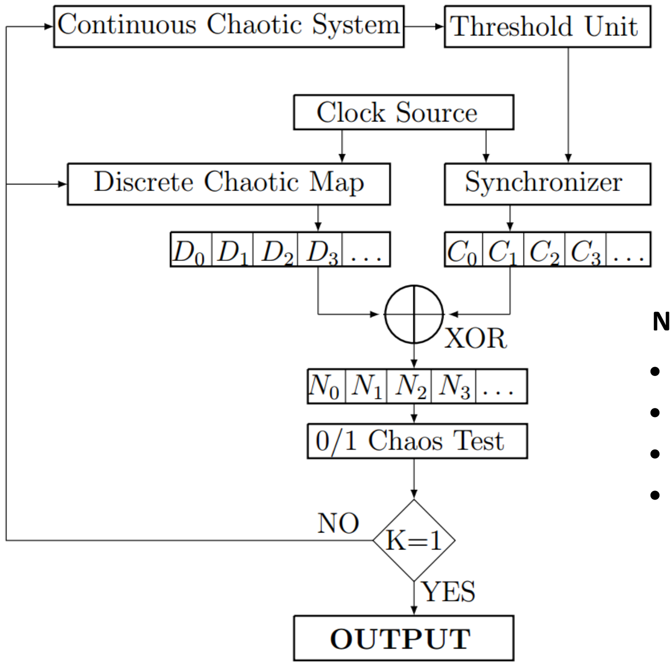
Abstract

Generator was developed to improve security in hardware chaos-based cryptography. The generator has an improved level of chaotic properties in comparison with the existing single source (input) digital chaotic bit generators. The 0-1 test is used to show the improved chaotic behavior of our generator having a chaotic continuous input (Chua, Rössler or Lorenz system) intermingled with a discrete input (logistic, Tinkerbell or Henon map) with various parameters. The obtained sequences of bits have random nature, with increased entropy levels, even in the cases of small number of bit representations.

Highlights / Key features

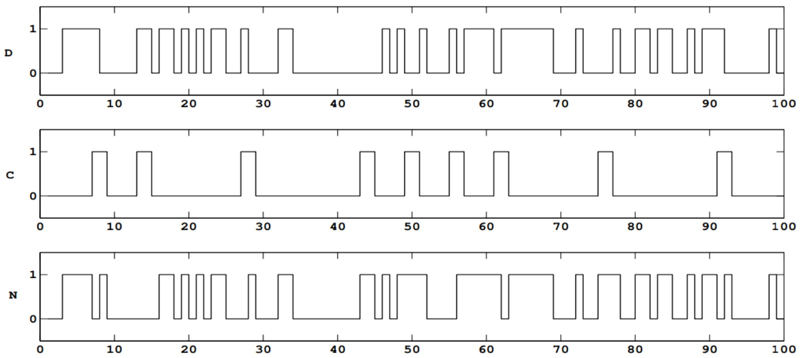
- improving security in the chaos based cryptography;
- level of entropy similar to entropy of quantum randomness;
- implementation using FPAAs and FPGA;
- adaptation of 0-1 test for chaos in chaos-based cryptography

A hybrid chaos-based pseudo-random bit generator


Continuous Chaotic System
Threshold Unit
Clock Source
Discrete Chaotic Map
Synchronizer
D_0 D_1 D_2 D_3 . . .
C_0 C_1 C_2 C_3 . . .
XOR
N_0 N_1 N_2 N_3 . . .
0/1 Chaos Test
NO
K=1
YES
OUTPUT

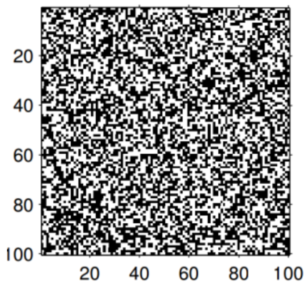
New chaotic generator with mixed-mode inputs

- standalone hardware security module as TRBG
- prevention of periodicity in the chaotic signals
- hardware implementation using FPGA and FPAA
- possibility of integration with any embedded system

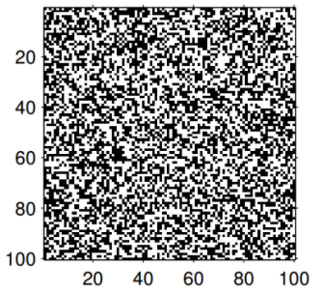


Sequences of chaotic bits

Chaos Based Cryptography

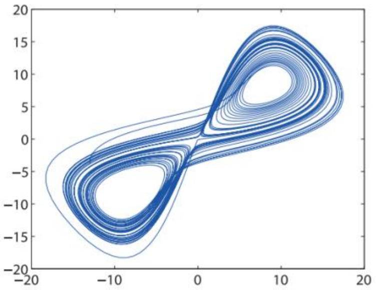


QUANTIS random bits

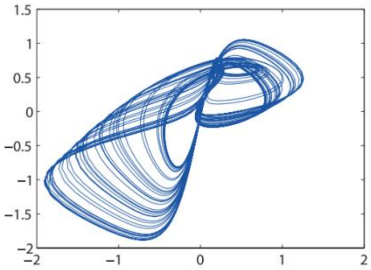


Hybrid chaotic bits

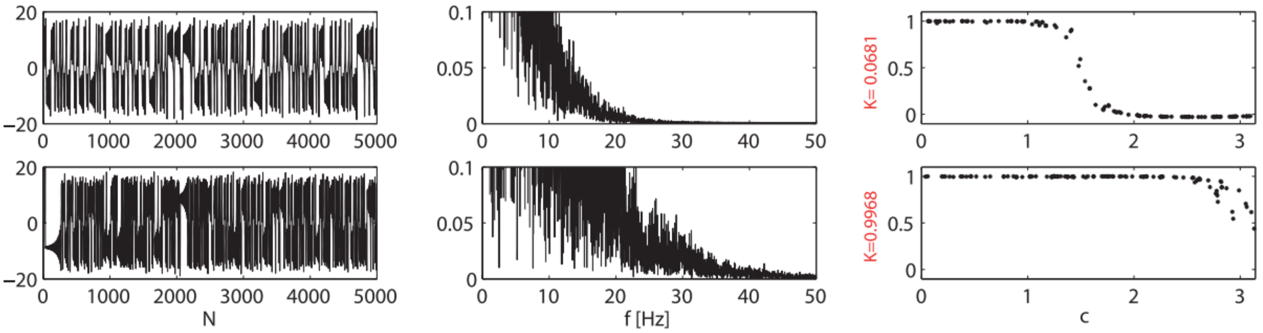
New chaotic generator with mixed-mode inputs has similar level of randomness as commercial quantum random generator from ID Quantique (IDQ). Proposed generator is much easier in practical use and in the integration in modern embedded cryptographic systems than IDQ solutions.



Lorenz attractor



Memristor attractor



New method of prevent oversampling in 0-1 test for chaos

Main Contributions

M. Melosik, W. Marszałek, Using the 0-1 test for chaos to detect hardware trojans in chaotic bit generators Electronics Letters, vol. 52, no. 11, pp. 919-921, 2016, IF=0.93

M. Melosik, W. Marszałek, On the 0/1 test for chaos in continuous systems, Bull. Pol. Ac.: Tech vol. 64, no. 3, pp. 521-528 IF=0.94

Chaos Based Cryptography

Hardware trojans in chaos-based cryptography

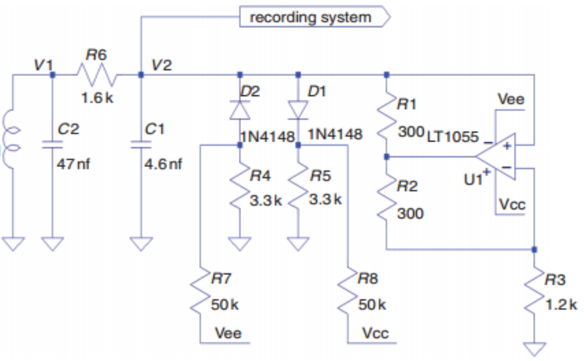
Abstract

The use of the 0-1 test for chaos to monitor chaotic bit generators susceptible to unauthorised changes and modifications of the circuits' parameters (hardware trojans) is presented. The 0-1 test proves that the chaotic nature of the continuous time signals is inherited by the bit sequences even when a simple threshold comparator is used. Simulation results for selected chaotic circuits are presented.

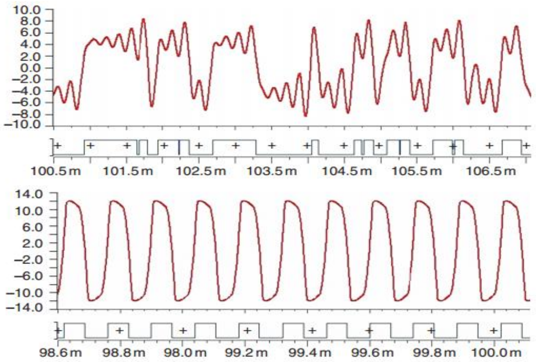
Highlights / Key features

- detecting hardware trojnas directly on PCB;
- development of hardware trojans for selected chaotic generators;
- demonstration of vulnerability to hardware attacks;

Trojans in continuous chaotic system



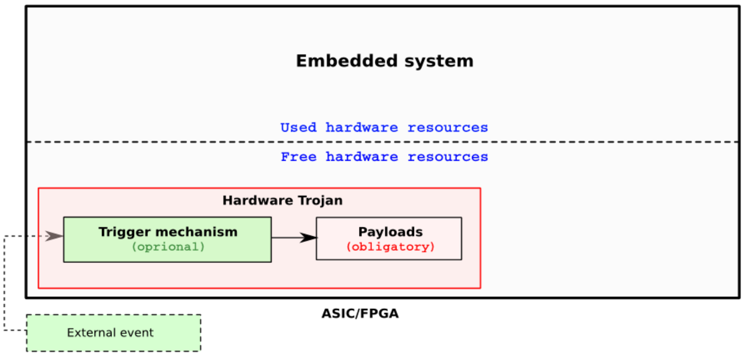
Chua chaotic circuit



Trojan results

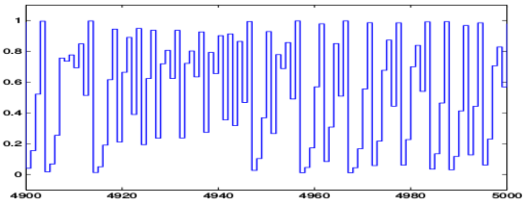
The extension of the research presented in **IEEE Design & Test, 2015** (S. Ghosh, A. Basak, S. Bhunia *How secure are printed circuit boards against trojan attacks?*)

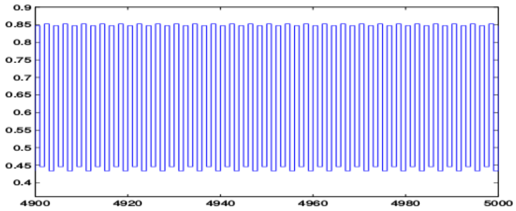
Trojans in continuous chaotic system

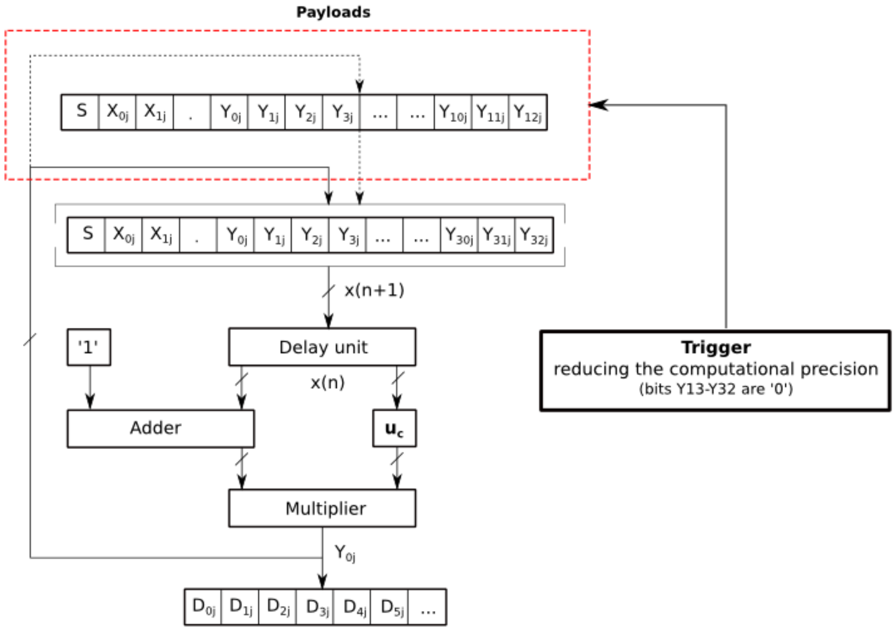


Structure of hardware trojan

Chaos Based Cryptography







Hardware trojan in chaotic logistic map

Development of possible hardware trojans in digital chaotic generators based on FPGA architectures.

Main Contributions

M. Melosik, W. Marszałek, A hybrid chaos-based pseudo-random bit generator in VHDL-AMS, IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS 2014), College station Texas, USA

W. Marszałek, M. Melosik, Circuits with Mixed Mode Oscillations in VHDL-AMS, IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS 2013) Columbus, Ohio, USA