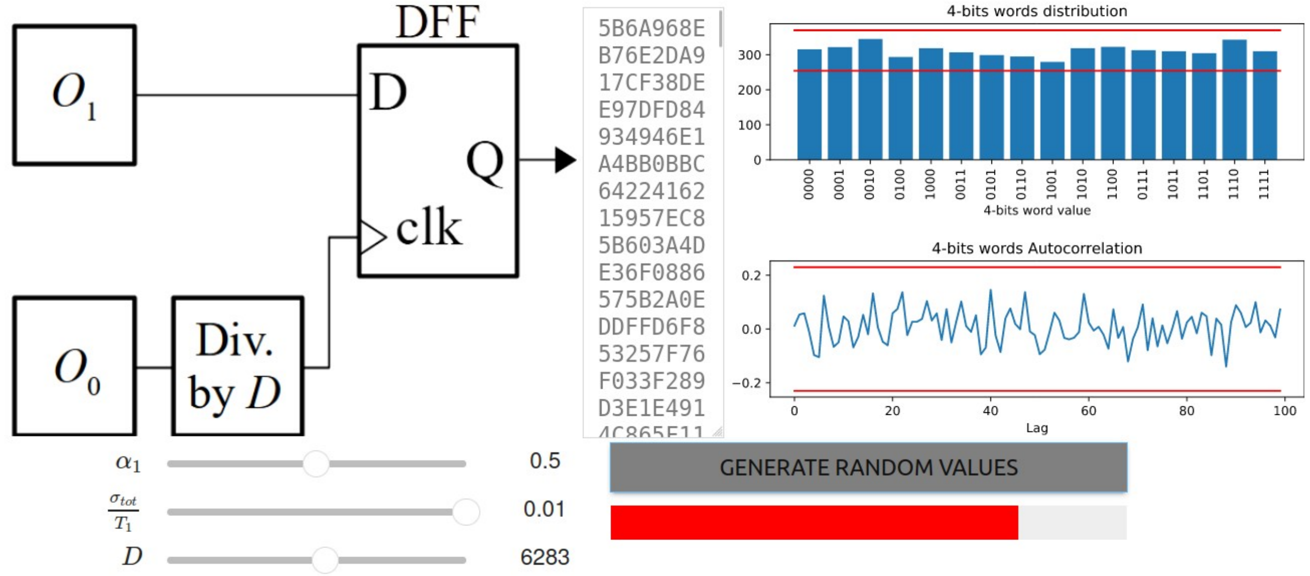
*Cyrille STROESSER*

# Task 5

## Exercise 1



```
5B6A968E
B76E2DA9
17CF38DE
E97DFD84
934946E1
A4BB0BBC
64224162
15957EC8
5B603A4D
E36F0886
575B2A0E
DDFFD6F8
53257F76
F033F289
D3E1E491
4C865E11
```

$\alpha_1$ 0.5

$\frac{\sigma_{tot}}{T_1}$ 0.01

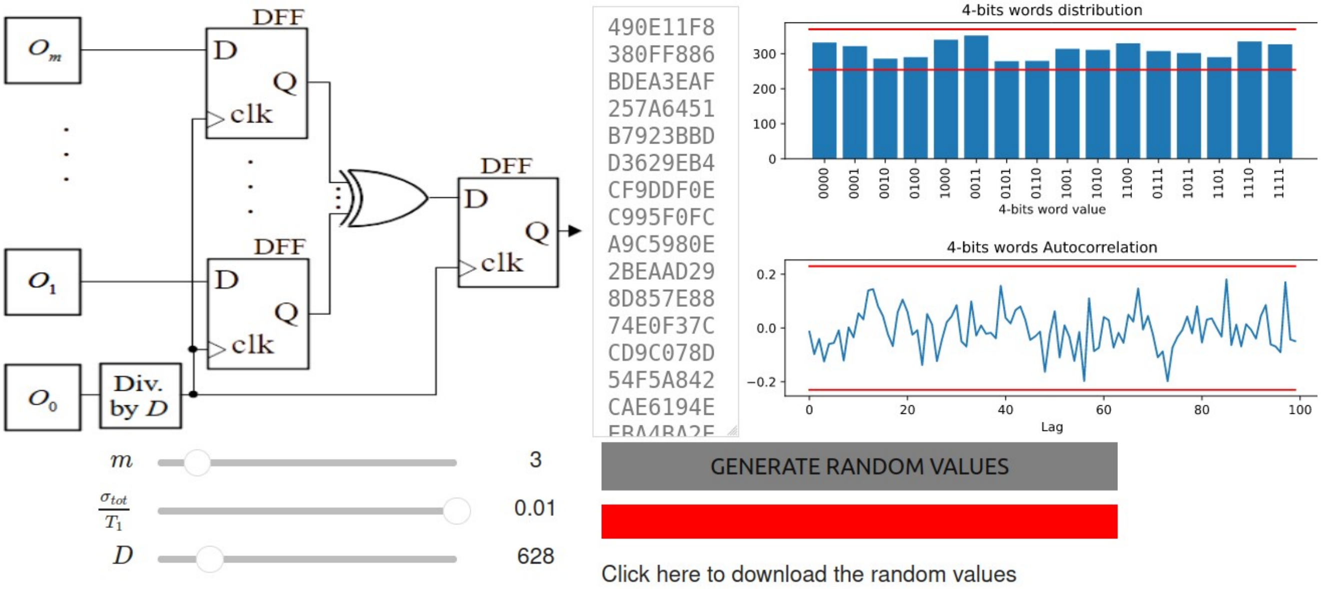
$D$ 6283

To have the best randomness, we’re playing with the variables alpha, Jitter and D. We found out that:
- we need a high Jitta to have less auto-correlation
- alpha must equal 0.5 to get the most flat distribution

With **6283** duty cycles we manage to find a pretty good distribution and low auto-correlation.

*Cyrille STROESSER*

# Exercise 2



```
490E11F8
380FF886
BDEA3EAF
257A6451
B7923BBD
D3629EB4
CF9DDF0E
C995F0FC
A9C5980E
2BEAAD29
8D857E88
74E0F37C
CD9C078D
54F5A842
CAE6194E
FBA4BA2E
```

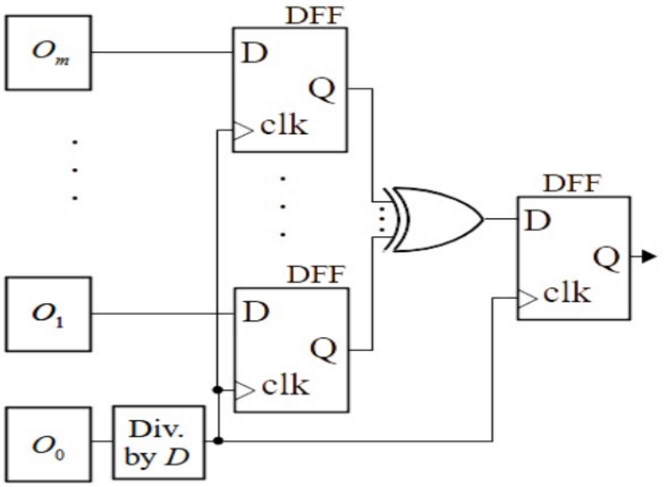
$m$ 3

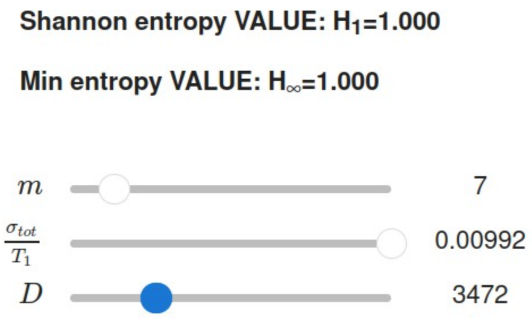
$\frac{\sigma_{tot}}{T_1}$ 0.01

$D$ 628

As it is expensive to increase the number oscillators and duty cycles, we will try to find the best random generator with the lowest values of m and D. With 3 oscillators, 628 duty cycles and still the highest jitter, we manage to have an ideal random generator.

## Exercise 3





**Shannon entropy VALUE: $H_1$=1.000**

**Min entropy VALUE: $H_\infty$=1.000**

$m$ 7

$\frac{\sigma_{tot}}{T_1}$ 0.00992

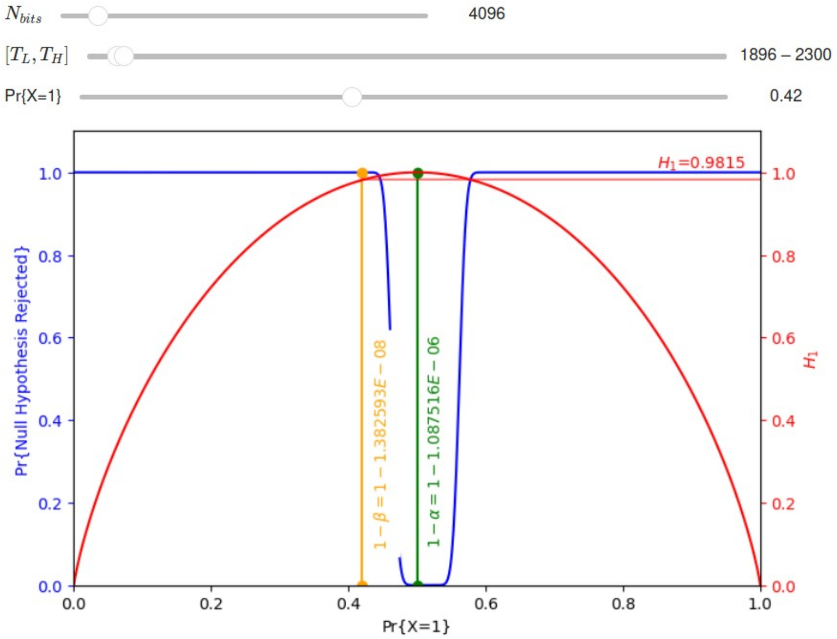
$D$ 3472

To have the best entropy with the lowest cost, we need 3472 duty cycles and 7 oscillators.

## Exercise 4

**For n= 4096:**

The lowest threshold giving and α bigger than $10^{-6}$ is 1896 with α =1.087e-06. The hightest Shannon entropy for β smaller than 10e-6 is $H_1$=0.9815 with  β=1.383e-08.



$N_{bits}$ 4096

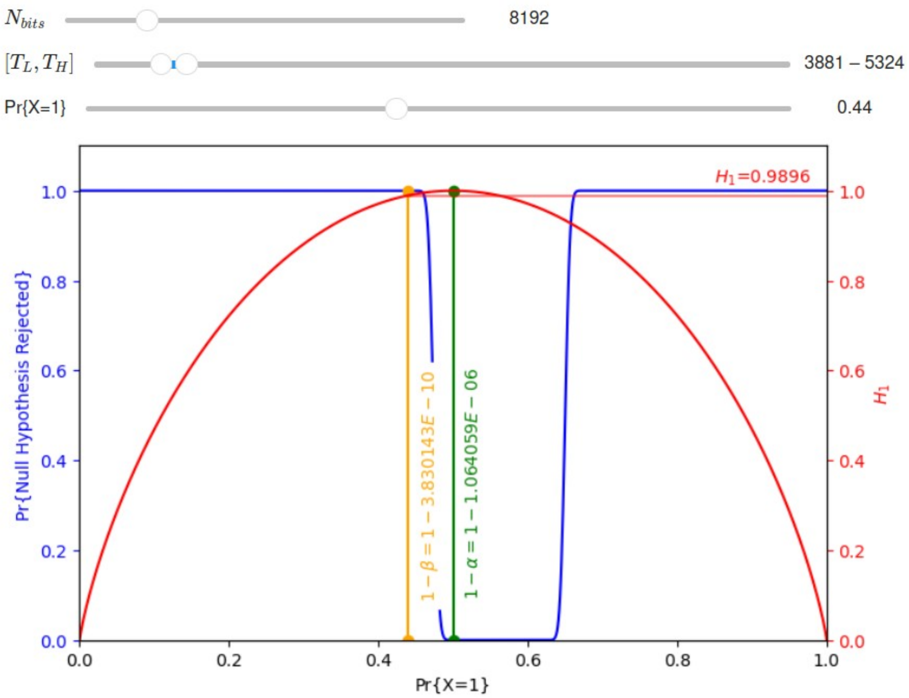
$[T_L, T_H]$ 1896 – 2300

Pr{X=1} 0.42

*Cyrille STROESSER*

**For n= 8192:**

The lowest threshold giving and α bigger than $10^{-6}$ is 3881 with α =1.064e-06. The hightest Shannon entropy for β smaller than 10e-6 is $H_1$=0.9896 with β=3.830e-10.



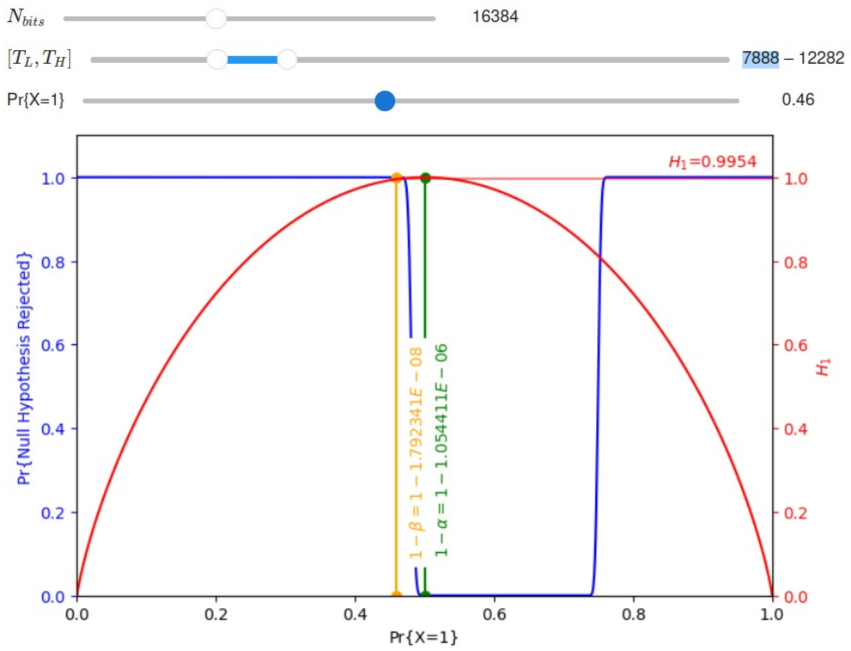
$N_{bits}$ 8192

$[T_L, T_H]$ 3881 – 5324

Pr{X=1} 0.44

**For n=16384:**

The lowest threshold giving and α bigger than $10^{-6}$ is 7888 with α =1.054e-06. The hightest Shannon entropy for β smaller than 10e-6 is $H_1$=0.9974 with β=4.581e-10.



$N_{bits}$ 16384

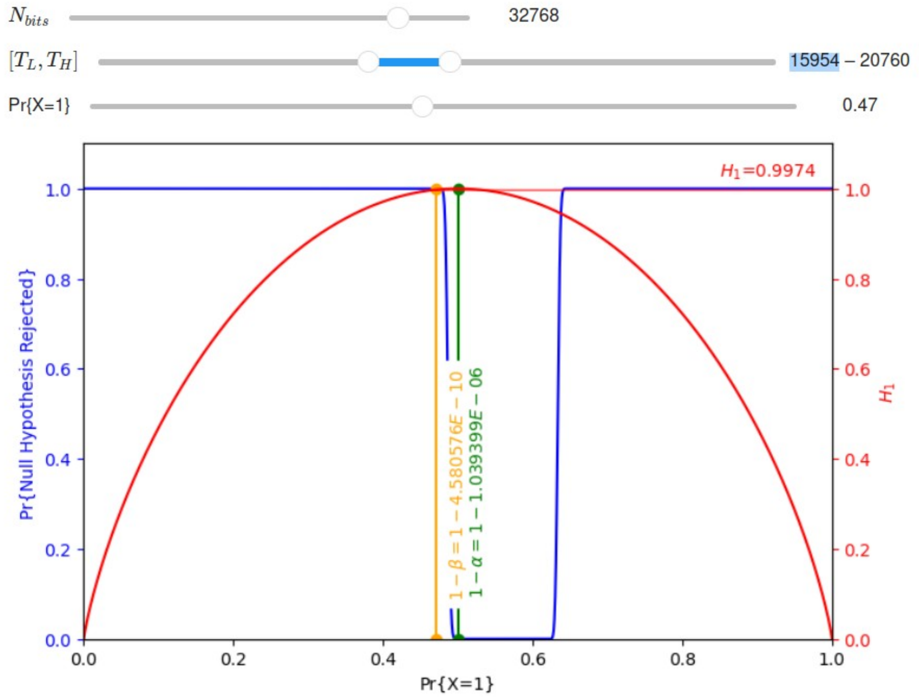
$[T_L, T_H]$ 7888 – 12282

Pr{X=1} 0.46

*Cyrille STROESSER*

**For n=32768:**

The lowest threshold giving and α bigger than $10^{-6}$ is 15954 with α =1.039e-06. The hightest Shannon entropy for β smaller than 10e-6 is $H_1$=0.9954 with β=1.792e-08.



$N_{bits}$ 32768

$[T_L, T_H]$ 15954 – 20760

Pr{X=1} 0.47

Monobit tests such as AIS31 or FIPS 140-1 require:

- the bit sequence to test
- a threshold of number of bits equal to zero or one
- significance level: probability to reject a true null hypothesis

*Cyrille STROESSER*

## Exercise 5

| **M** | **$\sigma_{to}t$ /T1** | **D** |
|---|---|---|
| *1* | *0.0* | Impossible |
| | *0.0001* | Impossible |
| | *0.001* | Impossible |
| | *0.01* | Impossible |
| *2* | *0.0* | Impossible |
| | *0.0001* | Impossible |
| | *0.001* | Impossible |
| | *0.01* | 4712 |
| *3* | *0.0* | Impossible |
| | *0.0001* | Impossible |
| | *0.001* | 78539 |
| | *0.01* | 1570 |
| *4* | *0.0* | Impossible |
| | *0.0001* | Impossible |
| | *0.001* | 47123 |
| | *0.01* | 157 |
| *5* | *0.0* | Impossible |
| | *0.0001* | 47123 |
| | *0.001* | 6283 |
| | *0.01* | 157 |
| *6* | *0.0* | 3141 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *7* | *0.0* | 9424 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *8* | *0.0* | 62831 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *9* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *10* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *11* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |

| | | |
|---|---|---|
| | *0.01* | 157 |
| *12* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *13* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *14* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *15* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |
| *16* | *0.0* | 157 |
| | *0.0001* | 157 |
| | *0.001* | 157 |
| | *0.01* | 157 |