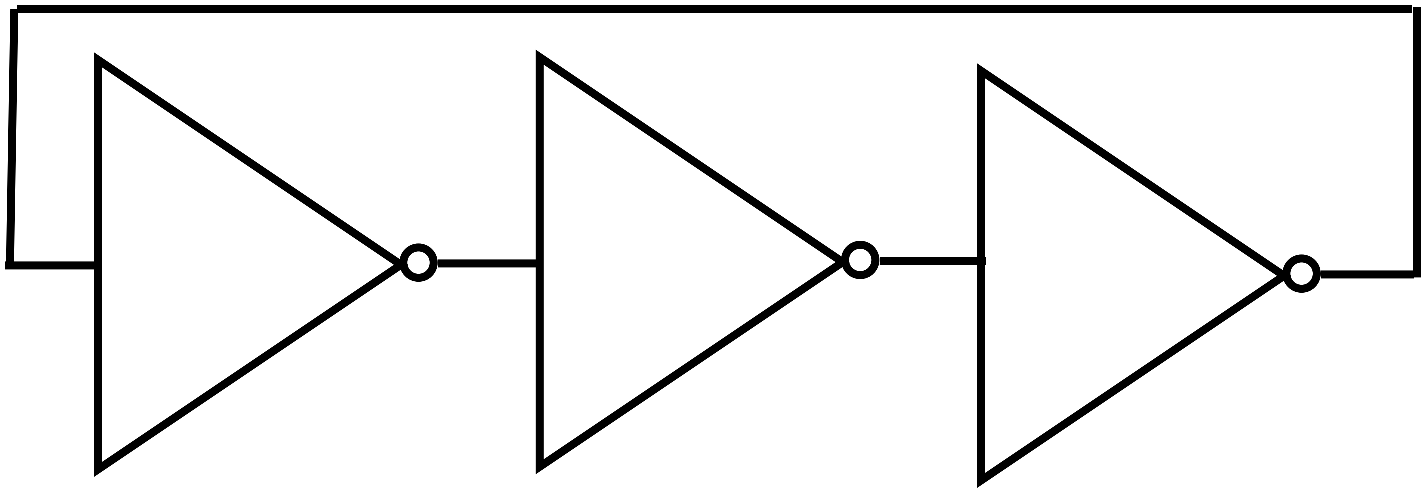
Fibonacci Ring Oscillators as True Random Number Generators A Security Risk

Markus Dichtl

Why classical ring oscillators take so long to achieve randomness?



Jitter means random variations in the period length of the RO. But most jitter contributions are (partially) eliminated by others. It takes n periods to achieve an accumulated jitter proportional to √n.

Faster Digital TRNGs

In 2004, Jovan Golić (Telecom Italia) invented two strongly improved variants of ROs,

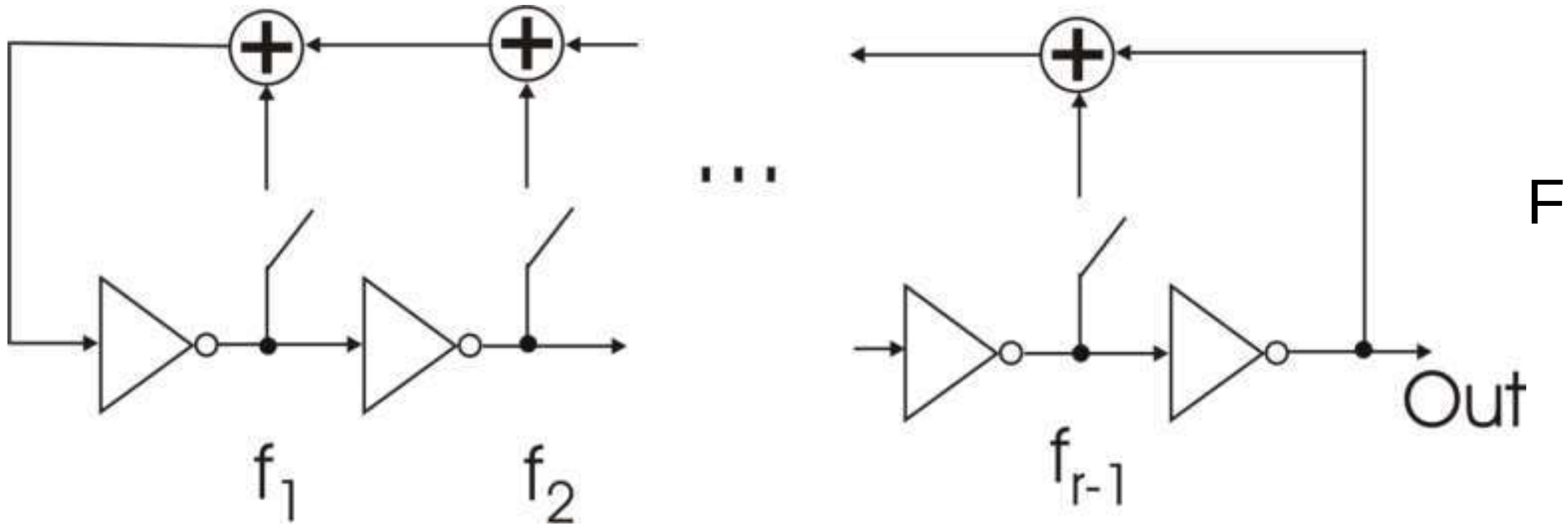
Fibonacci ring oscillators (**FIRO**) and

Galois ring oscillators (**GARO**)

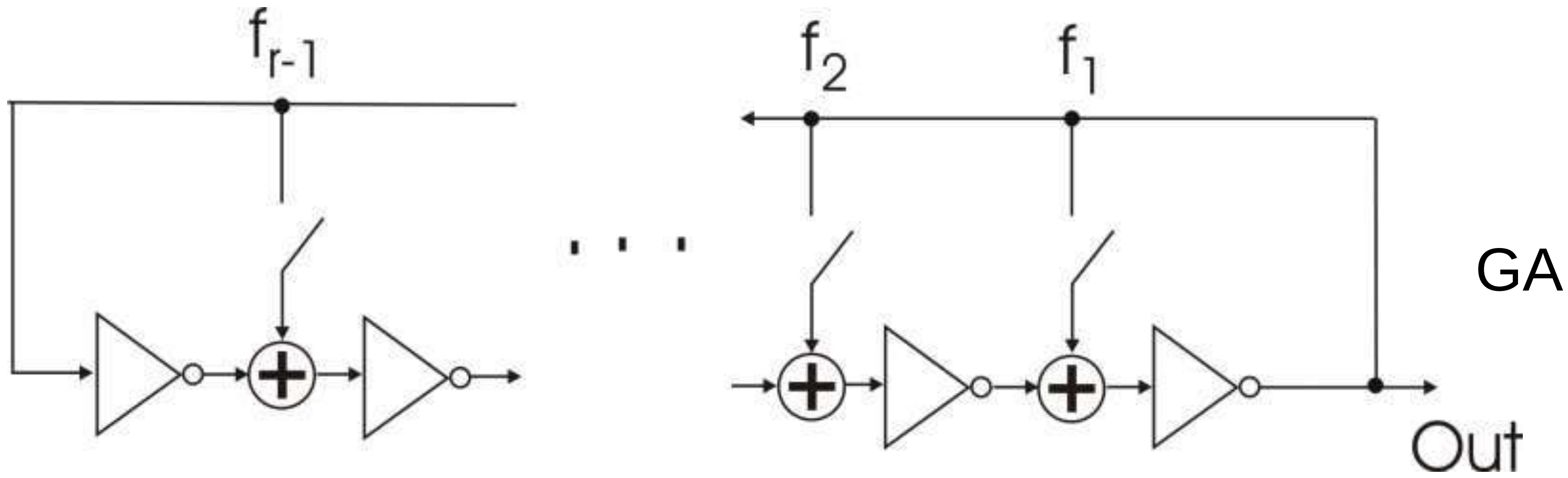
The designs show similarities with Fibonacci and Galois LFSRs, albeit the registers are replaced with inverters

J. Dj. Golić , “New Methods for Digital Generation and Postprocessing of Random Data,” IEEE Trans. Computers, vol. 55(10), pp. 1217-1229, Oct. 2006

FIROs and GAROs

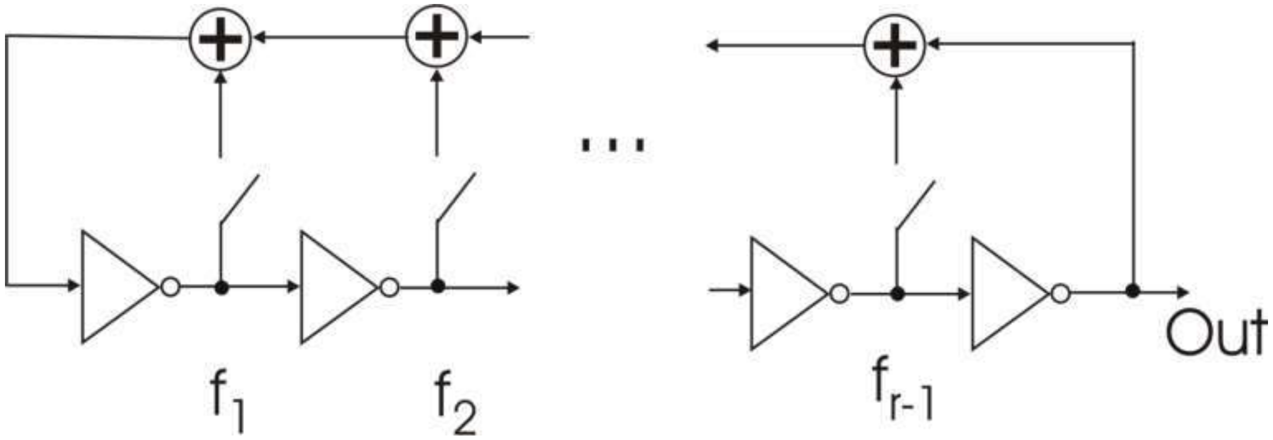


FIRO



GARO

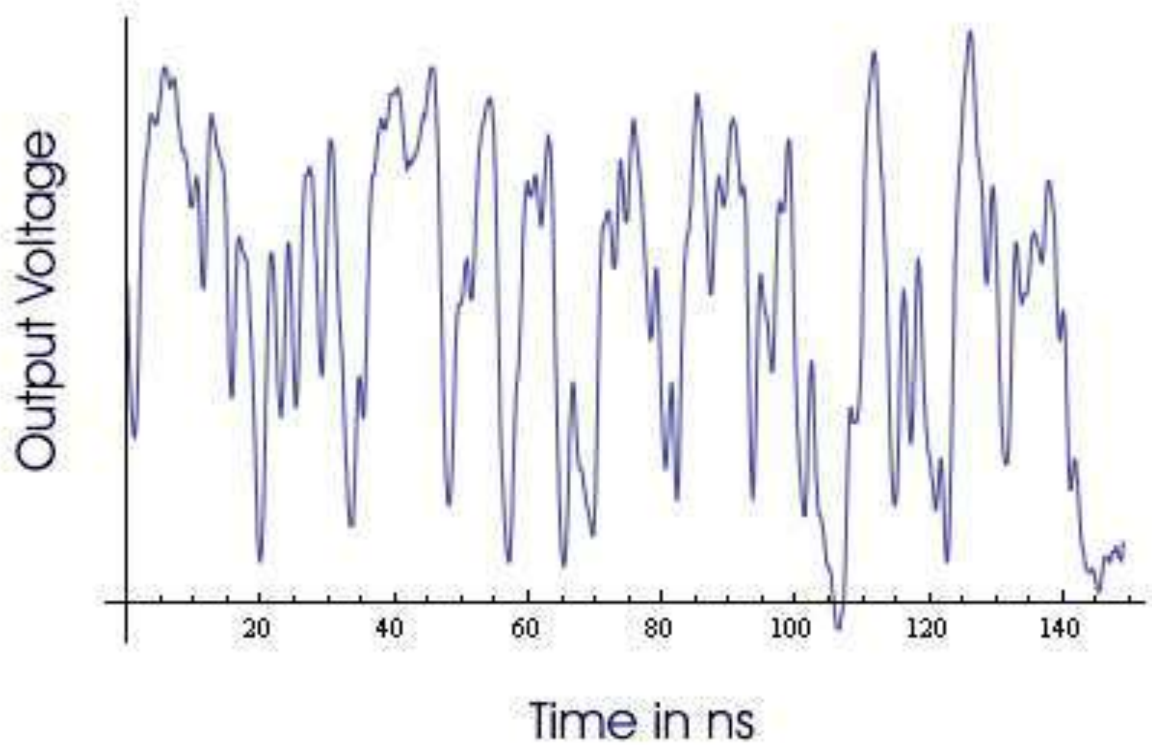
How can FIROs and GAROs achieve randomness faster?



When a signal is subject to a random timing variation, very quickly afterwards the variation branches out to several copies of the signal. This drastically reduces the risk of the jitter contribution to be eliminated.

FIROs and GAROs are assumed to oscillate chaotically.

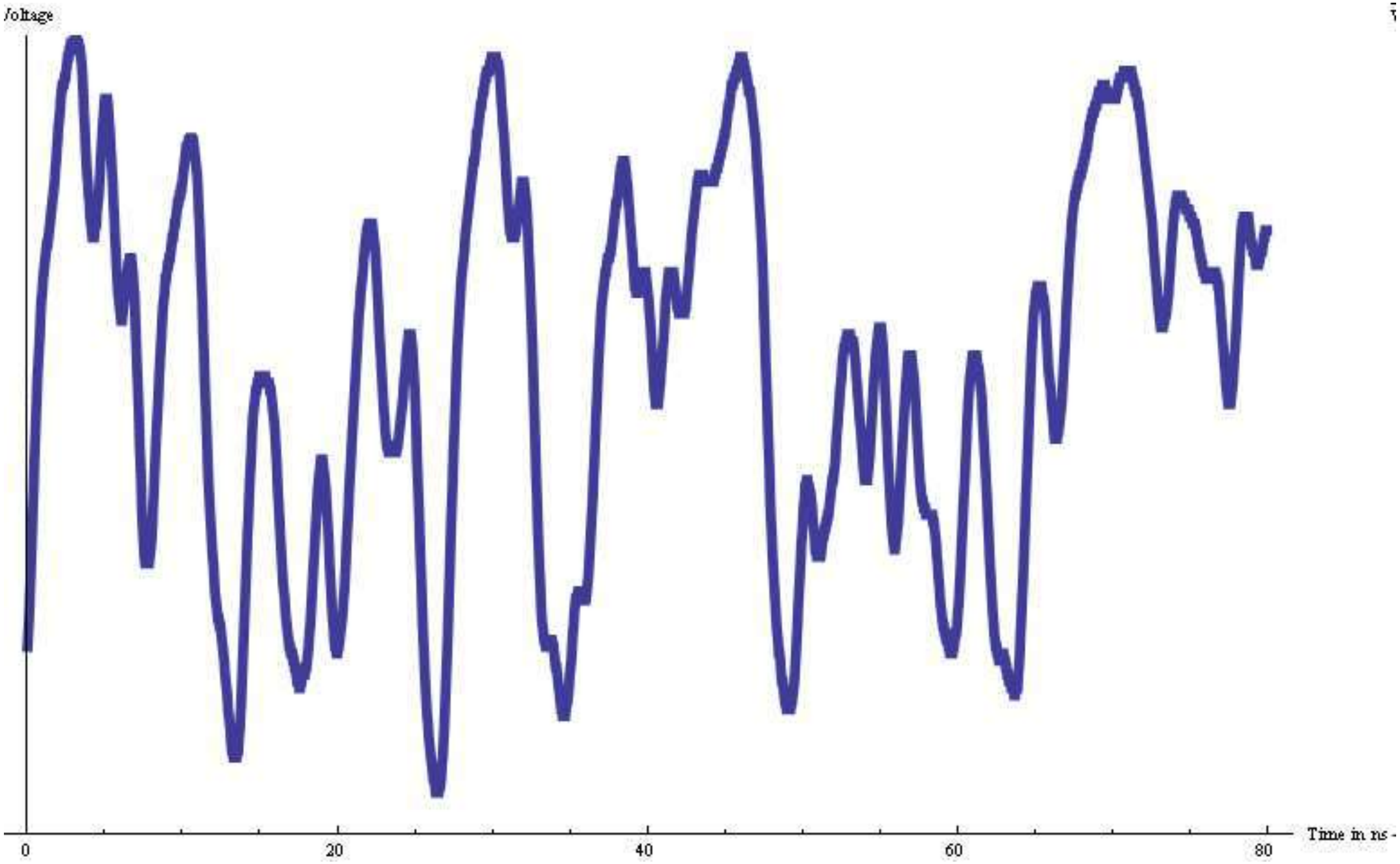
Starting a FIRO from a static state



(Feedback polynomial $x^{15}+x^{14}+x^{7}+x^{6}+x^{5}+x^{4}+x^{2}+1$)

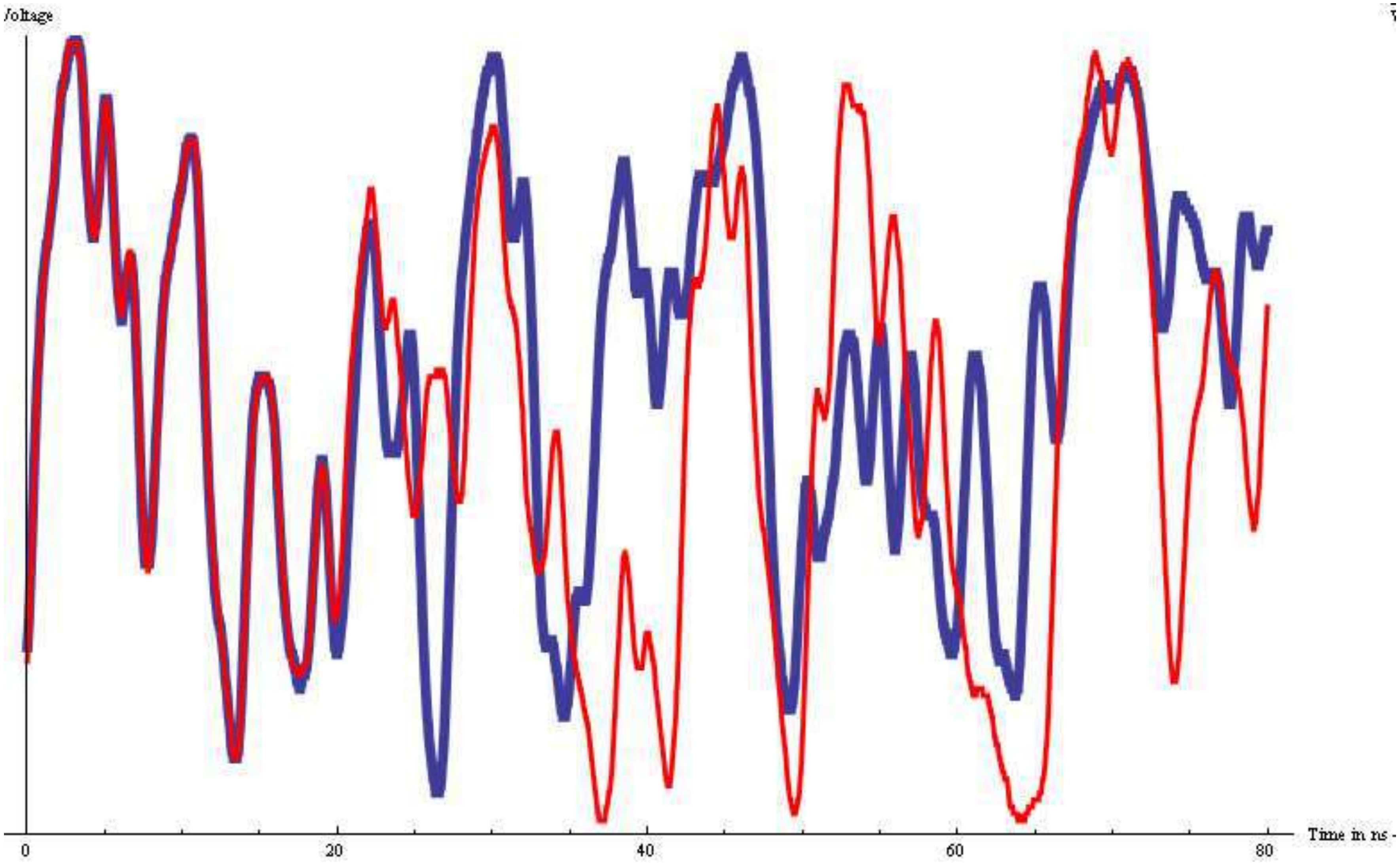
Is this random?

Restarting a FIRO from identical states I



Restricted © Siemens AG 2017

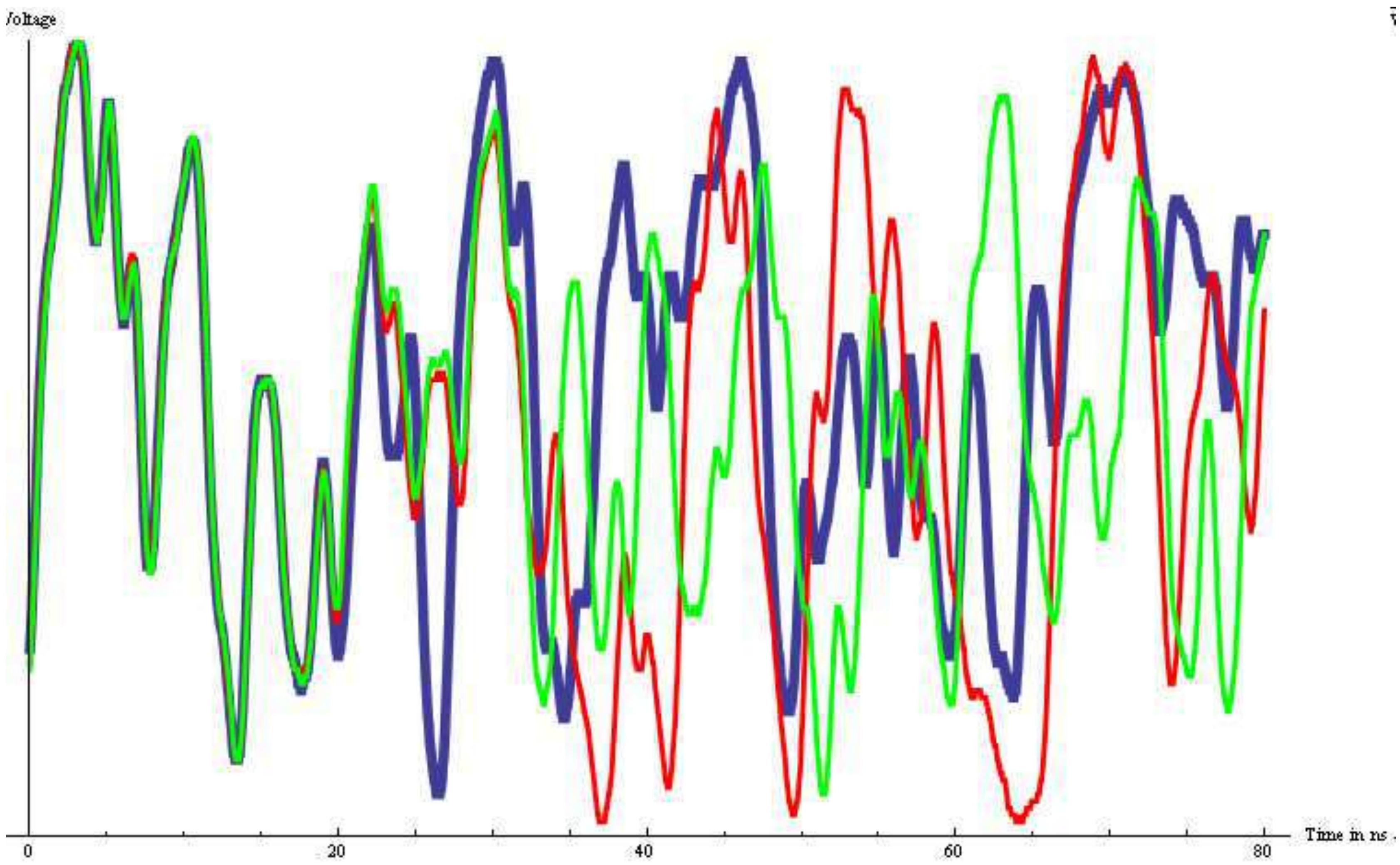
Restarting a FIRO from identical states II



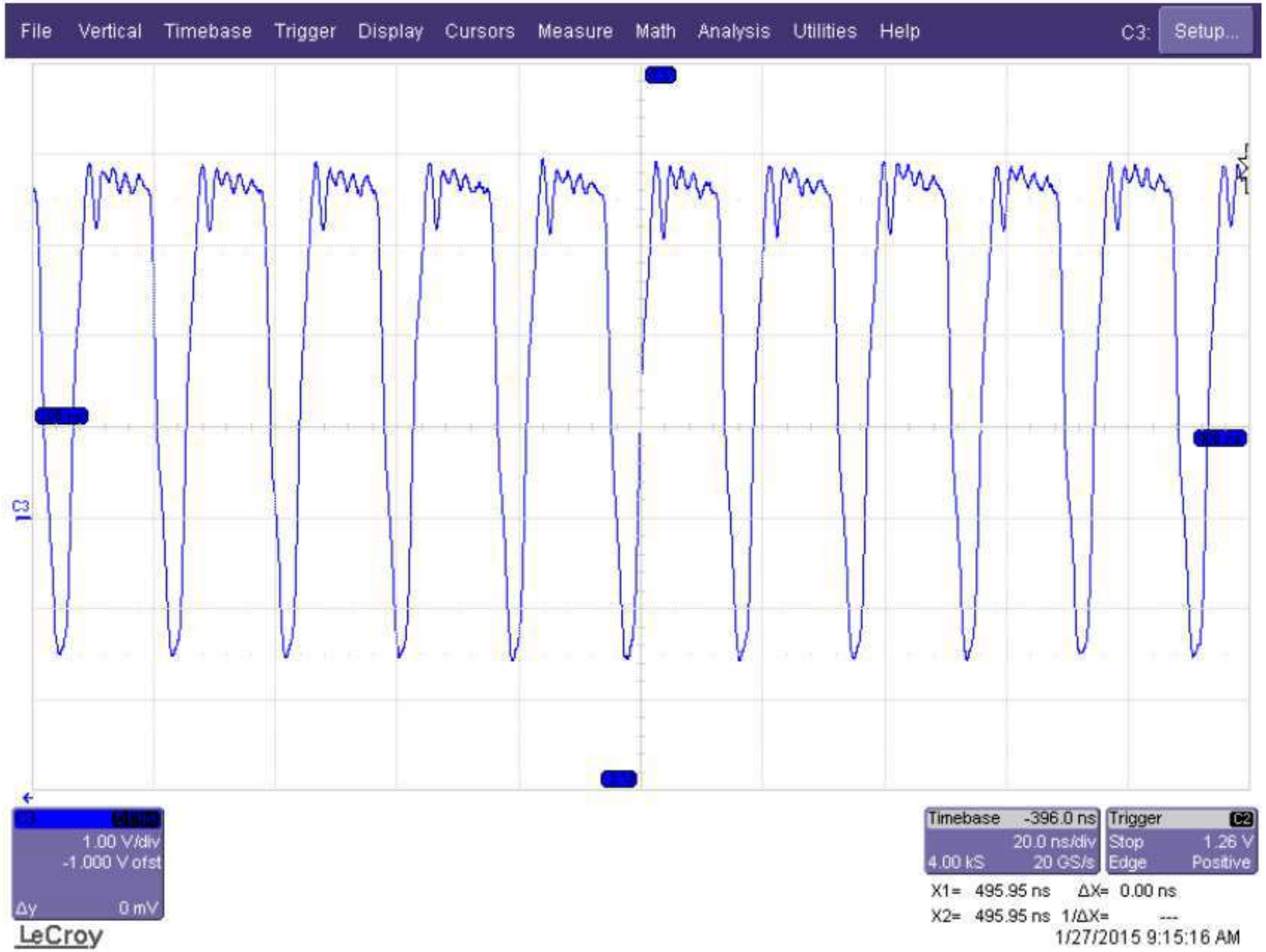
Restarting a FIRO from identical states III

SIEMENS

Ingenuity for life



But...



C3 1.00 V/div -1.000 V ofst Δy 0 mV

Timebase -396.0 ns 20.0 ns/div 4.00 kS 20 GS/s

Trigger C2 Stop 1.26 V Edge Positive

X1= 495.95 ns ΔX= 0.00 ns
X2= 495.95 ns 1/ΔX= ---
1/27/2015 9:15:16 AM

Oscillogram of a periodic FIRO oscillation

Feedback polynomial
$x^{16} + x^7 + x^2 + 1$

Periodic FIRO oscillations were already reported for very short FIROs in the paper

„Dichtl, Golic: Highspeed True Random Number Generation with Logic Gates Only“ at CHES 2008

For the periodic oscillations, jitter accumulates as poorly as for classical ROs

Many questions

Is this a very rare phenomenon?

How rare?

Is it really periodic?

What does it really mean to be periodic?

How to find out periodicity automatically?

Can we live with TRNGs which **probably** work correctly?

Looking for a suitable quantitative evaluation

Evaluation of thousands of oscilloscope traces seemed doable (automatically), but not really desirable.

The prefered approach was the determination of periodic behaviour on the FPGA board.

The idea was to **sample all inverters of the FIRO simultaneously** and periodically in order to extract as much information as possible about the state.

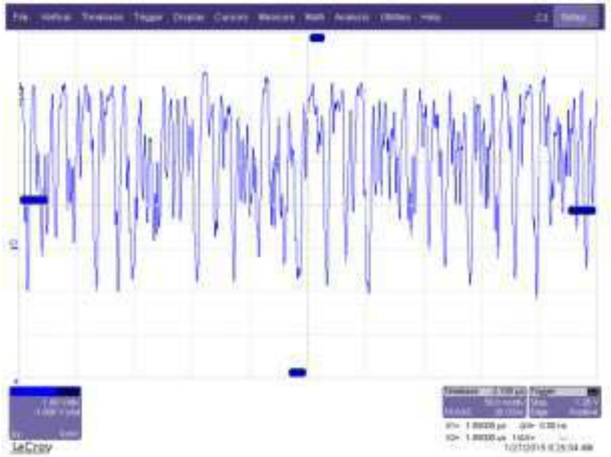
Temporarily separated: Aquisition of the data and their download from the FPGA board.

The distinguishing feature

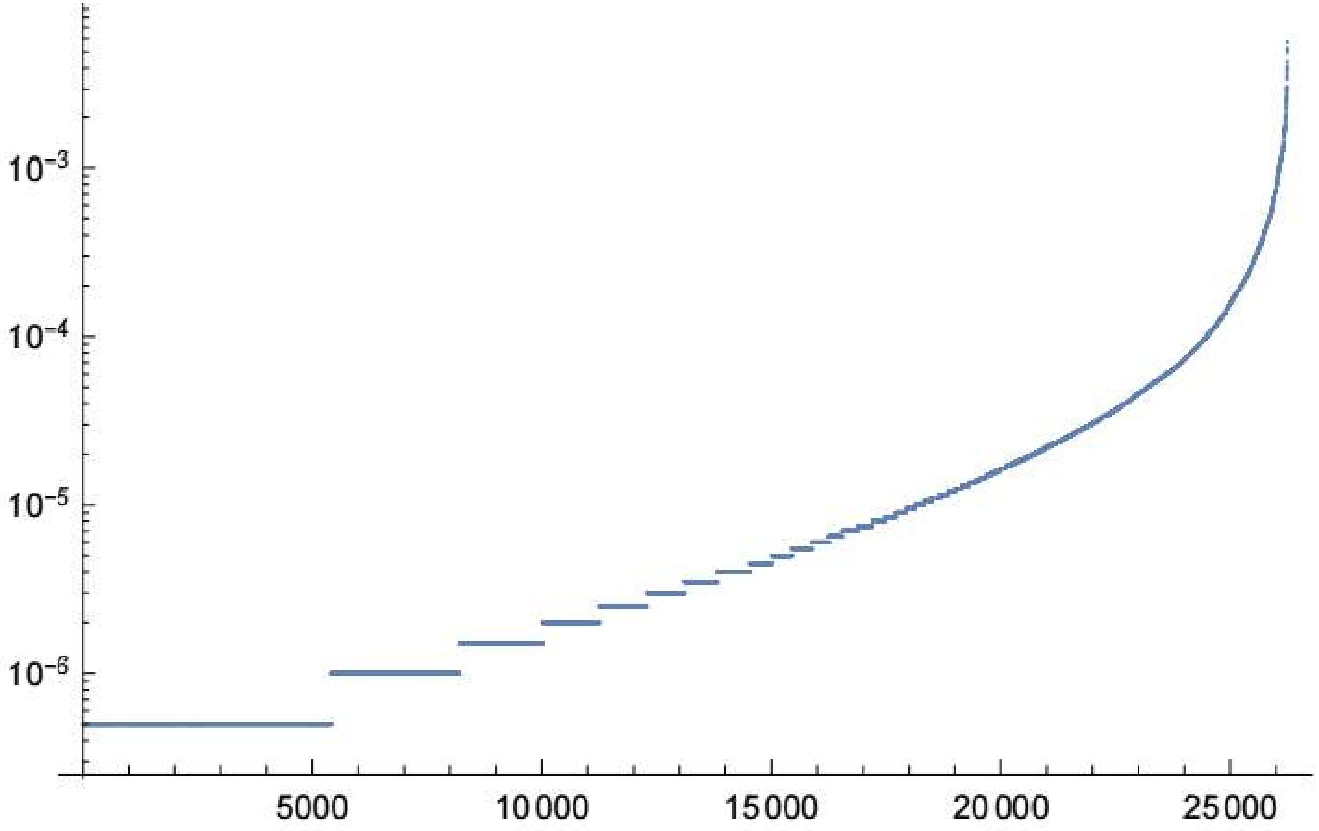
For **periodic** oscillations, there are **few different patterns sampled**.
For **chaotic** oscillation, there are **many different patterns sampled**.

Sampling every 600ns, 10000 samples:
Previous periodic case: only 63 different samples

Chaotic case, feedback polynomial $x^{16} + x^{6} + x^{3} + 1$: 3442 different samples



For the chaotic case, probabilites of the patterns vary enormously



Sorted probabilities (logarithmic ordinates) of 2 million samples from a chaotic FIRO oscillation. The feedback polynomial was again $x^{16} + x^6 + x^3 + 1$

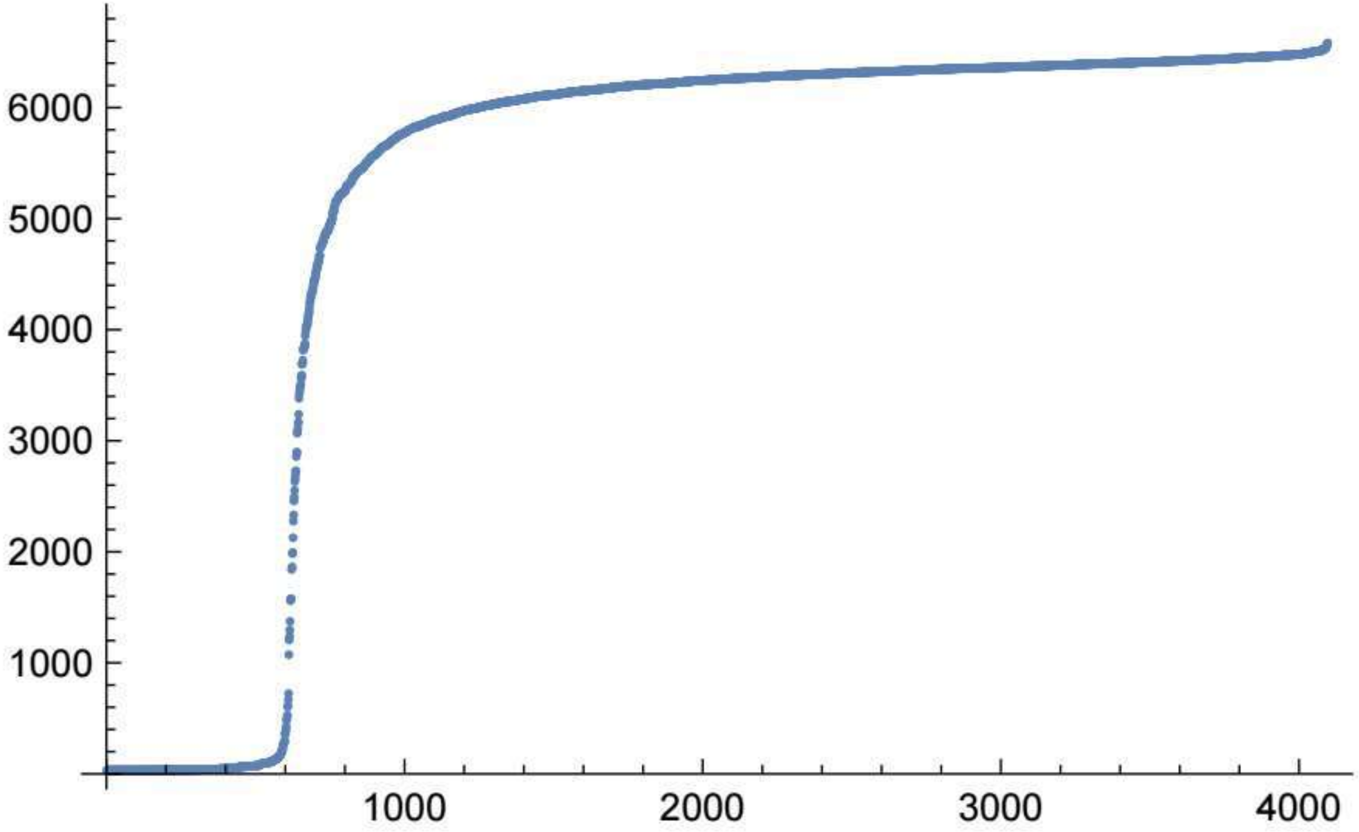
Systematically trying (almost) all FIROs of length 16

The fixed point free FIROs of length 16 were tried out systematically, however feedback from the first inverter output to ist input was excluded. This resulted in 4096 feedback configurations.The systematic generation was implemented on the FPGA.

In each case, the FPGA was started from a fixed inital state, and 10000 16 bit samples were taken with a temporal separation of 600ns. The samples were stored in RAM.

For each feedback configuration, the number of different samples was determined.

The number of different samples for FIRO length 16, sorted



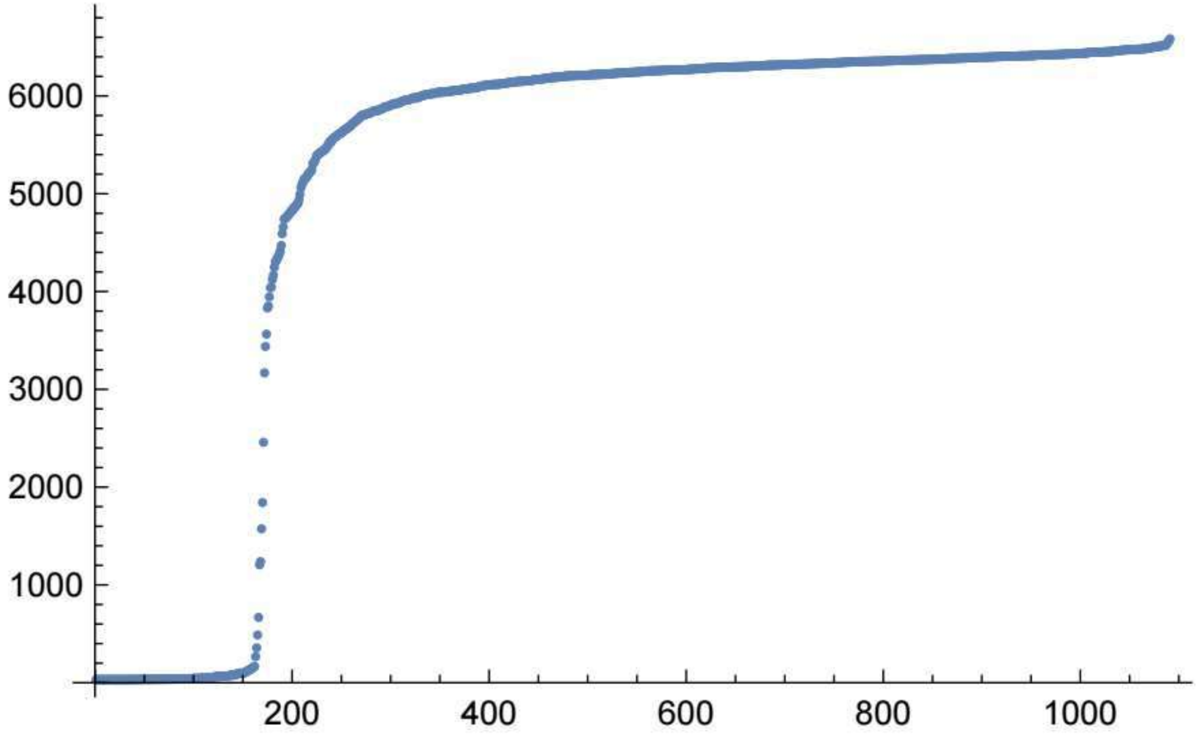
Among the 4096 FIROs of length 16, in 542 cases (13.23%) 100 or less different samples were observed, a clear indication of periodic oscillation.

A TRNG design which fails with a probability of 13.23% inacceptible.

What about the intermediate cases?

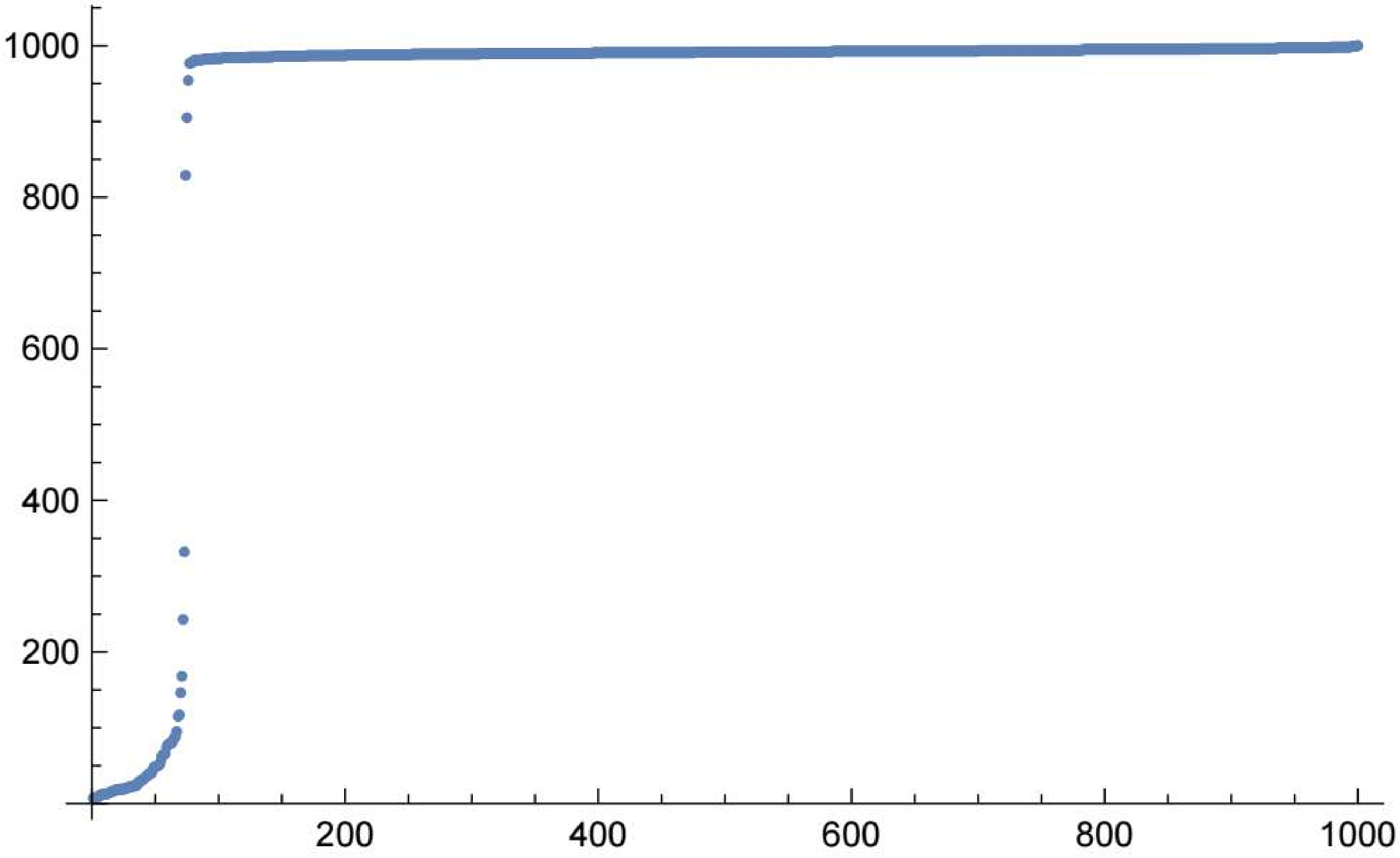
Are the failures due to ignoring a irreducibility criterion required by Jovan Golic?

SIEMENS
Ingenuity for life



In order to determine the influence of the Golic irreducibility criterion, the subset of 1091 cases of the 4096 which meet the Golic criterion were evaluated separately.
In 13.84 % of the cases, there were 100 or less different patterns.
This does not imply that the Golic criterion makes things worse. This is just statistics.

Do longer FIROs help?

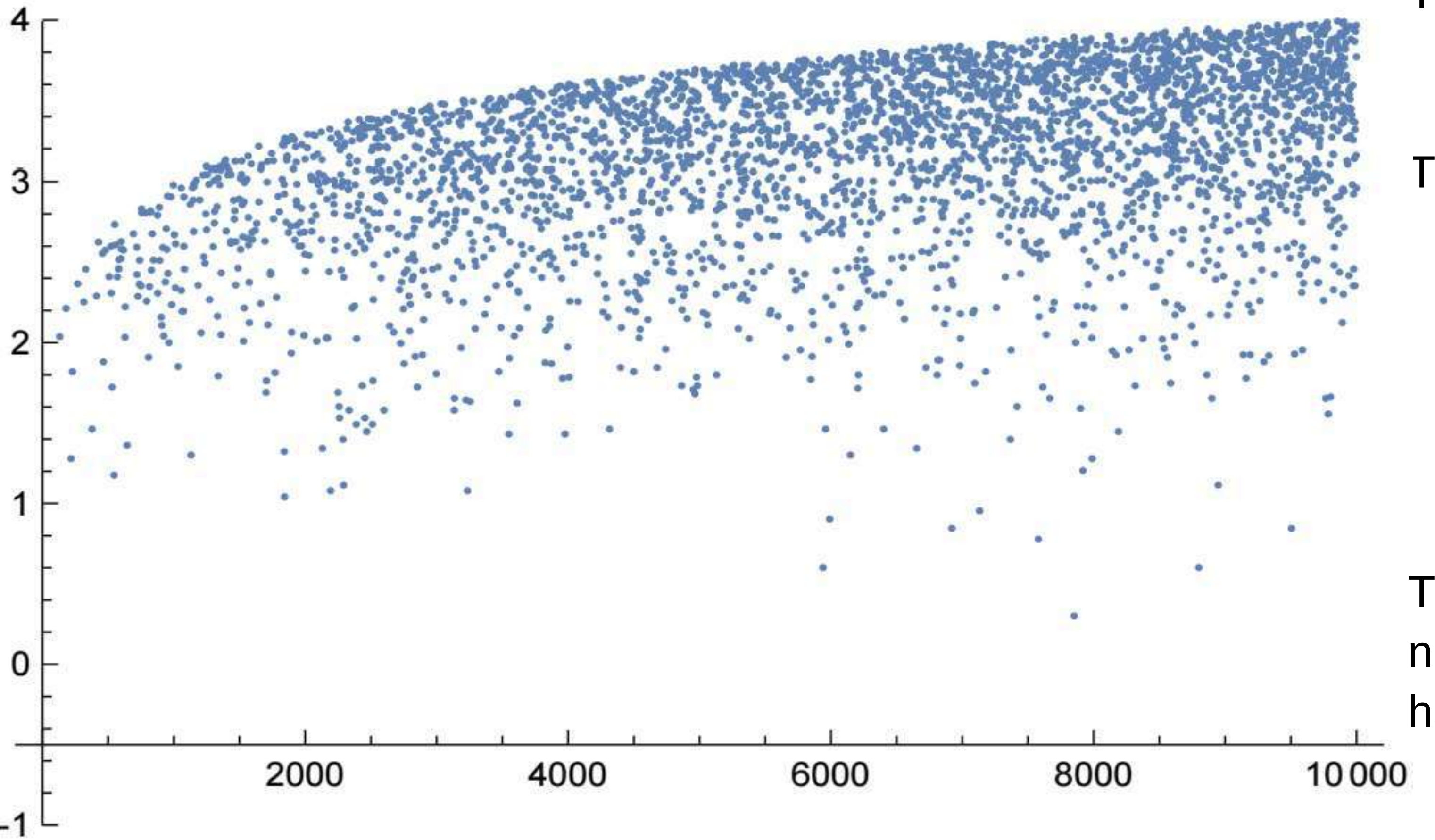


Somewhat. For 1000 random fixed point free FIROs of length 32 meeting the Golic criterion, the number of different 32-bits samples among the 1000 taken was determined.

In 6.7 % of the cases, less than 100 different patterns occurred.

However, it is quite impossible to compare the 16- and 32-bit results.

A new kind of images helps to understand FIROs with intermediate numbers of different samples



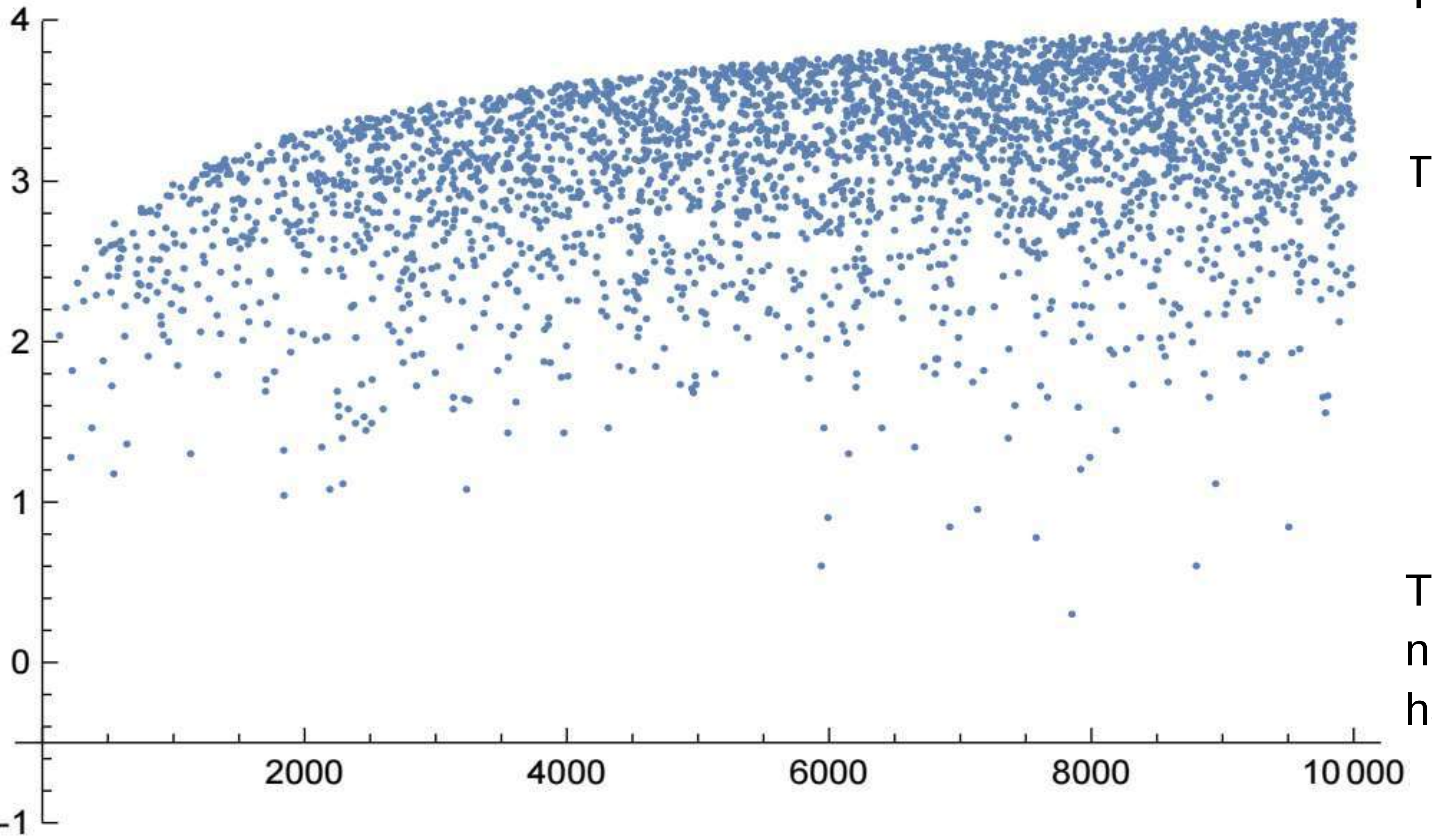
The abscissa represents the sequence of samples in time.

The ordinate of a dot represents how many samples earlier the pattern sampled at the time of the abscissa was sampled the last time previously.If the sample has not occurred previously, there is no dot.

The figure shows the decimal logarithm of the number of samples the sampled 16 bit value has been sampled before for the last time

Permanently chaotic oscillation

A new kind of images helps to understand FIROs with intermediate numbers of different samples



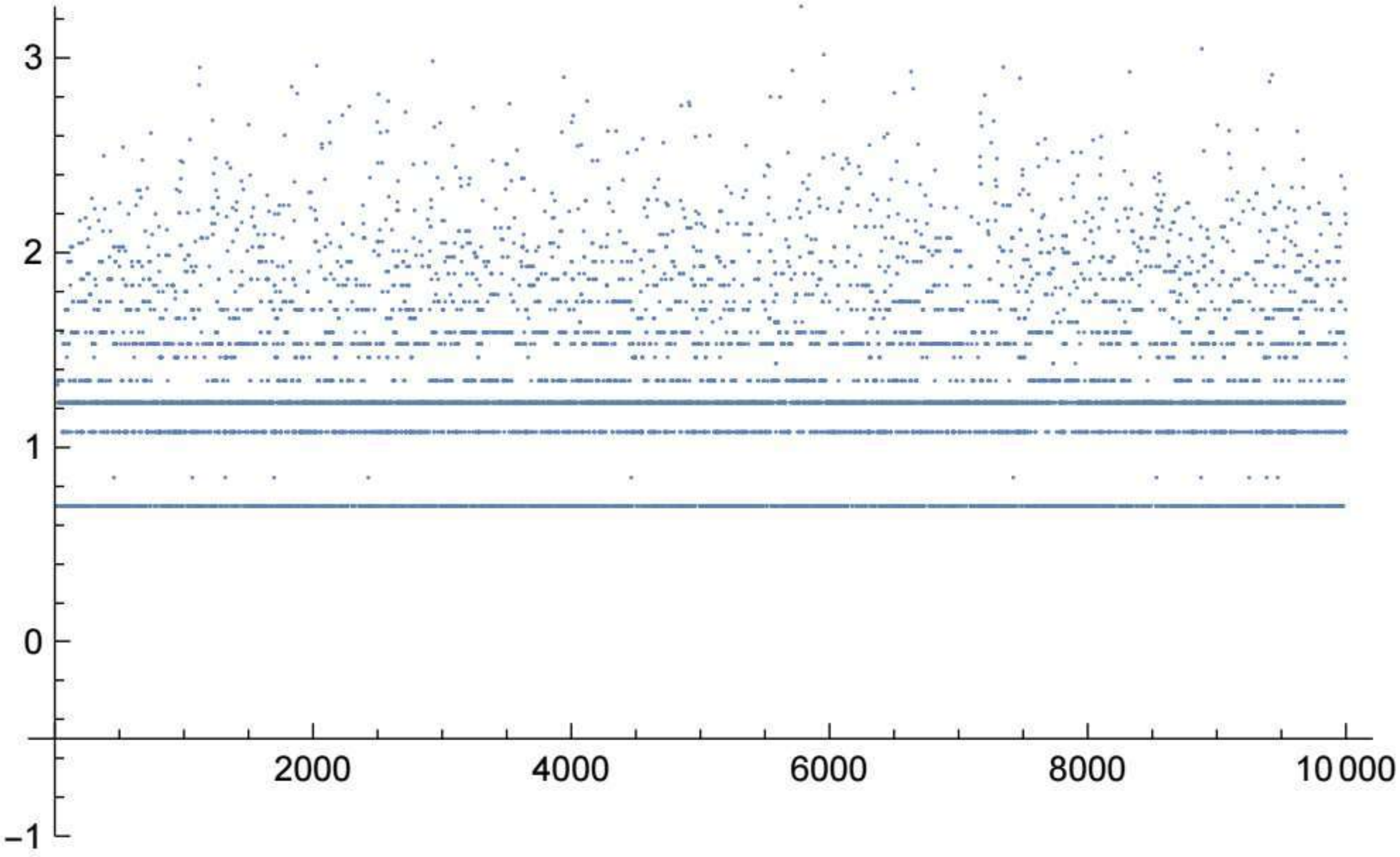
The abscissa represents the sequence of samples in time.

The ordinate of a dot represents how many samples earlier the pattern sampled at the time of the abscissa was sampled the last time previously.If the sample has not occurred previously, there is no dot.

The figure shows the decimal logarithm of the number of samples the sampled 16 bit value has been sampled before for the last time

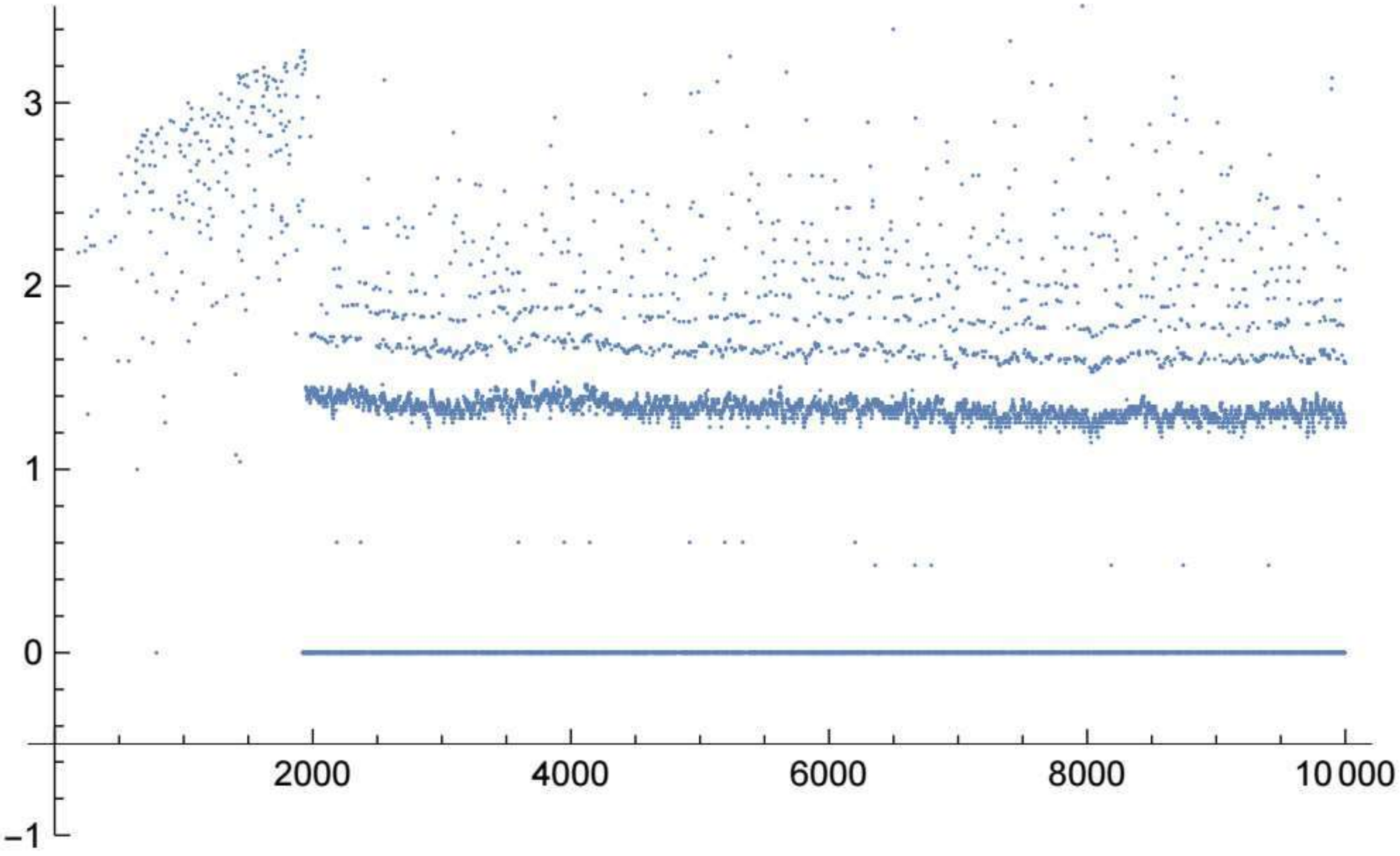
Permanently chaotic oscillation

The new kind of image for a periodic oscillation



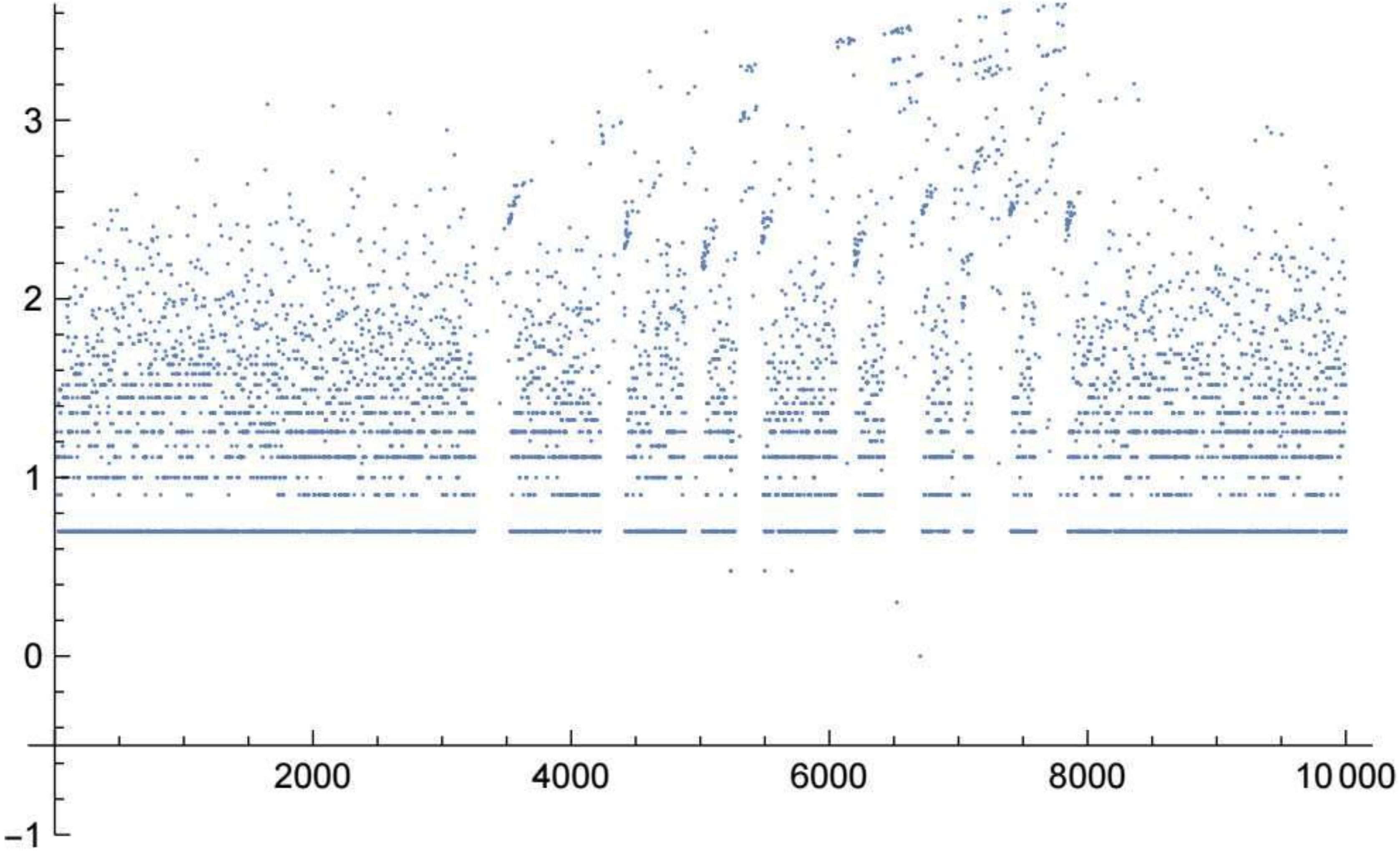
FIRO starting chaotically, continuing periodically

SIEMENS
Ingenuity for life



FIRO starting periodically, occasional chaos

SIEMENS
Ingenuity for life



Conclusions

SIEMENS
Ingenuity for life

- TRNGs remain a challenging topic
- Periodic FIROs may be detected by the methods used in this presentation, but this requires much more FPGA resources
- There are no good or bad feedback polynomials, as the behaviour depends strongly on the individual chip
- To use GAROs instead of FIROs would be the wrong conclusion, as they also can oscillate periodically