# The art of cryptography: Heads and tails – Cryptographic random generation summer 2015

## True random generators

Prof. Dr. Joachim von zur Gathen

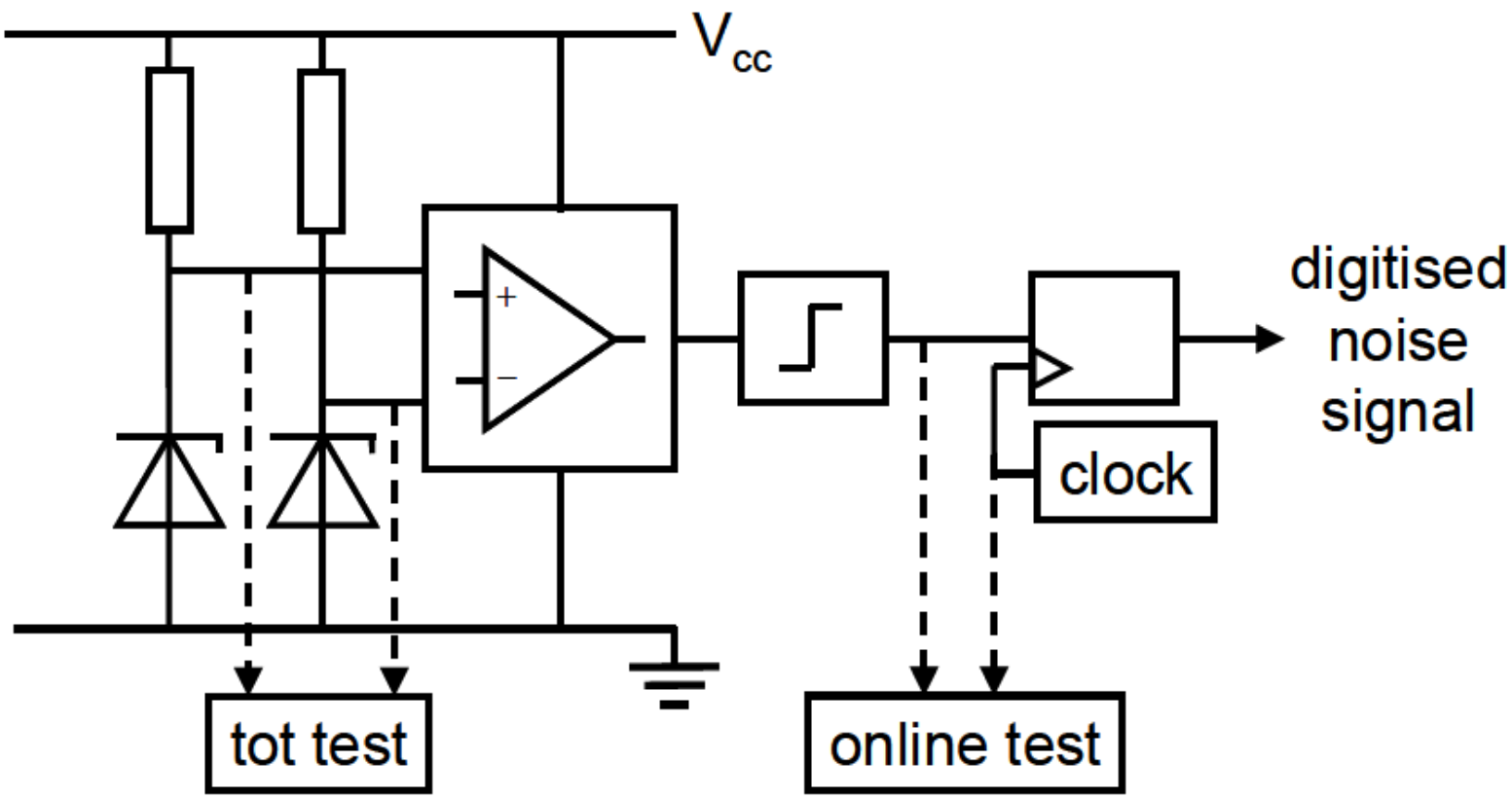
A *software-based generator* measures some process such as

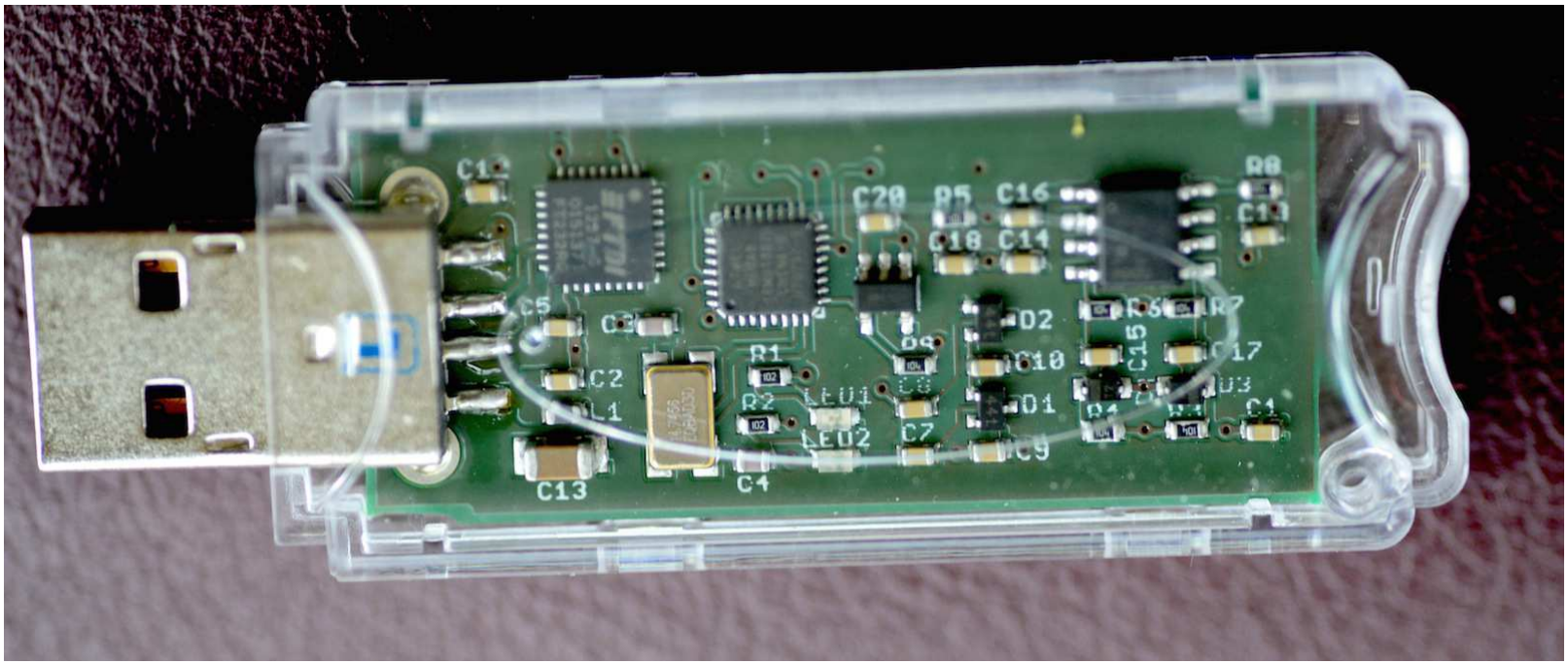
- the system clock,
- key stroke or mouse movements,
- system or network parameters,
- the contents of certain registers,
- user input.

The second type of method are *hardware-based generators* which measure some physical process, such as

- radioactive decay–but plutonium-endowed laptops face a problem with user acceptance,
- sector access times in a sealed hard disk,
- semi conductor thermal noise,
- ring oscillators sampled at independent rates.
- capacitor charge or noisy diodes.


THRESHOLD
MODE
CHERNOBYL-TOUR.COM
μSv/h
OPERATIONAL MODES
GAMMA DOSE RATE
ALARM CLOCK
GAMMA DOSE
TIME
TERRA-P ECOTEST.UA
www.chernobyl-tour.com

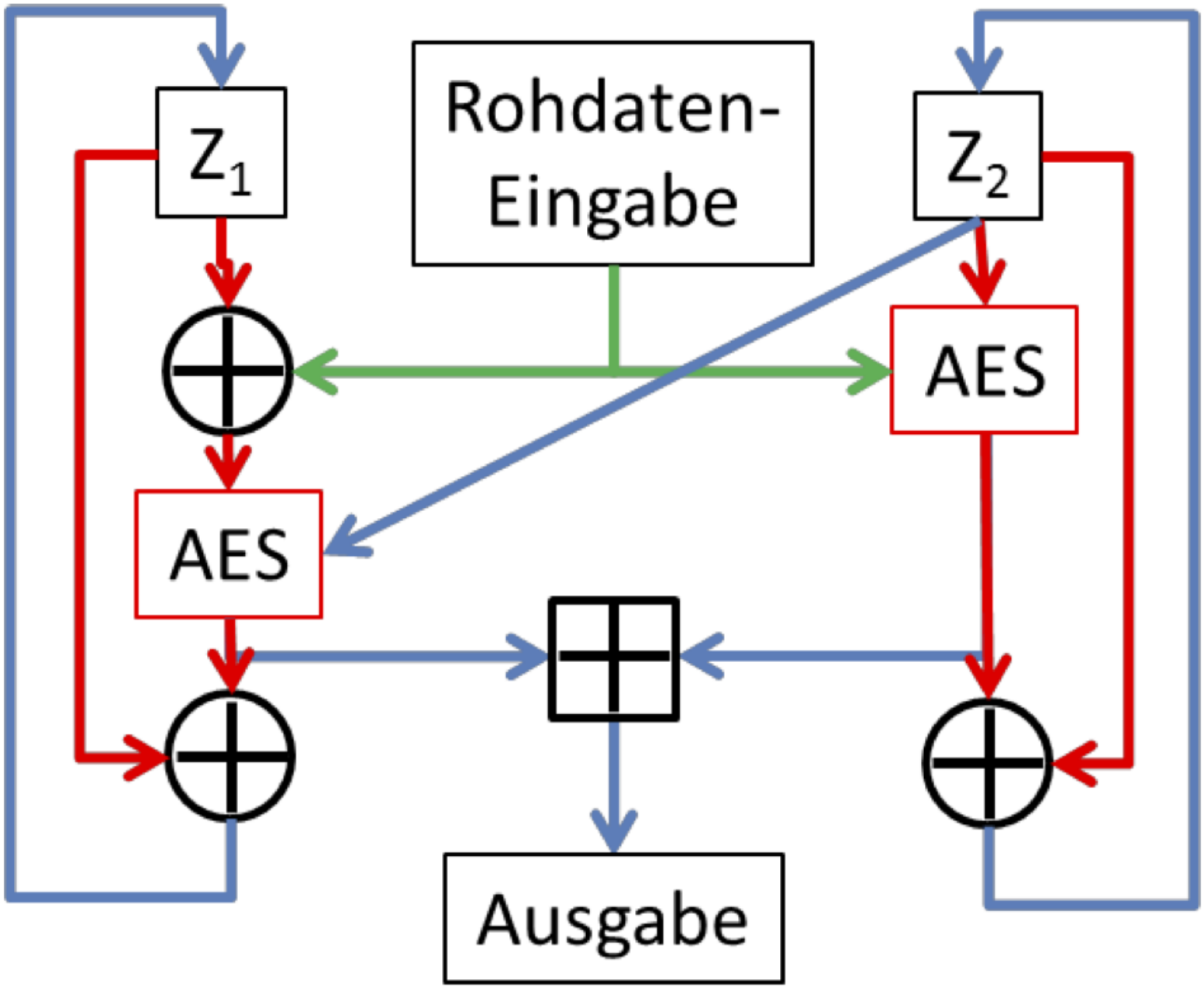

$V_{cc}$
+
−
digitised
noise
signal
clock
tot test
online test


C1
C20
R5
C16
R8
C18
C14
C5
C3
D2
R1
C15
C17
C2
R2
LED1
D1
C1
L1
LED2
C7
C9
C13
C4

*The random source of the generator consists of two equal noisy diodes. For example, Zener diodes have a reverse avalanche effect (depending on diode type at 3–4 Volts or about 10 V) and produce more than 1mV noisy voltage at about 10 MHz. The Flicker Noise in Schottky diodes is associated with static current flow in both resistive and depletion regions (caused by traps due to crystal defects and contaminants, which randomly capture and release carriers). Both diodes provide symmetric input to an operational amplifier to amplify the difference of noise voltages. The output of the operational amplifier is provided to a Schmitt trigger, where the mean voltage of the amplifier meets the threshold of the Schmitt trigger. The output signal of the Schmitt trigger consists of zero and one signals of random length. This signal is latched to the digitized random signal with a clock, which should be at least 20 times slower than the output signal of the Schmitt trigger.*

## Postprocessing

- von Neumann
- XOR
- AES

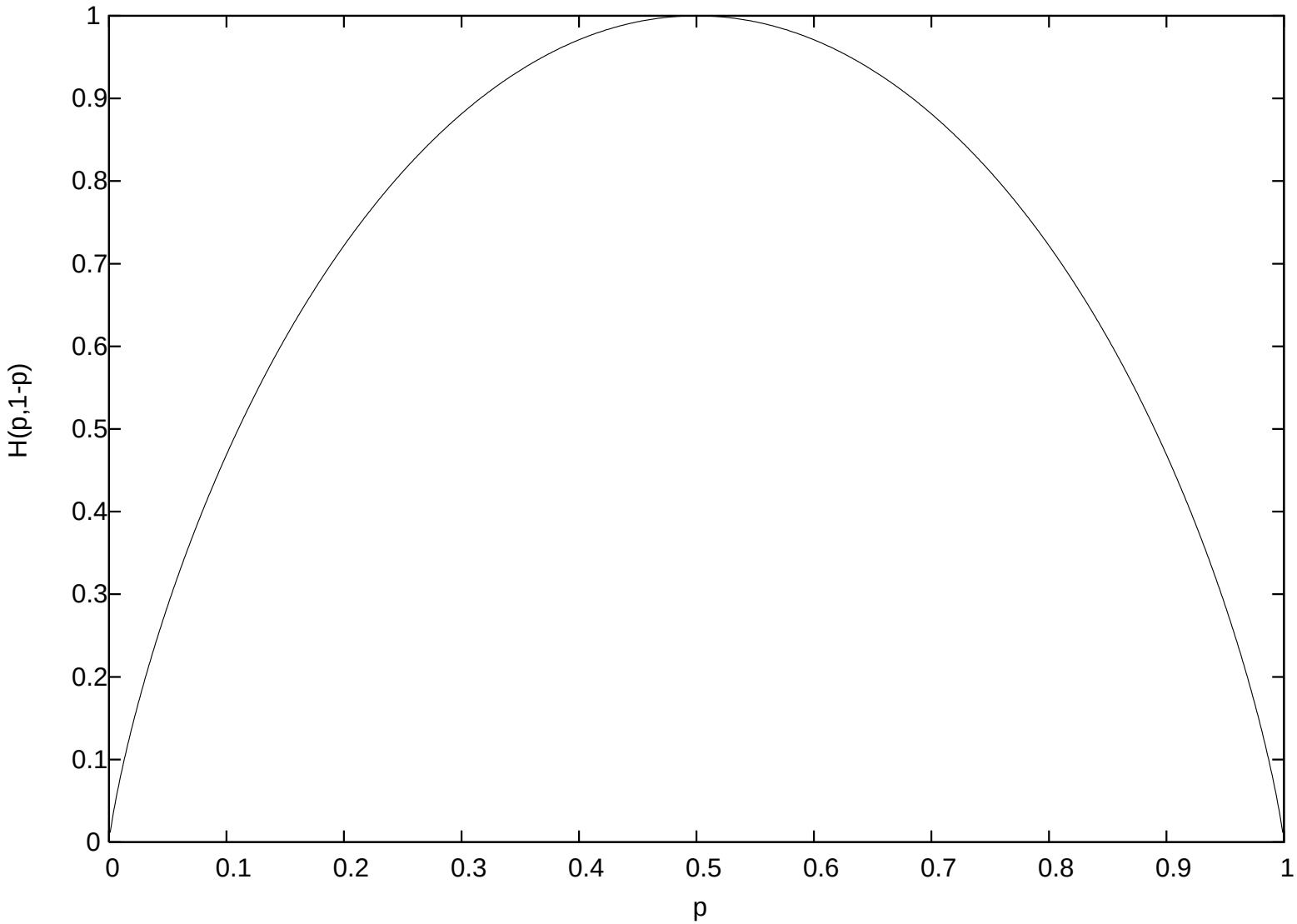

Z1
Rohdaten-
Eingabe
Z2
AES
AES
Ausgabe

Let $p = (p_1, p_2, \ldots, p_s)$ be a probability distribution. Then its *entropy* $H(p)$ is

$$H(p) = \sum_{1 \le i \le s} p_i \log_2(p_i^{-1}).$$

The entropy has the following property:

$$0 \le H(p) \le H\big(\frac{1}{s}, \frac{1}{s}, \ldots, \frac{1}{s}\big) = \log_2 s.$$


H(p,1-p)
p
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1