Methodology for the Fault Analysis and Evaluation of True Random Number Generators

Mathilde Soucarros, Jessy Clédière, Cécile Dumas, Philippe Elbaz-Vincent

DGA/CEA/Institut Fourier

21/06/2012

Outline

Outline

Applications

- Utilizations of random numbers :
  - gaming,
  - numerical simulation,
  - security, etc.
- More precisely in cryptography :
  - keys,
  - signatures,
  - nonces,
  - countermeasures, etc.
- Desired properties : independant and identically distributed numbers + unpredictable
- Consequences of deviations : PS3, RSA public keys

Applications

- Utilizations of random numbers :
  - gaming,
  - numerical simulation,
  - security, etc.
- More precisely in cryptography :
  - keys,
  - signatures,
  - nonces,
  - countermeasures, etc.
- Desired properties : independant and identically distributed numbers + unpredictable
- Consequences of deviations : PS3, RSA public keys

Applications

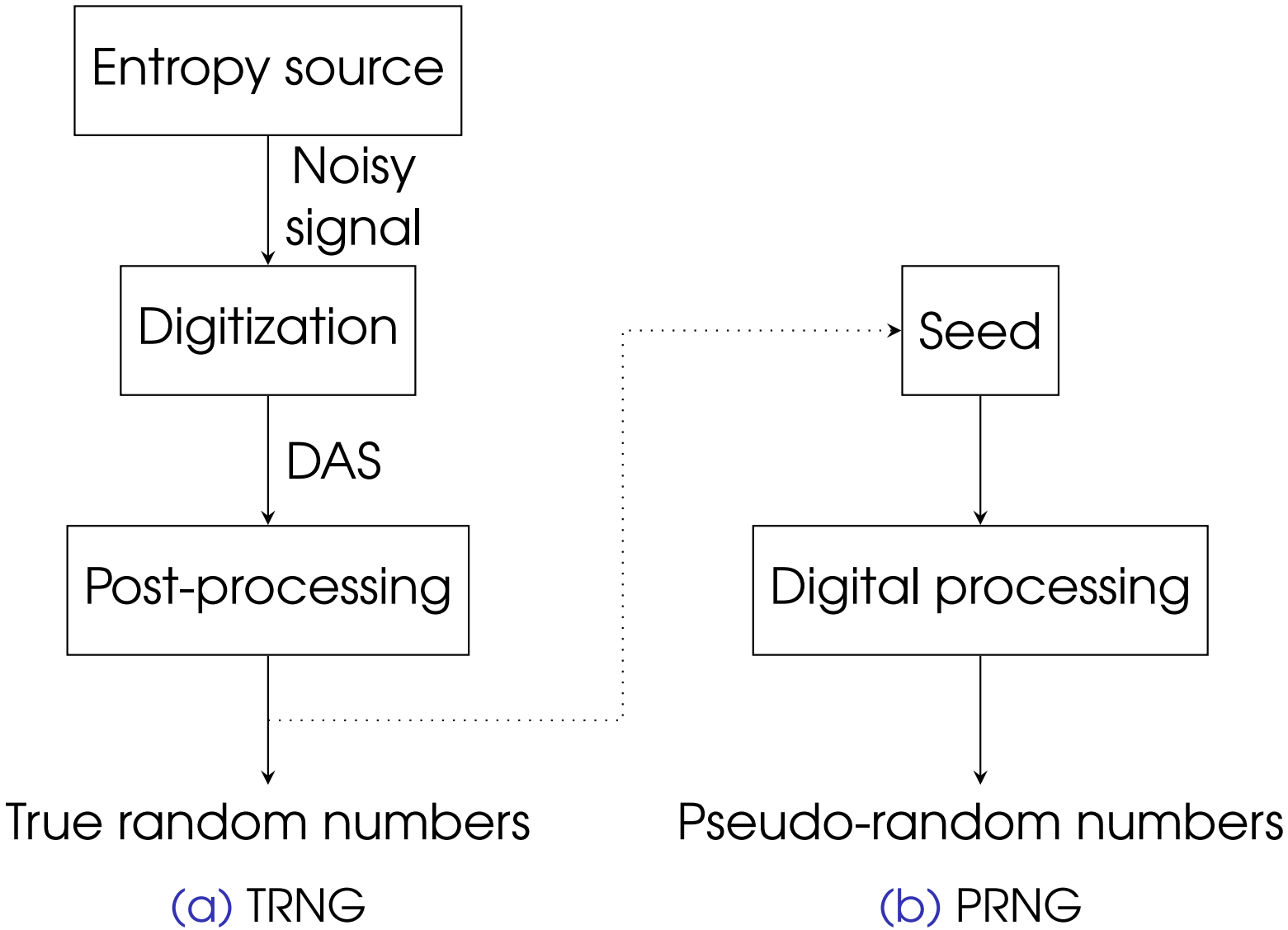
- Utilizations of random numbers :
  - gaming,
  - numerical simulation,
  - security, etc.
- More precisely in cryptography :
  - keys,
  - signatures,
  - nonces,
  - countermeasures, etc.
- Desired properties : independant and identically distributed numbers + unpredictable
- Consequences of deviations : PS3, RSA public keys

Applications

- Utilizations of random numbers :
  - gaming,
  - numerical simulation,
  - security, etc.
- More precisely in cryptography :
  - keys,
  - signatures,
  - nonces,
  - countermeasures, etc.
- Desired properties : independant and identically distributed numbers + unpredictable
- Consequences of deviations : PS3, RSA public keys

Outline

Conception



(a) TRNG

(b) PRNG

Entropy sources

- True Random Number Generators :
  - radioactive decay,
  - thermal noise,
  - phase jitter of oscillators,
  - quantum optics, etc.

- Pseudo-Random Number Generators :
  - linear congruential generators,
  - LFSRs,
  - cryptographic algorithms, etc.

Entropy sources

- True Random Number Generators :
  - radioactive decay,
  - thermal noise,
  - phase jitter of oscillators,
  - quantum optics, etc.

- Pseudo-Random Number Generators :
  - linear congruential generators,
  - LFSRs,
  - cryptographic algorithms, etc.

TRNGs perturbation

- Perturbation of True Random Number Generators :
  - voltage,
  - clock,
  - temperature,
  - surounding activity,
  - frequency injection, etc.

Outline

Principle

- What is randomness ?

  01001101
  00000000
  01010101

- No universal test of randomness
- Evaluation of the properties of bit sequences
- Comparison with a real sequence of random bits

Principle

- What is randomness ?

  01001101
  00000000
  01010101

- No universal test of randomness
- Evaluation of the properties of bit sequences
- Comparison with a real sequence of random bits

Principle

- What is randomness ?

  01001101
  00000000
  01010101

- No universal test of randomness
- Evaluation of the properties of bit sequences
- Comparison with a real sequence of random bits

Principle

- What is randomness ?

  01001101
  00000000
  01010101

- No universal test of randomness
- Evaluation of the properties of bit sequences
- Comparison with a real sequence of random bits

Existing tests

- Most used :
  - One standard : AIS 31
  - Individual tests : FIPS, ENT
  - Batteries : Diehard, NIST, TestU01
- Methodology :
  - Compute statistics and probabilities that a sequence is random (p-values)
  - Decide if the sequence is random (threshold)
  - Observe the total fail rate
  - Decide if the generator is random

Existing tests

- Most used :
  - One standard : AIS 31
  - Individual tests : FIPS, ENT
  - Batteries : Diehard, NIST, TestU01
- Methodology :
  - Compute statistics and probabilities that a sequence is random (p-values)
  - Decide if the sequence is random (threshold)
  - Observe the total fail rate
  - Decide if the generator is random

Limitations

- Concrete information gained thanks to the tests results (detected flaws and their importance)

  Hidden biases

- Evolution in time

  Bias 1 + Bias 2 = Bias 3

- Short disturbances

Limitations

- Concrete information gained thanks to the tests results (detected flaws and their importance)

  Hidden biases

- Evolution in time

  Bias 1 + Bias 2 = Bias 3

- Short disturbances

Limitations

- Concrete information gained thanks to the tests results (detected flaws and their importance)

  Hidden biases

- Evolution in time

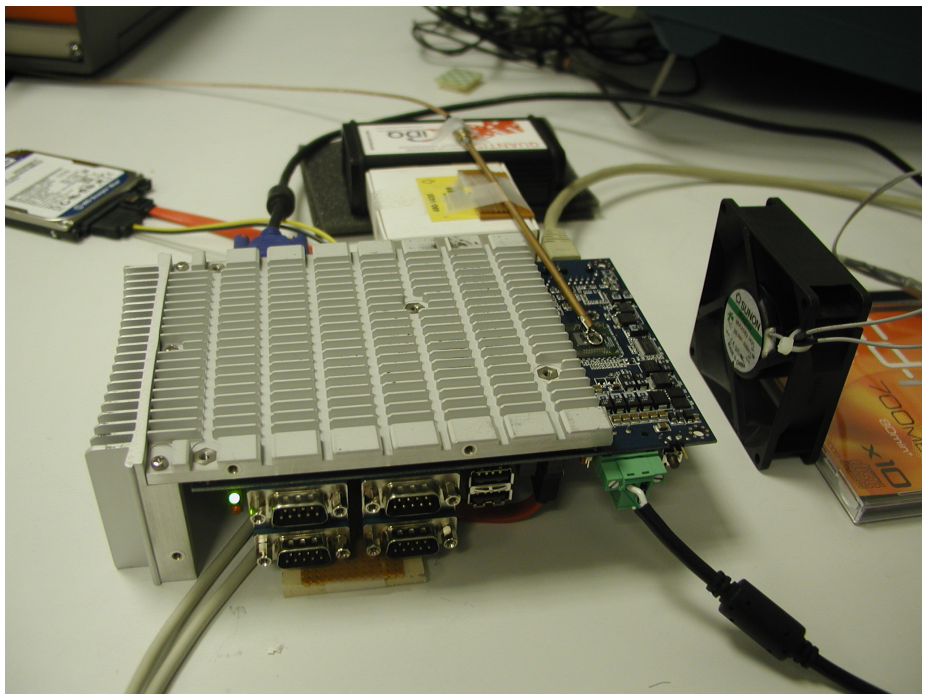
  Bias 1 + Bias 2 = Bias 3

- Short disturbances

Outline

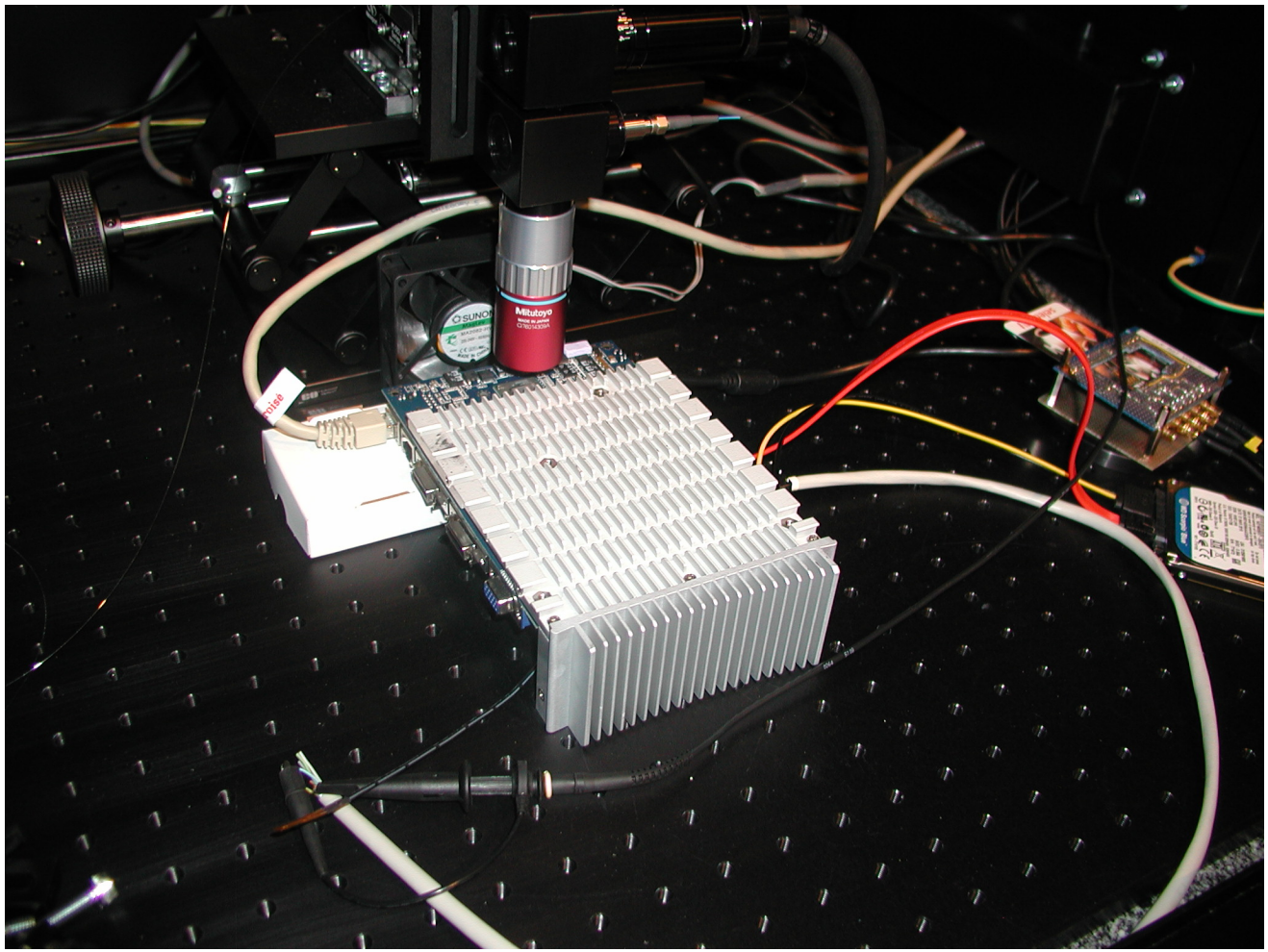
Temperature

(a) Liquid nitrogen



(b) Fan instead of heatsink

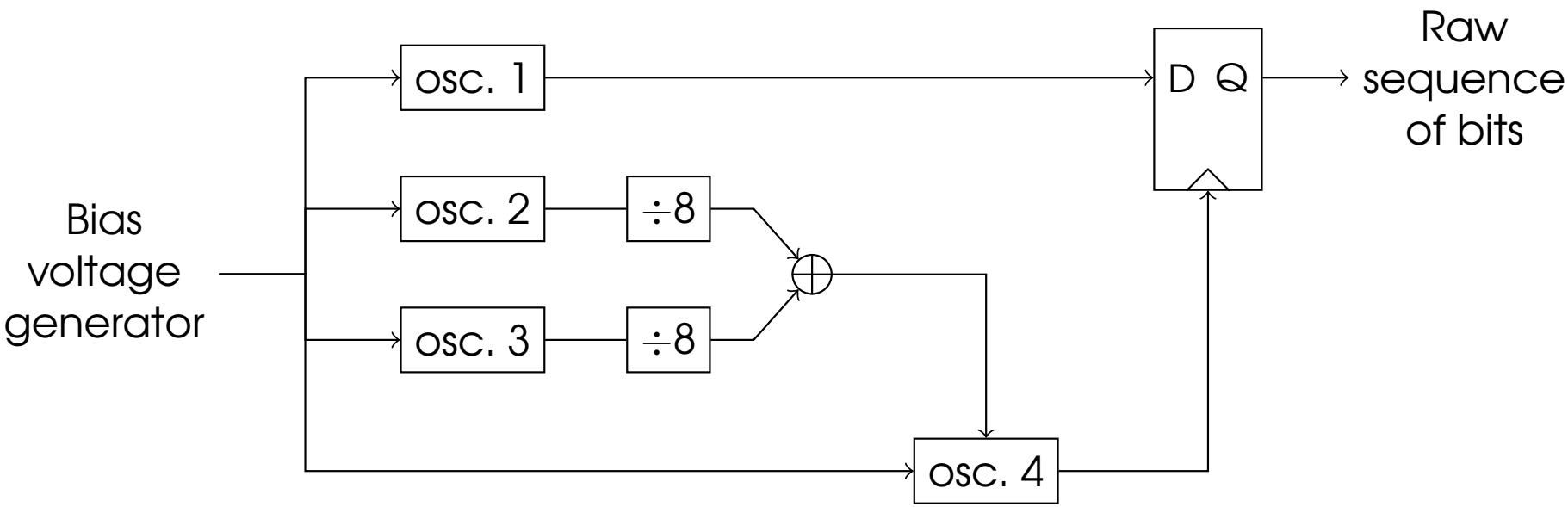
Laser



Outline

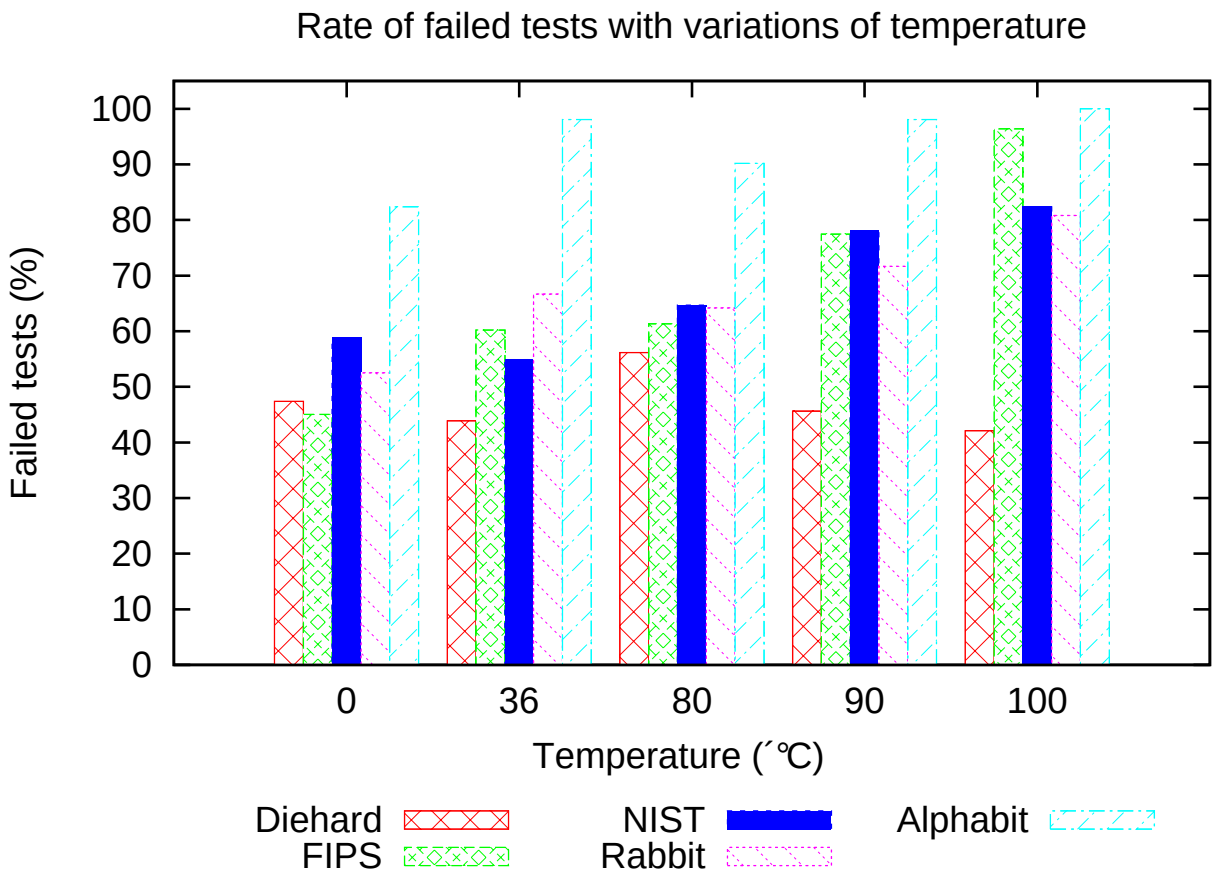
Studied TRNG

- Design of the entropy source based on the sampling of a high frequency oscillator by a slow frequency clock
- Accumulation of jitter



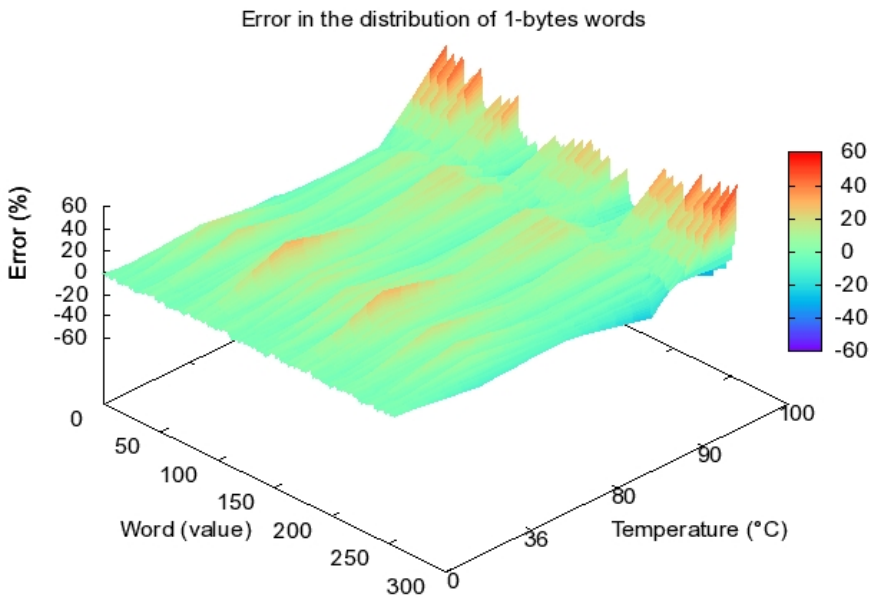
Temperature variations : test results

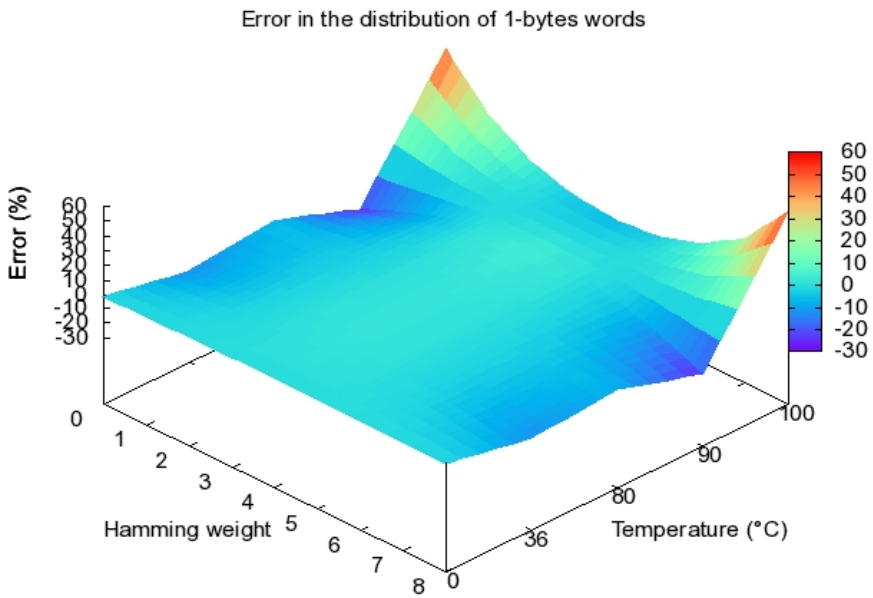
- Temperature from 0 °C up to 100 °C



Temperature variations : byte distribution

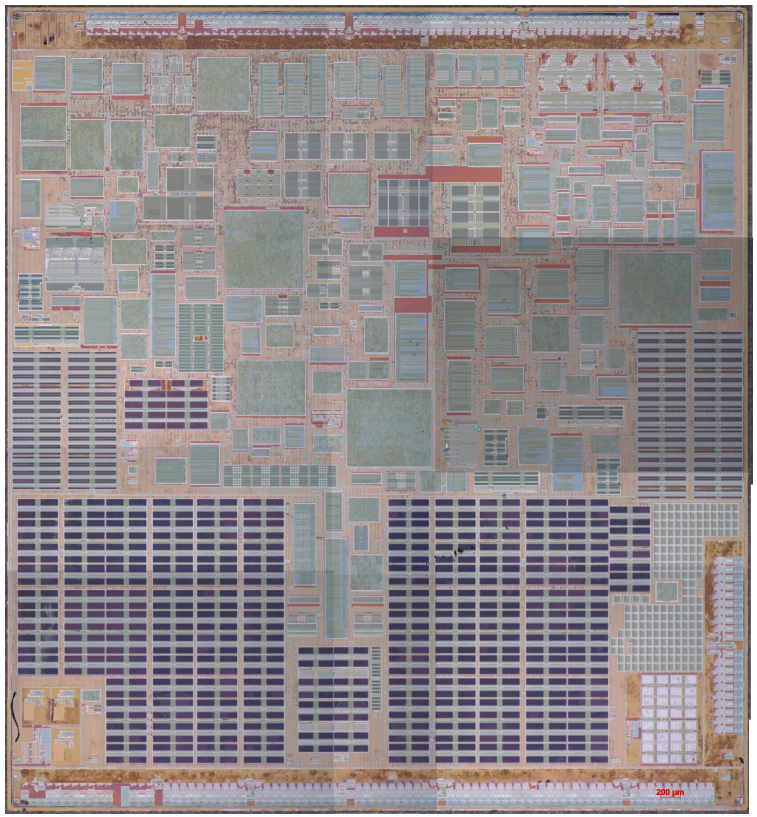
- Deviation in the byte distribution from the uniformity :
  $D_i = \frac{P_i - Pt_i}{Pt_i}$



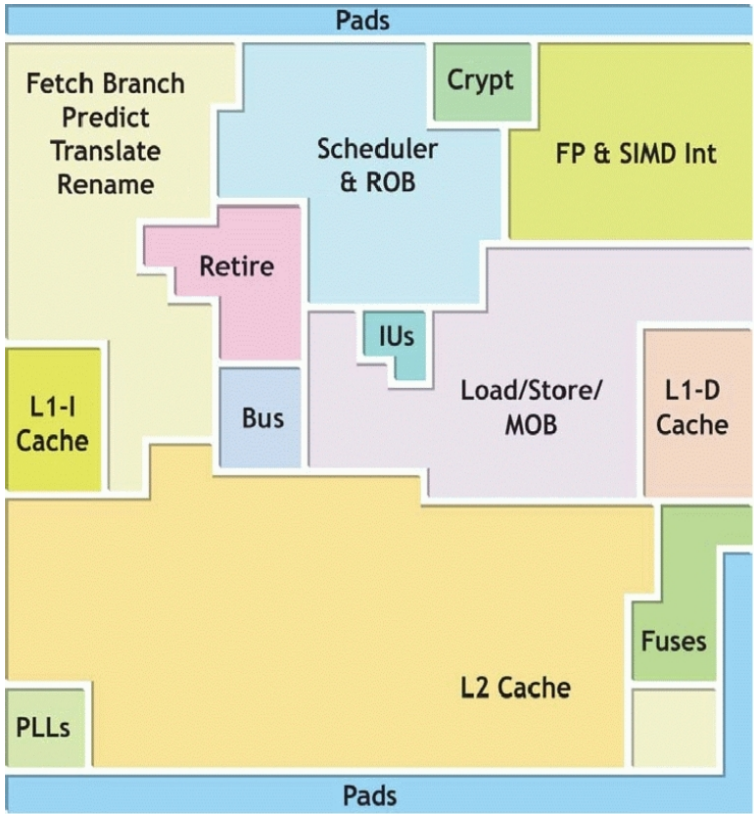


Laser shots : processor

- No information on the TRNG localization



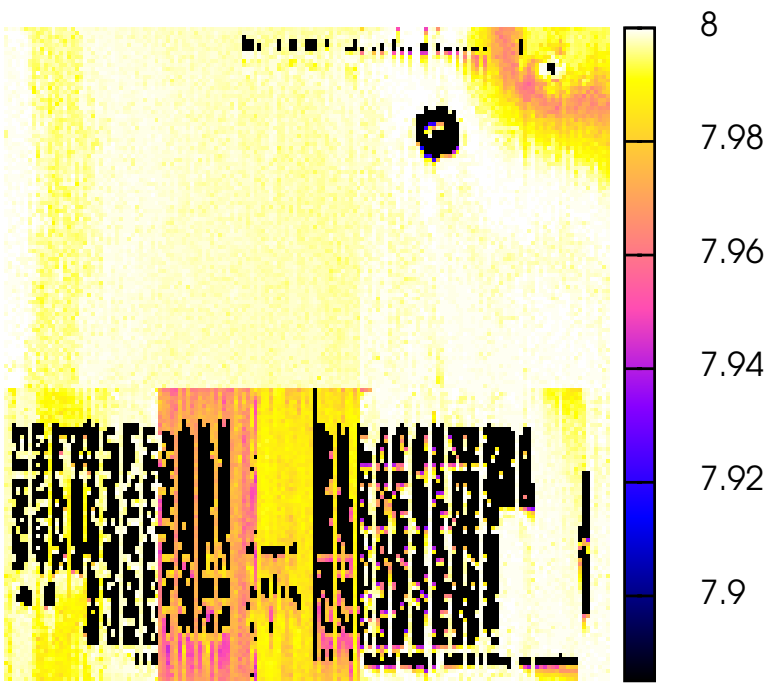
(a) Photography of the processor



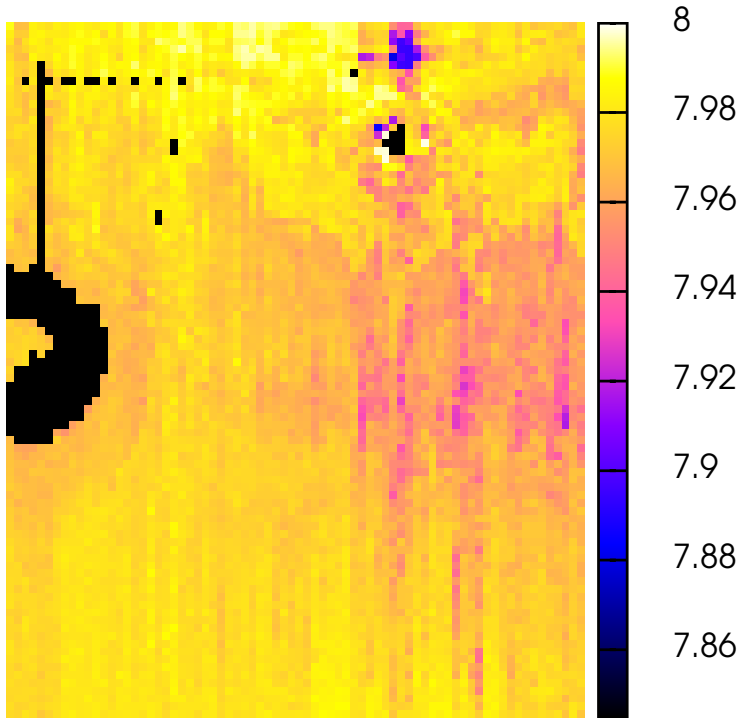
(b) Block diagram of the processor

Laser shots : cartography

- Processor entirely sweeped by steps of 50 µm and a power of 1.05 W then 30 µm and 3.75 W
- Entropy at every point : $H = -\sum_{i=0}^{255} P_i log(P_i)$



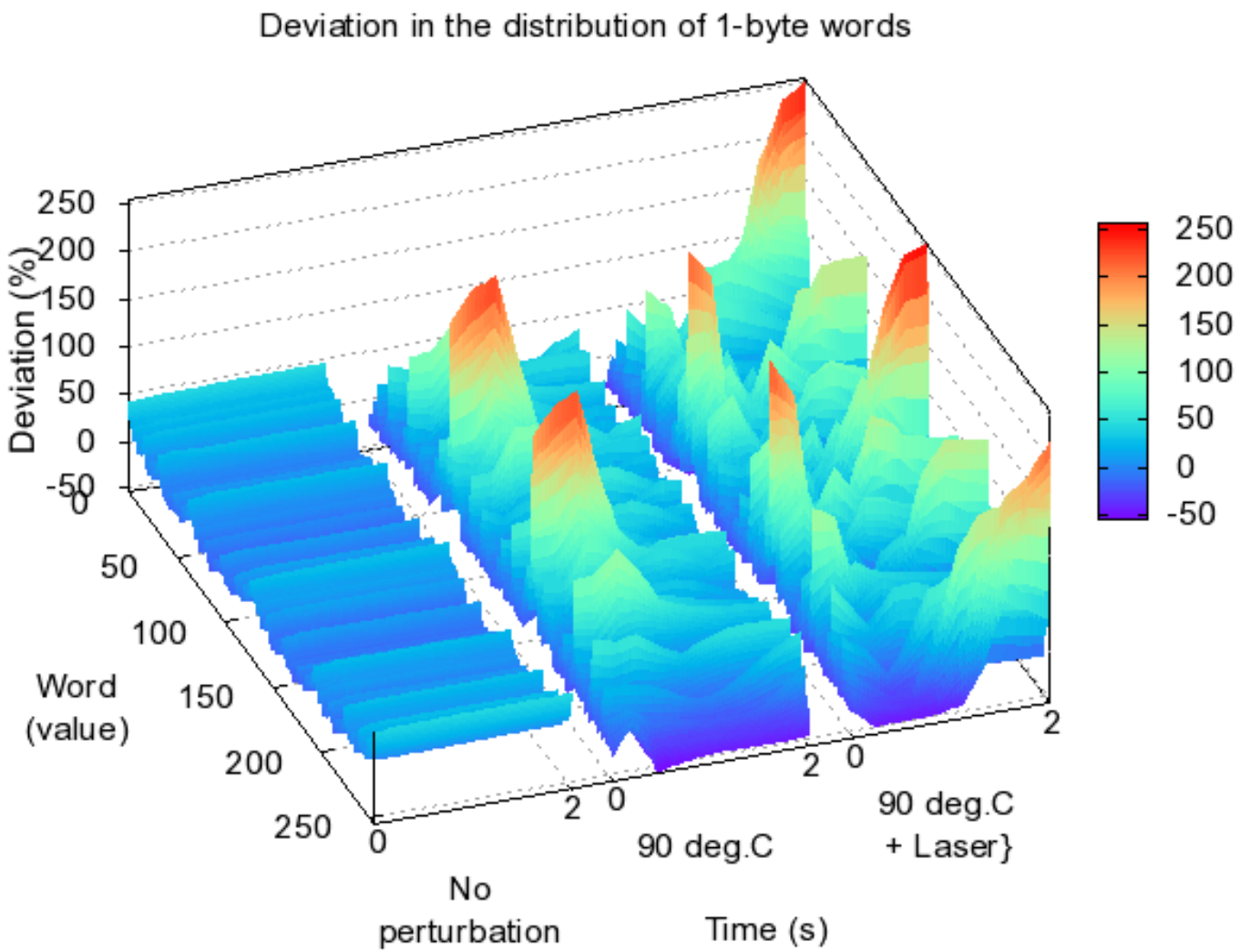
(a) Cartography of the entropy



(b) Zoom of an interesting zone

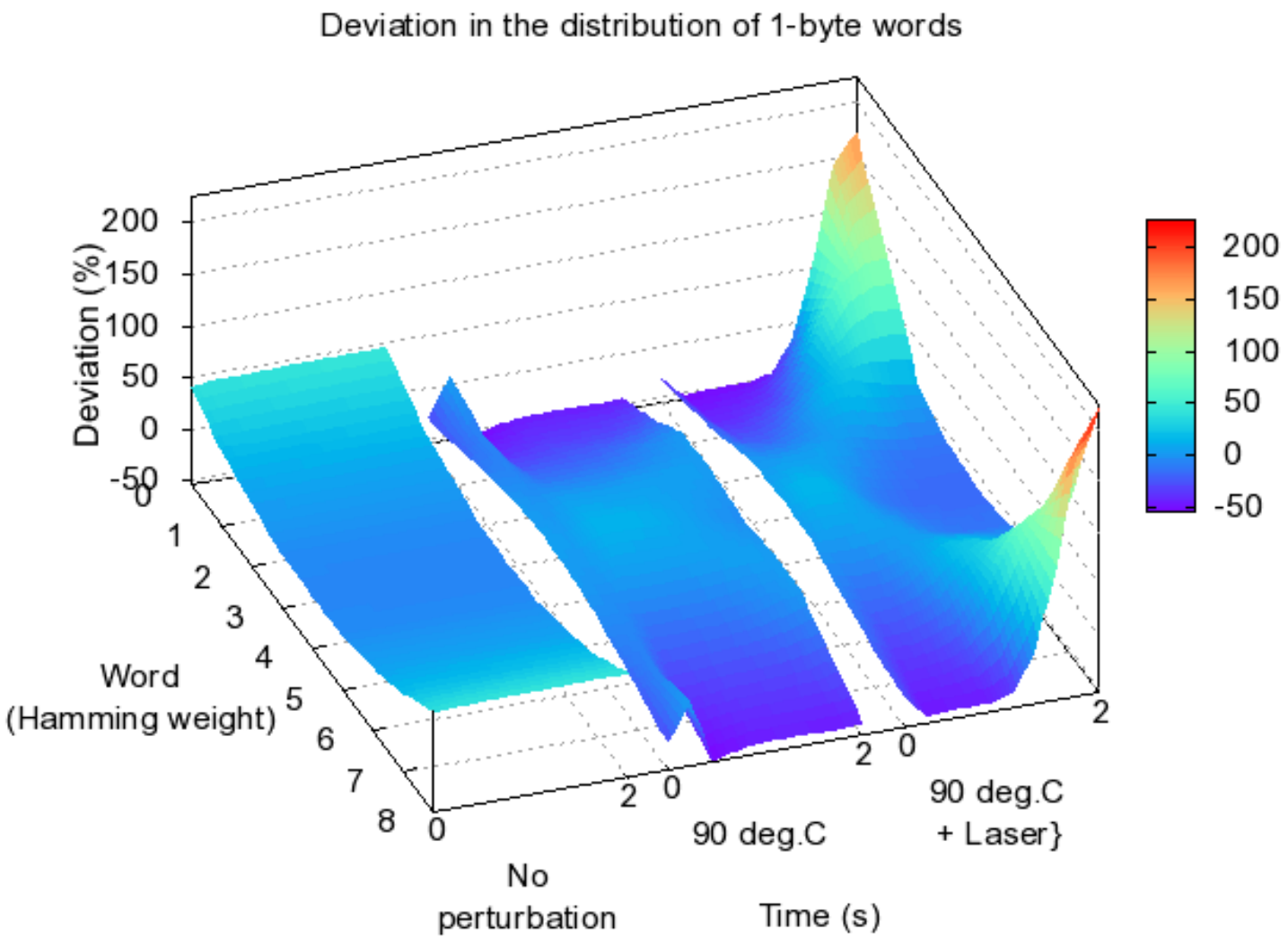
Combination of temperature and laser

- Laser shots focalized on the point of lowest entropy

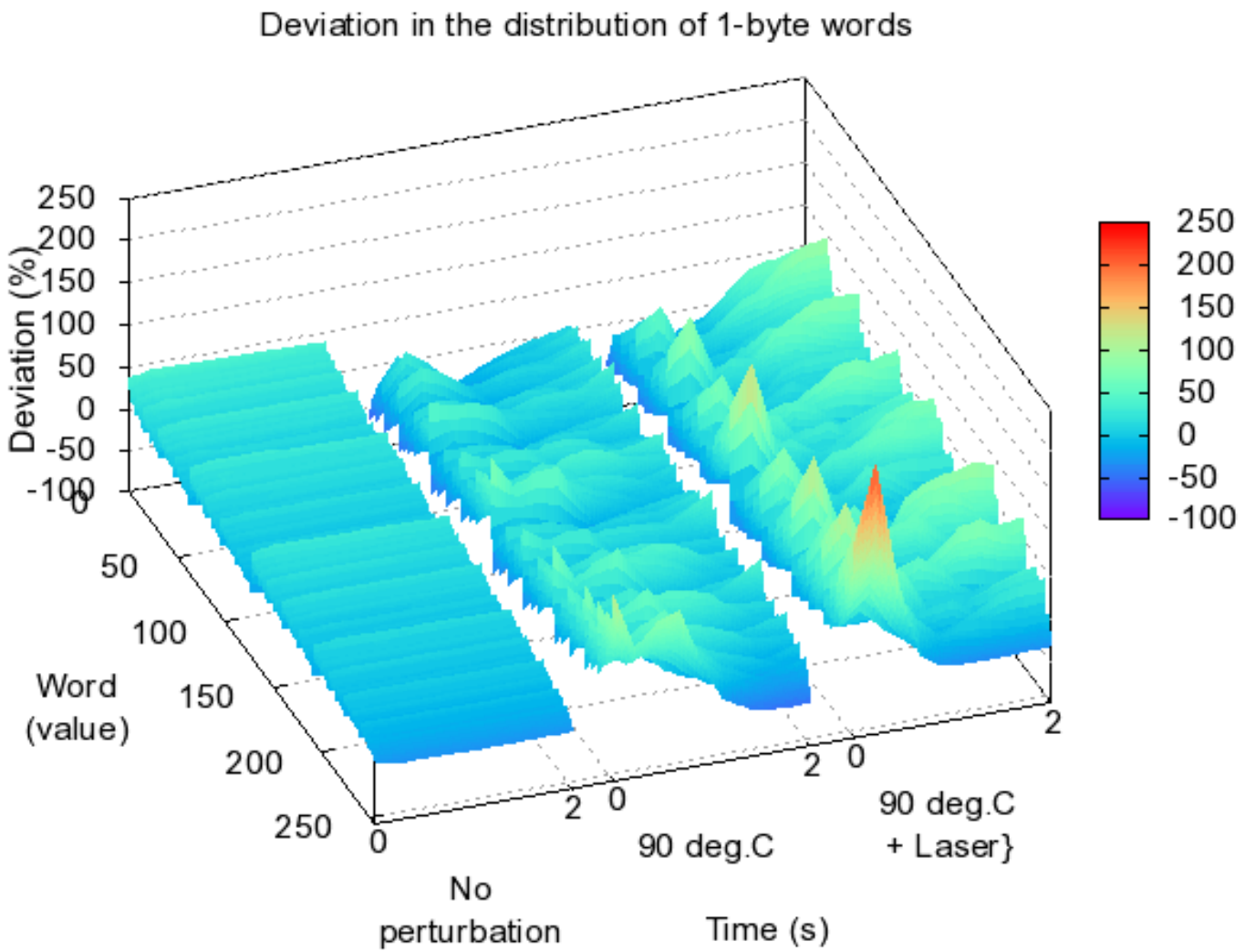


Combination of temperature and laser

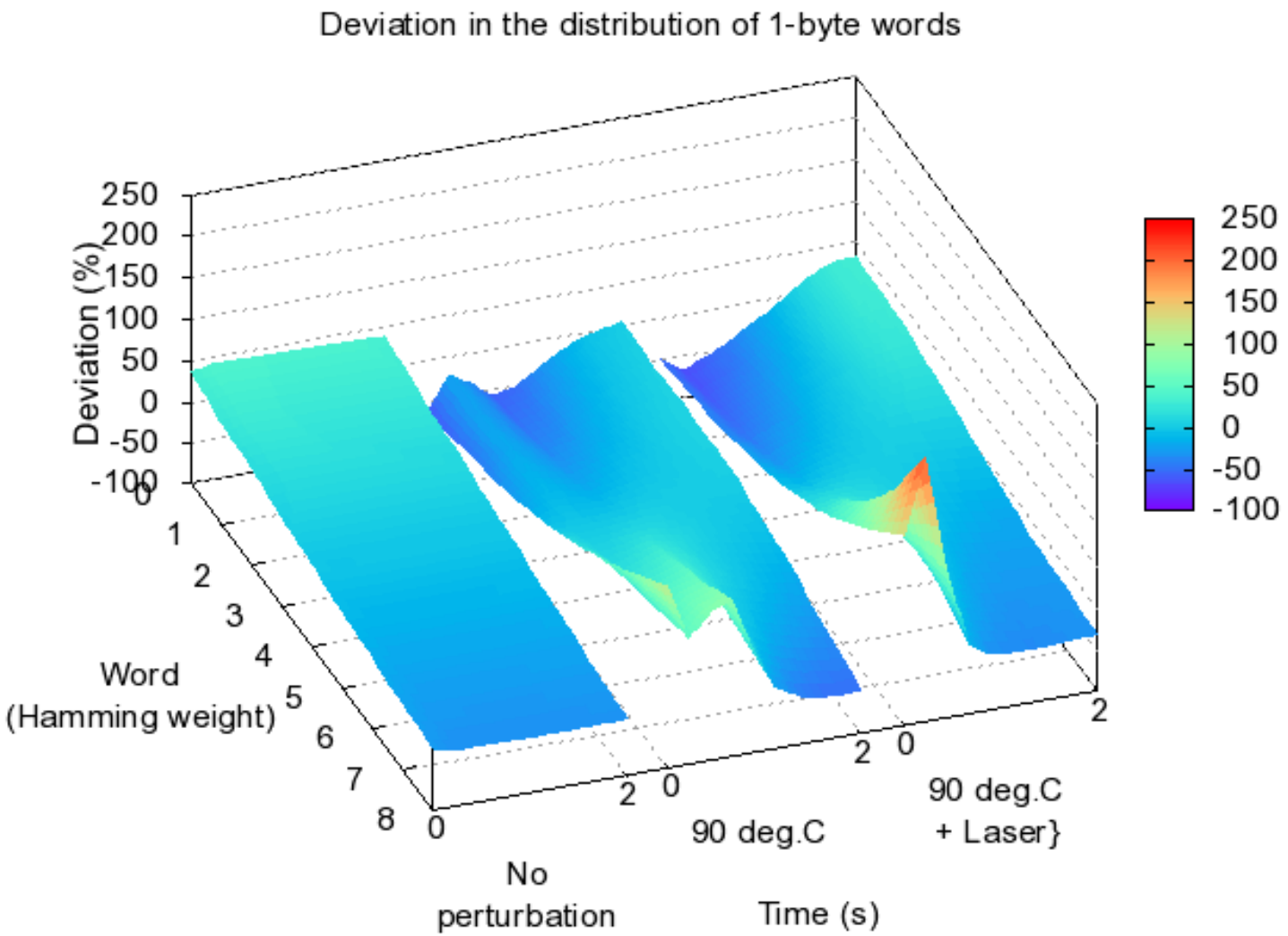
- Laser shots focalized on the point of lowest entropy



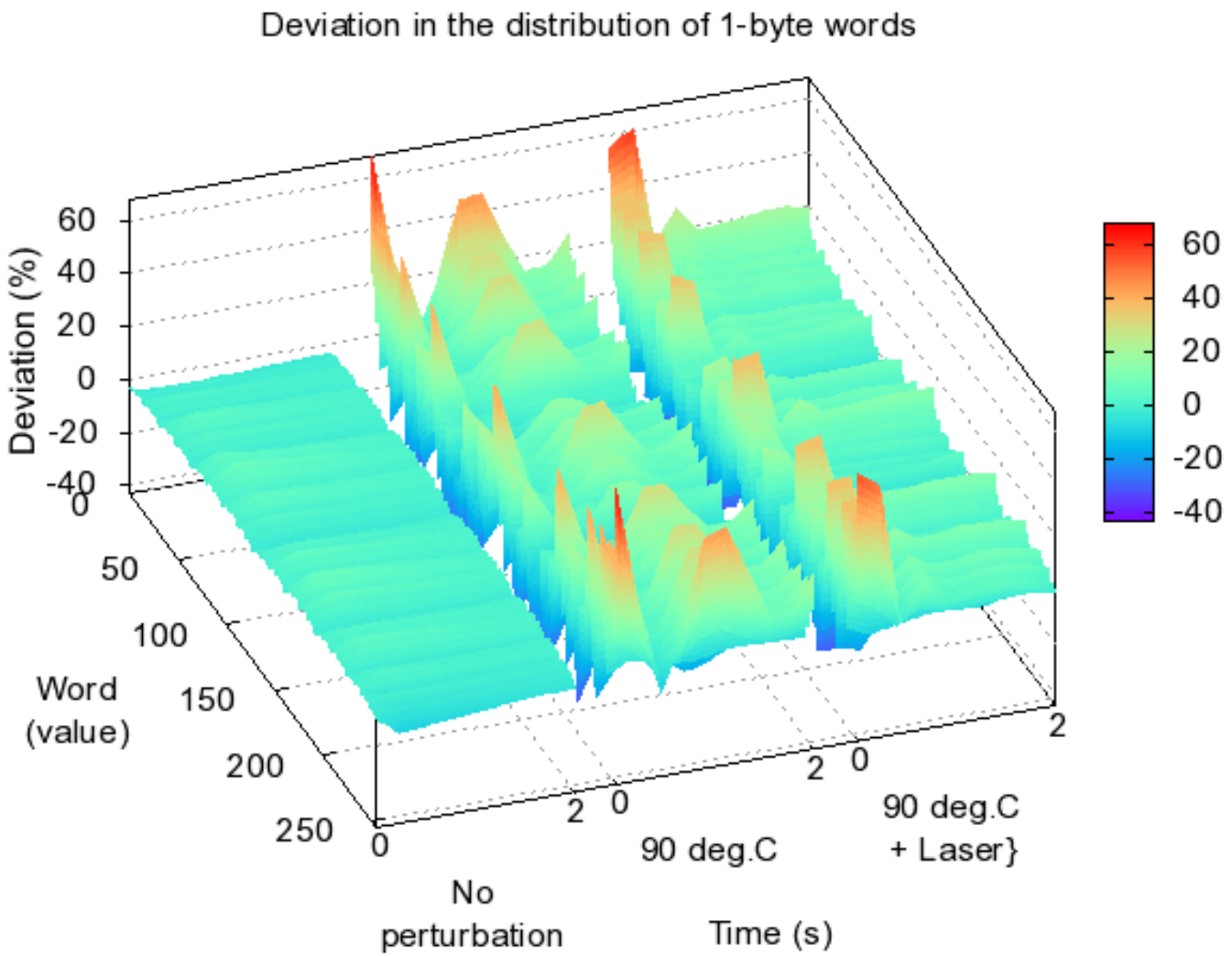
Post-processing : XOR



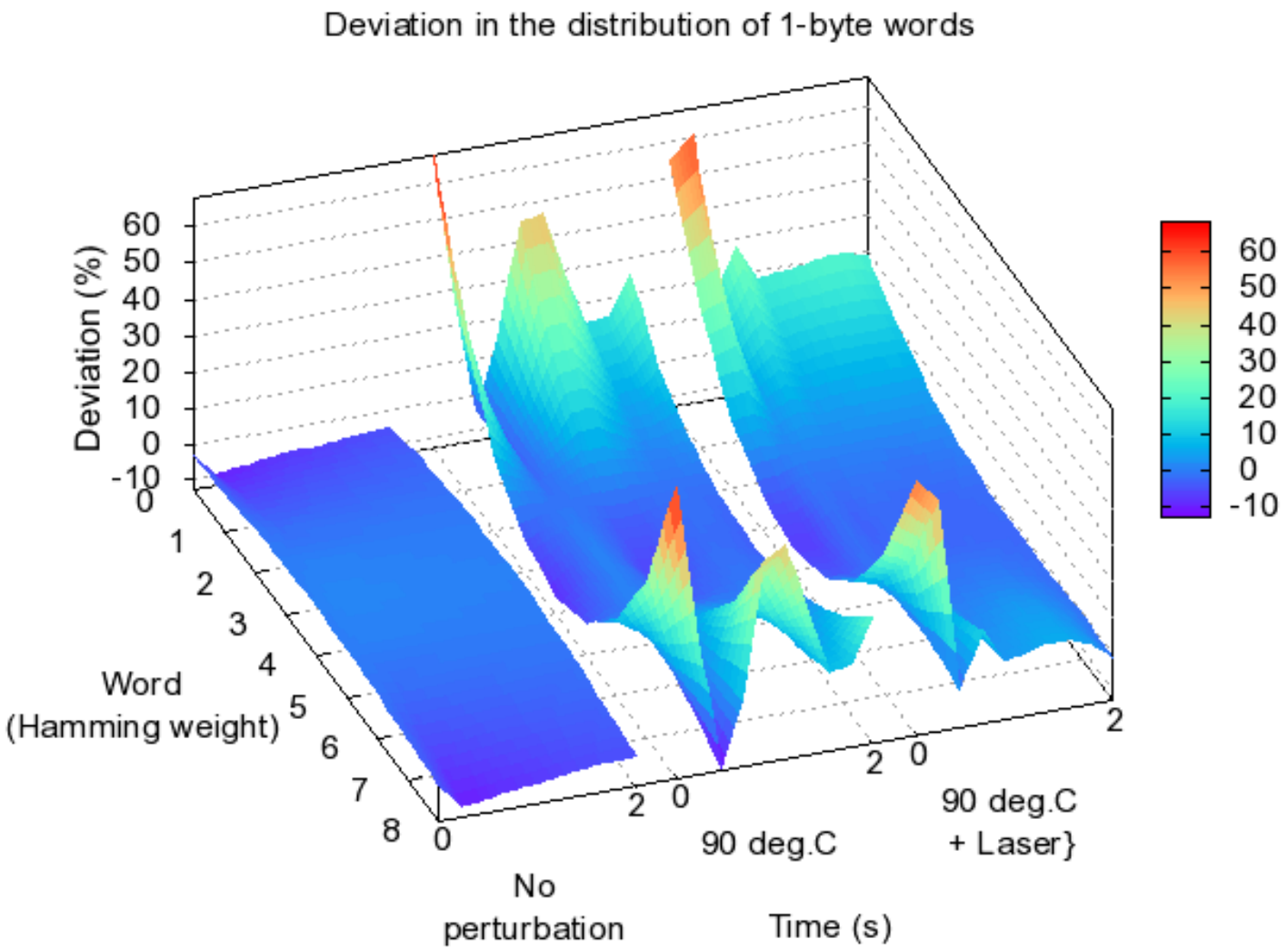
Post-processing : XOR



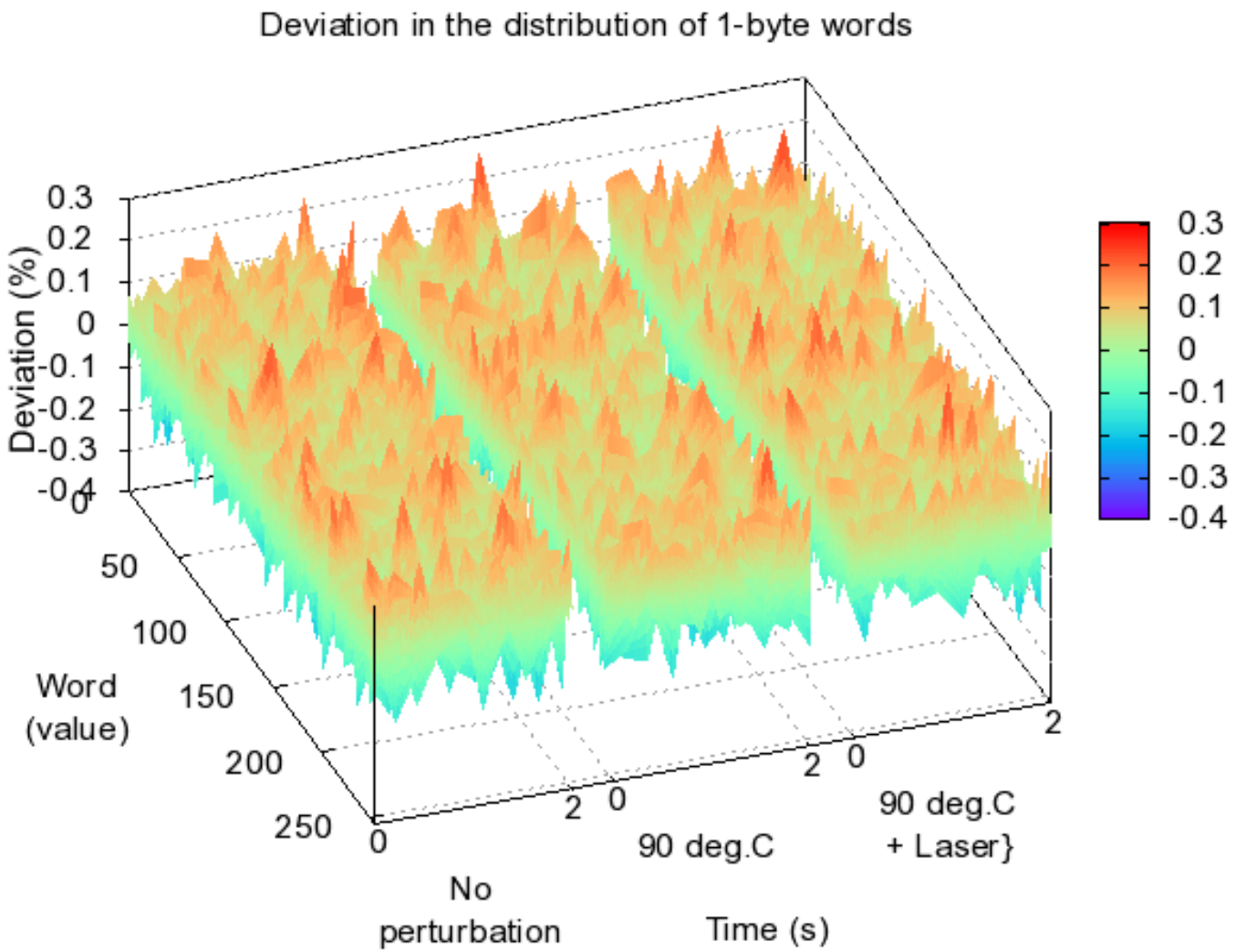
Post-processing : von Neumann corrector



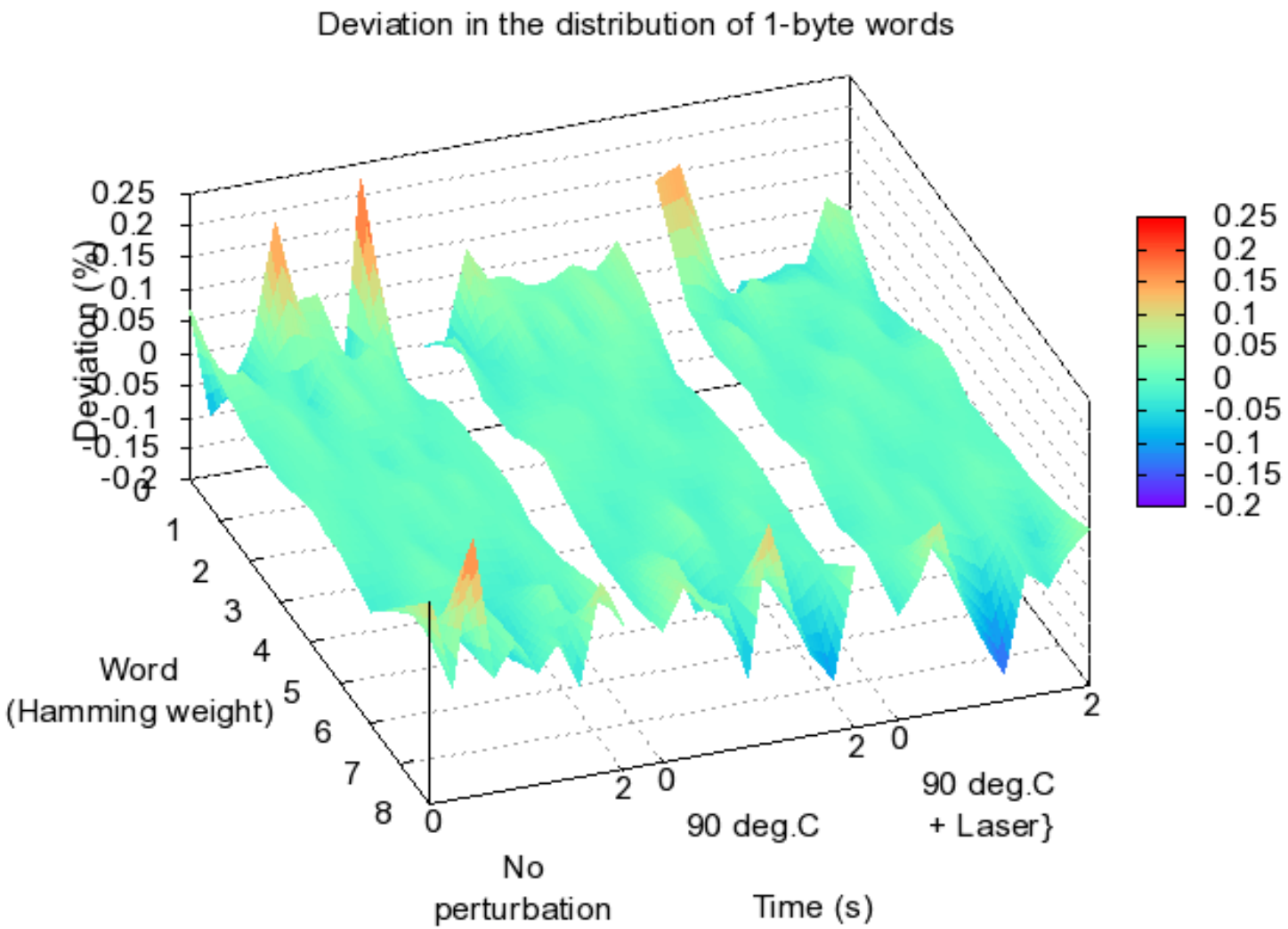
Post-processing : von Neumann corrector



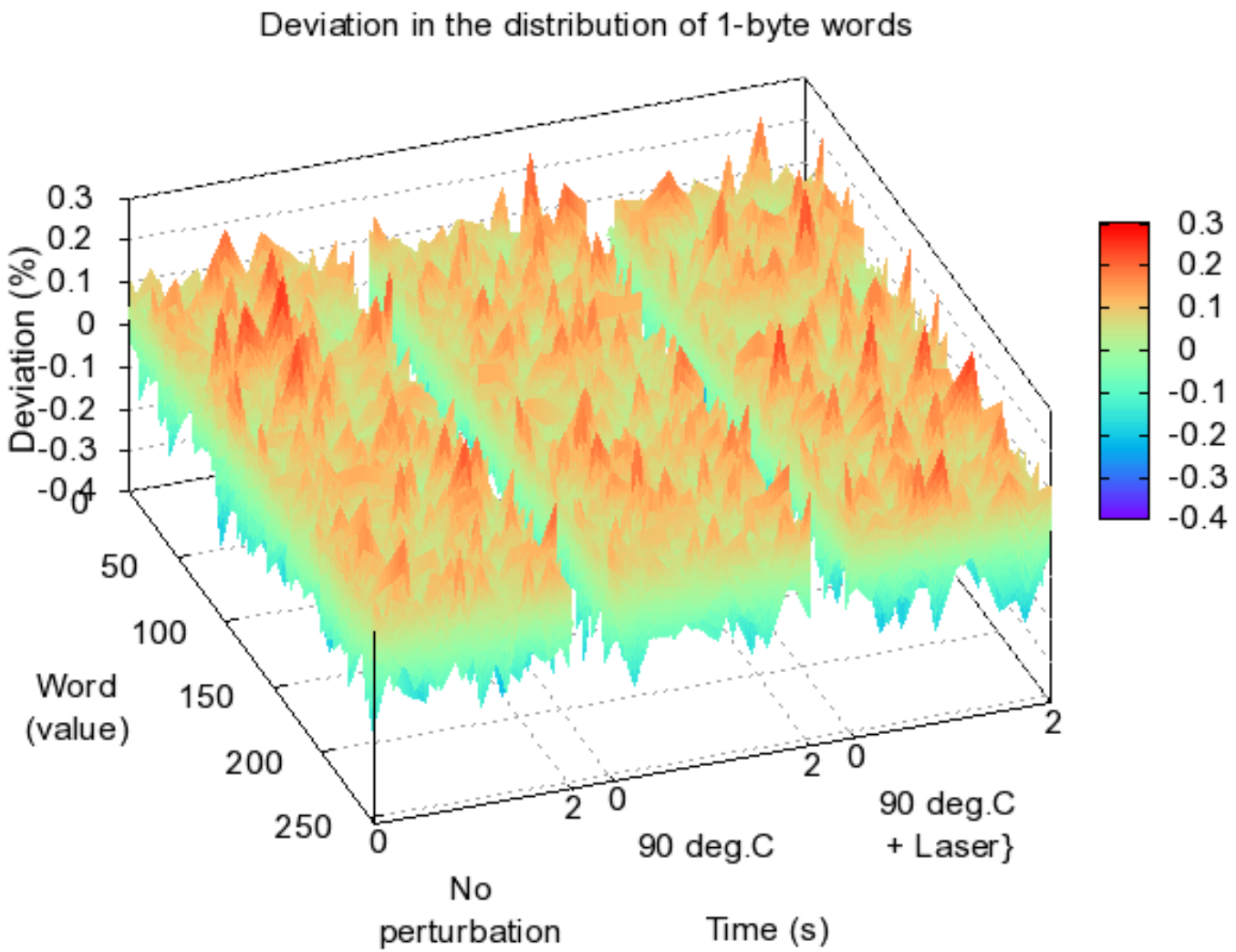
Post-processing : SHA-256



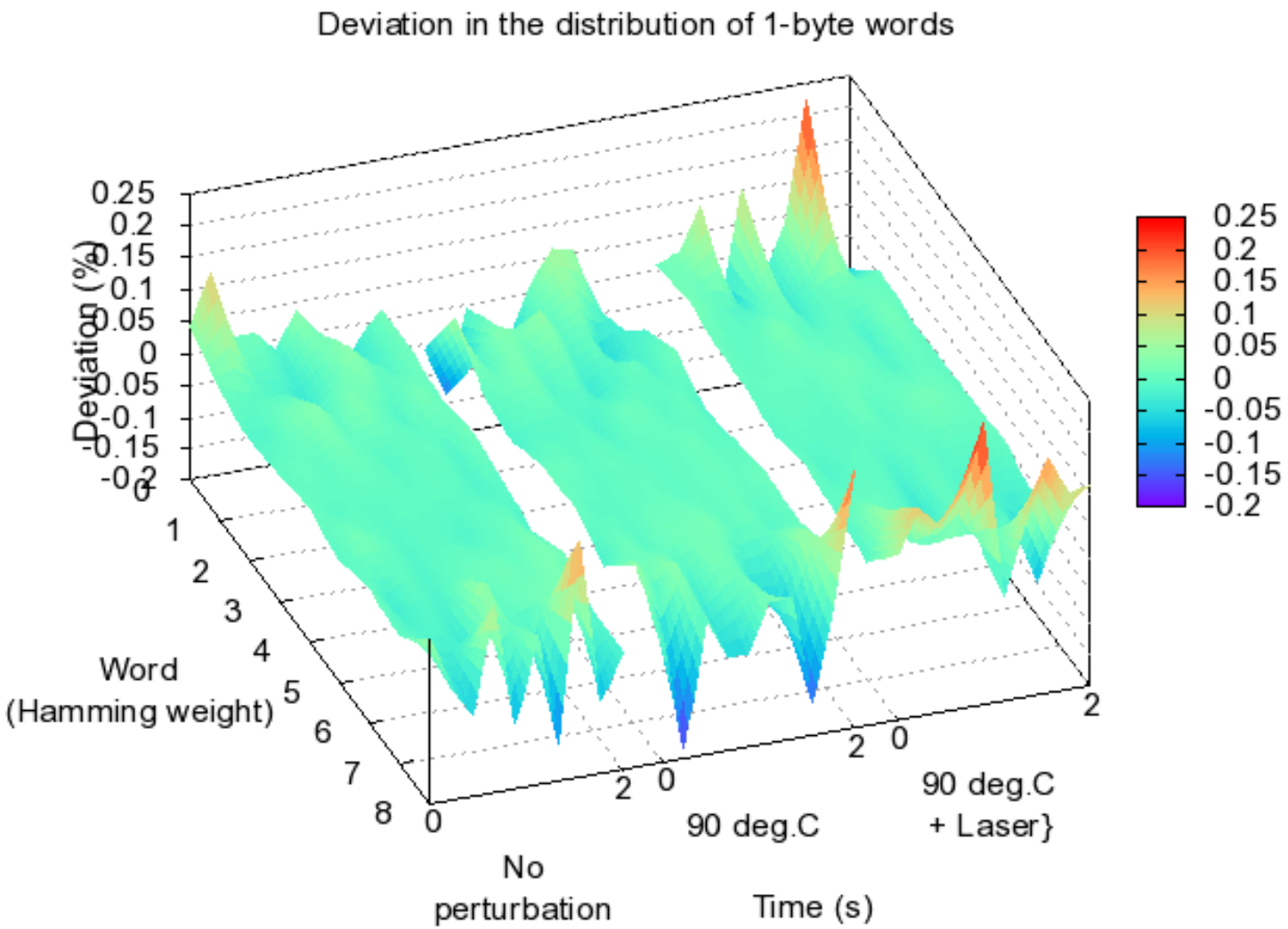
Post-processing : SHA-256



Post-processing : AES-128



Post-processing : AES-128



Outline

Conclusion

- The security of cryptographic schemes depends on the randomness of the numbers used so the behavior of TRNGs under stress must be studied
- Simple experiments can be enough to pertub the workings of a TRNG
- Need to adapt entropy designs and post-processings for best efficiency
- Meaning of test results must be examined carefully