chaos – real random numbers via electronics

Jan Maintok
Supervisor: Hermann Klein, Dipl. Ph.
Hans-Thoma-Gymnasium, 12th grade, Lörrach, Germany, jan.maintok@gmx.de

1 Why does one need random numbers?

Cryptography recently gained a high significance due to the revelations about the NSA and thus random numbers, who are important in cryptography, are getting more important. Computers can only generate so called pseudo random numbers, which results in a big security gap. Therefore this project aims to generate real random numbers in an easy way by using deterministic chaotic circuits.

2 The Lorenz-Attractor

One of the best known chaotic Systems is the Lorenz-Attractor, who is described by the following coupled differential equations:

$$\dot{X} = a(Y - X) \quad (1)$$

$$\dot{Y} = X(b - Z) - Y \quad (2)$$

$$\dot{Z} = XY - cZ \quad (3)$$

If you plot the trajectories of the solutions for X,Y and Z in a three-dimensional phase space you get the butterfly-like pattern below.

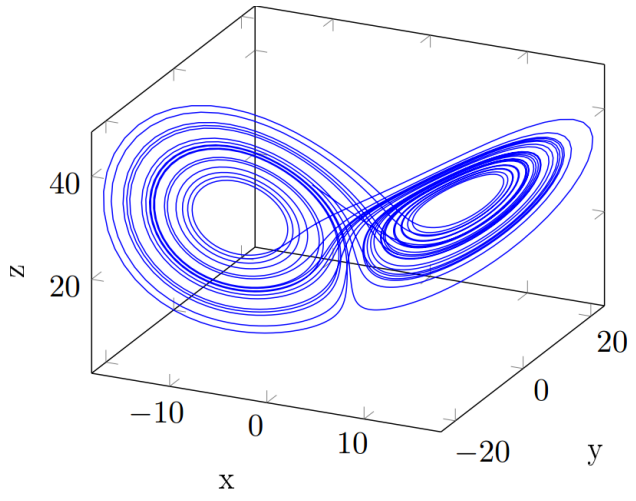
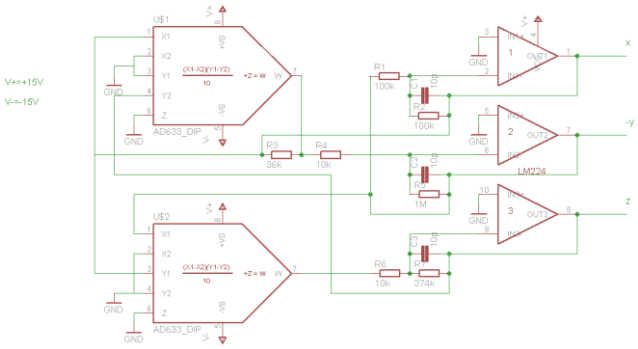


Fig.1 trajectories of the Lorenz-Attraktor

2.1 Solving the differential equations using electronics

Certain electronic components can convert these equations into an electronic signal, which can then be processed further to get the random numbers.

You can see the electronic circuit down below.



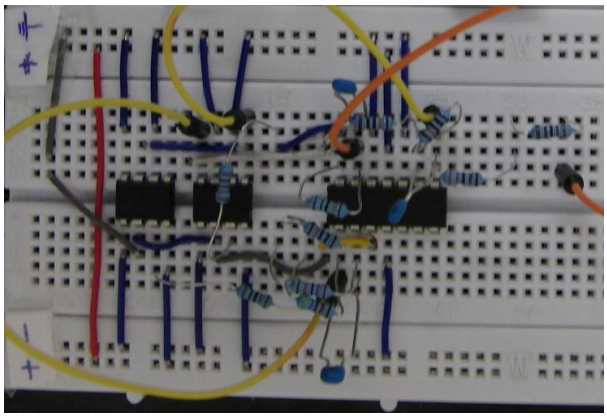


Fig.2 circuit diagram and the electronic circuit

3 Getting the random numbers

If the X-Signal is positive we write down a 1, if it is negative we write a 0, both events having the same probability. This process of getting the random numbers can also be see below.

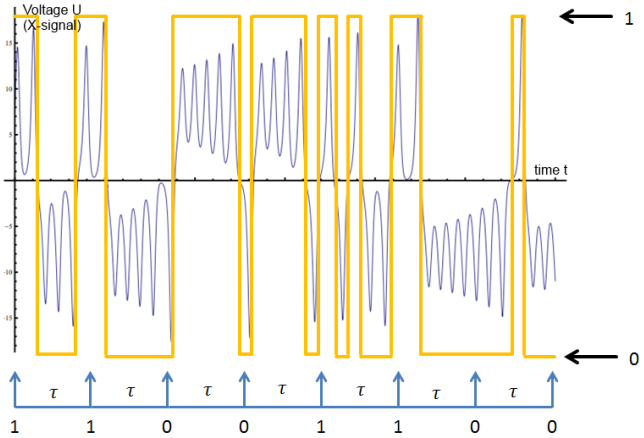


Fig.3 getting the random numbers

If the interval τ is big enough, there is no more correlation between two following Bits and it has been shown that these random numbers are real random numbers.