CRYPTARCHI 2017 Smolenice "Formalism to Assess the Entropy and Reliability of Loop PUF"

Jean-Luc Danger[1,2]
Olivier Rioul[1]
Sylvain Guilley[1,2]
Alexander Schaub[1]

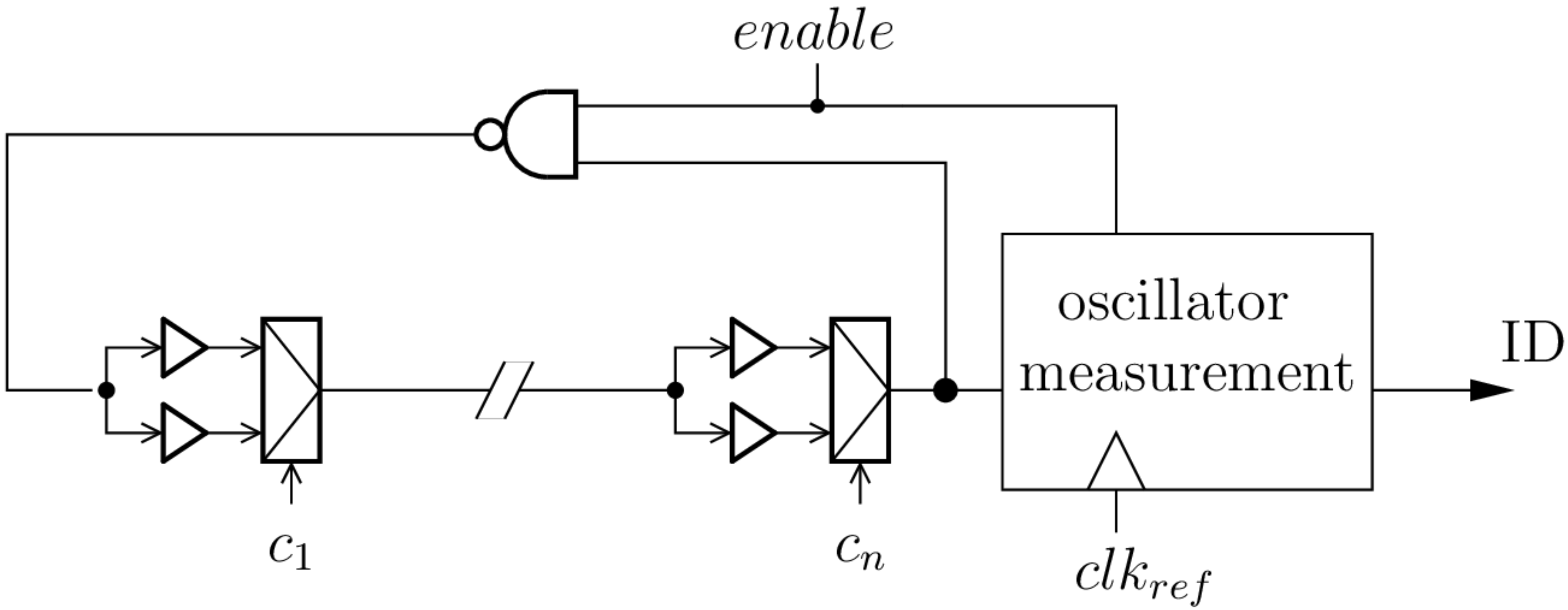
[1] **Télécom ParisTech, LTCI, UPSAY**
[2] **Secure-IC**

Outline

- Loop PUF architecture
- Entropy assessment
- Reliability assessment
- Results on real silicon
- Conclusions

* Depends on algorithm, not implementation

Loop PUF architecture



Operating Mode

Algorithm 2.1 Operating Mode with 2 complementary challenges

Input: Challenge C (a word of n bits)
Output: Response B

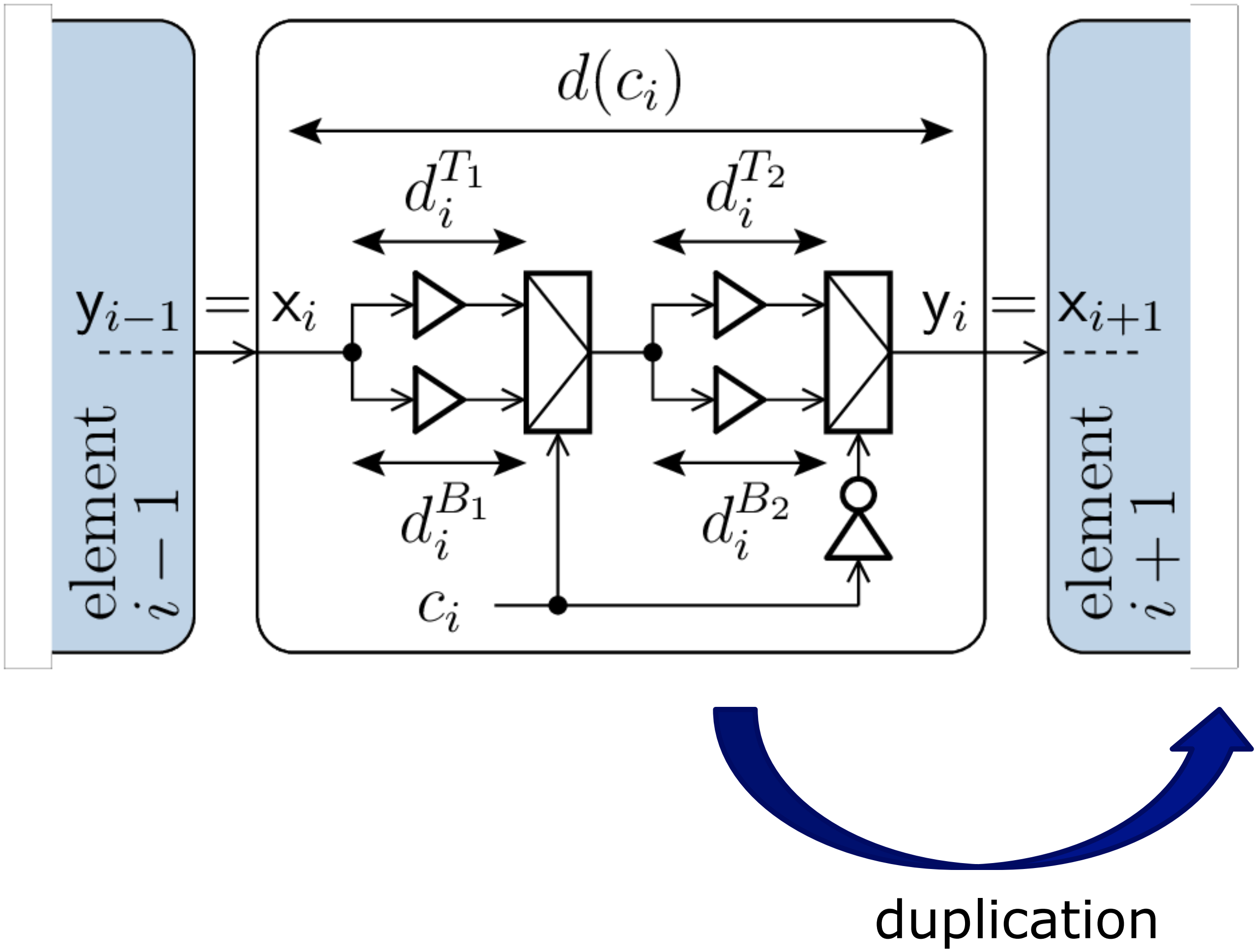
1: Set challenge C
2: Measure $d_C \leftarrow \lfloor L \sum_{i=1}^{n} d(c_i) \rfloor$
3: Set challenge $\neg C$
4: Measure $d_{\neg C} \leftarrow \lfloor L \sum_{i=1}^{n} d(\neg c_i) \rfloor$
5: Compute $\Delta = d_C - d_{\neg C}$
6: Return $B = \text{sign}(\Delta) \in \{\pm 1\}$

The information for each challenge is Δ

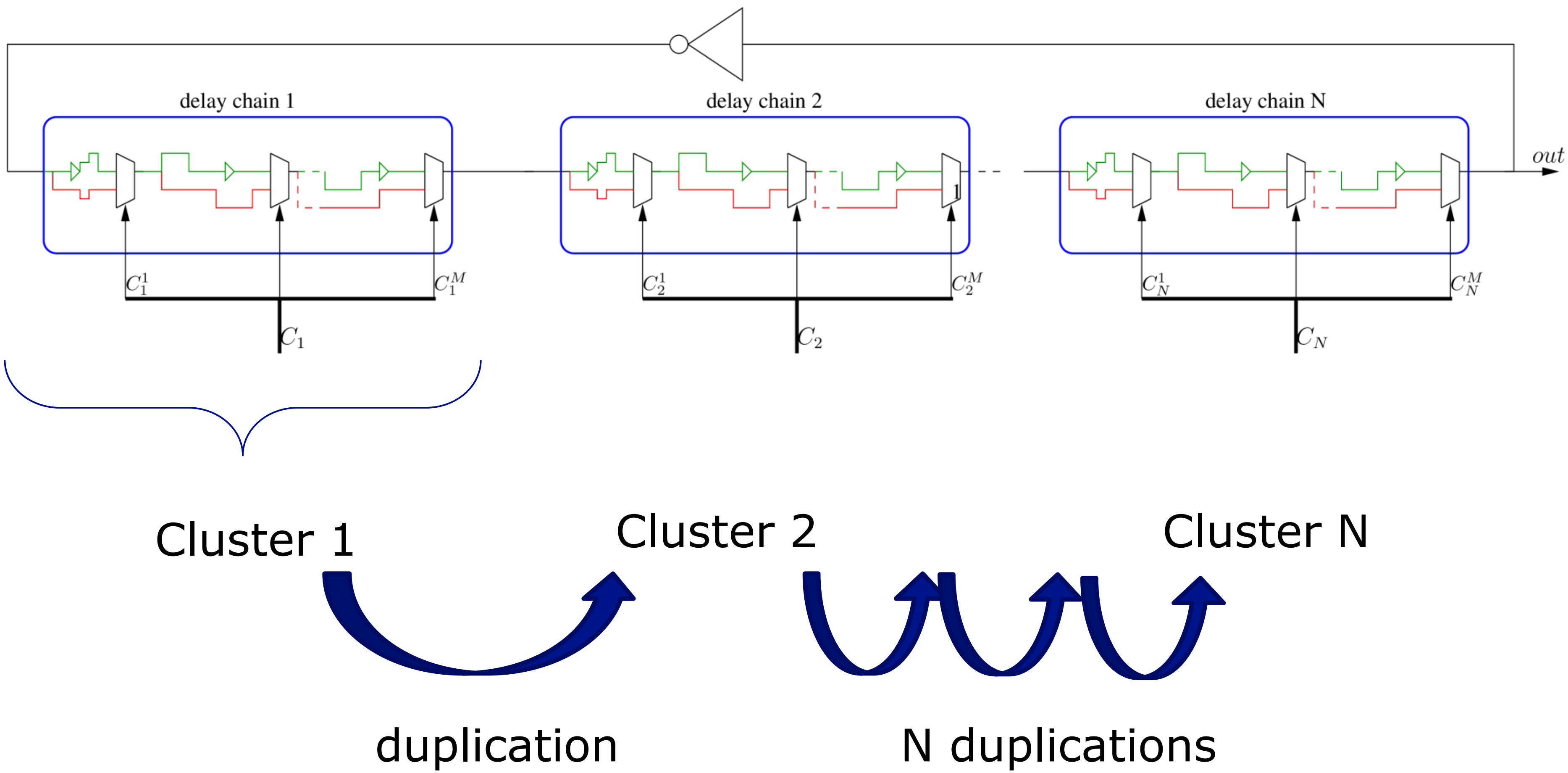
Sign = identifier

Module = reliability

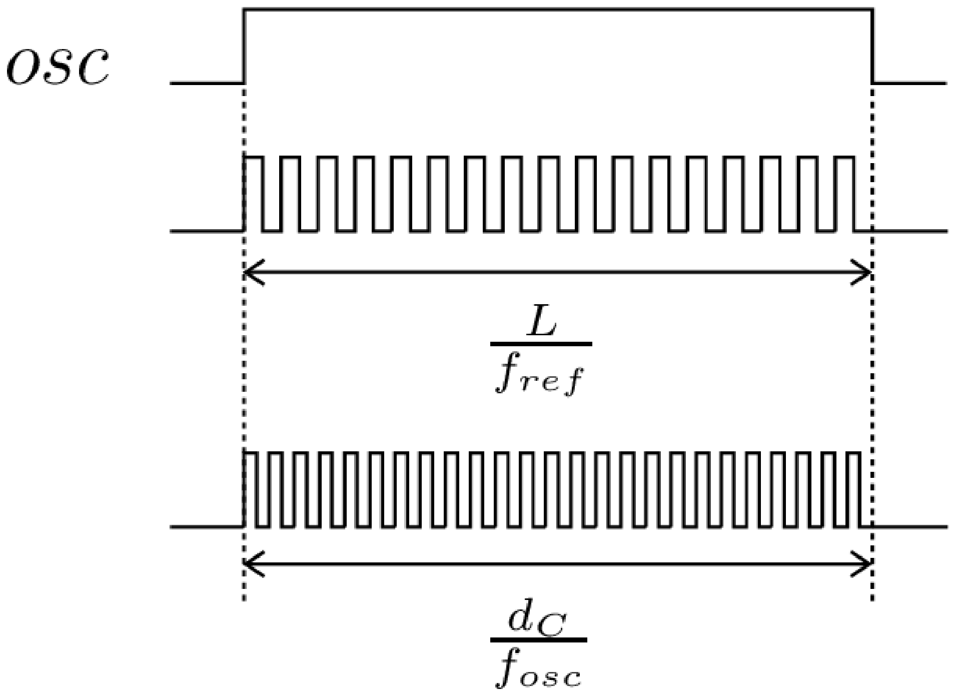
Balance of Delay Elements in ASIC



Balance of Delay Elements in FPGA



Delay measurement



$$d_C = L \cdot \frac{f_{osc}}{f_{ref}}$$

Entropy

❑ For a n-delay LPUF

- ➢ If challenge = Hadamard codeword of n bits => Entropy = n *

For instance for $n = 12$, the n by n Hadamard Matrix is:

$$
\mathcal{C}_{12} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1
\end{pmatrix}
$$

* Rioul, O., Solé, P., Guilley, S., & Danger, J. L. (2016, July). On the Entropy of Physically Unclonable Functions. In *Information Theory (ISIT), 2016 IEEE International Symposium on* (pp. 2928-2932). IEEE.

Entropy with more than n challenges

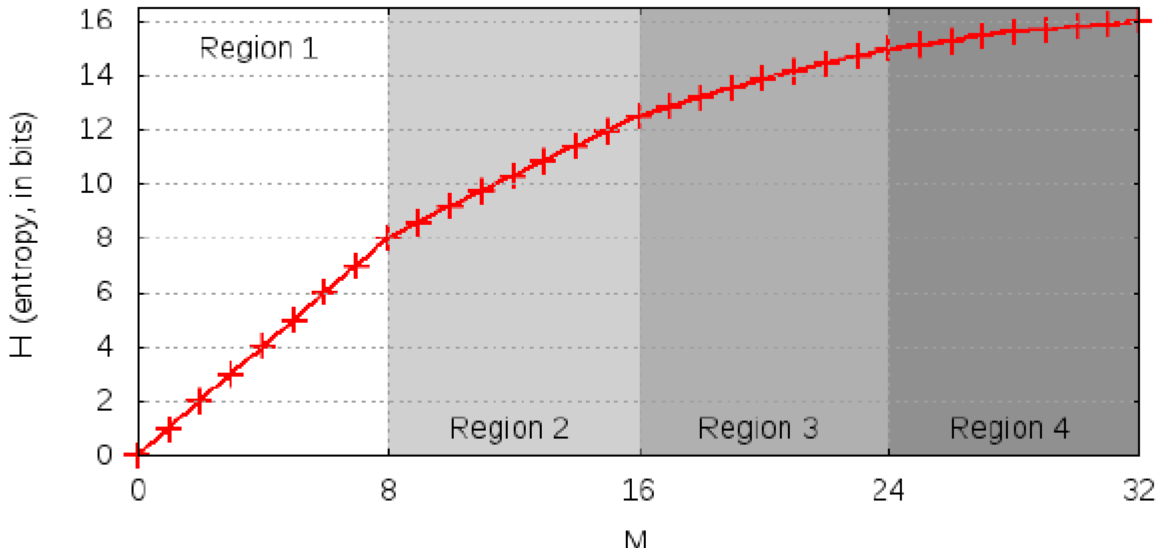


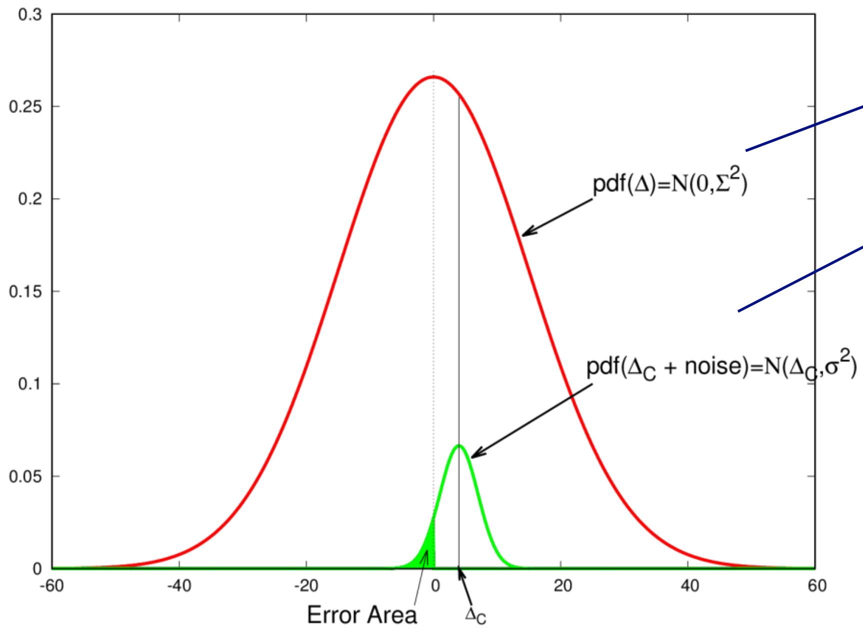
Figure 4: Entropy for n elements as a function of the number M of challenges.

LPUF reliability

$$BER = \mathbb{P}(\text{sign}(\Delta + N) \neq \text{sign}(\Delta)) = Q(\frac{|\Delta|}{\sigma})$$

$$N = \sim \mathcal{N}(0, \sigma^2) \qquad Q(x) = \frac{1}{2}(1 - \text{erf}\,\frac{x}{\sqrt{2}}) = \frac{1}{2}\,\text{erfc}(\frac{x}{\sqrt{2}})$$

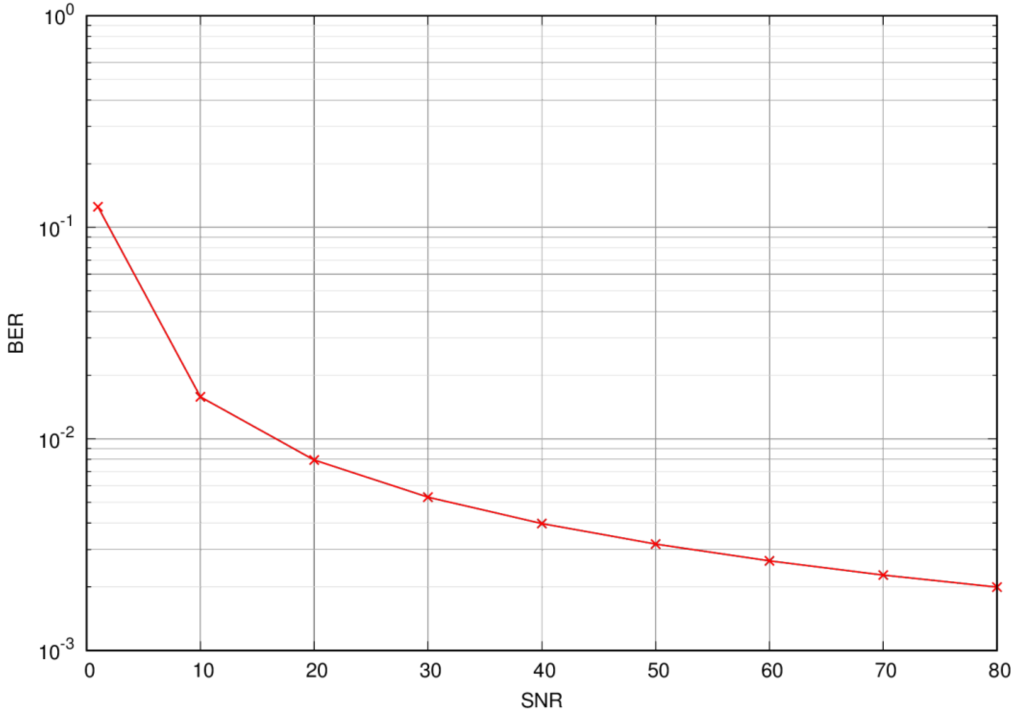
$$\widehat{BER} = \int_0^{+\infty} \mathbb{P}(\Delta) \cdot BER(\Delta) \cdot d\Delta$$



With $SNR = \frac{\Sigma}{\sigma}$

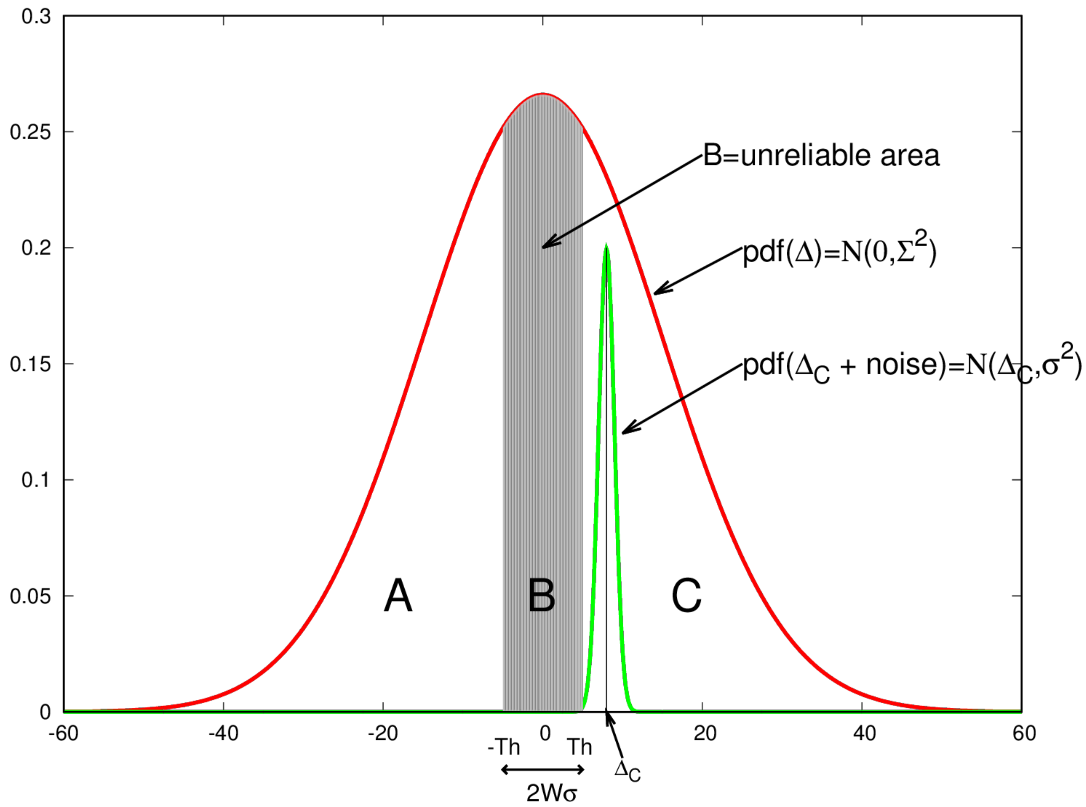
$$\boxed{\widehat{BER} = \frac{1}{4} - \frac{1}{2\pi}\arctan(SNR)}$$

LPUF reliability



The Reliability is not enough ~10^{-3} even with high SNR
=> Needs of secure sketch : Error Correcting codes and Helper data

Reliability enhancement by delay knowledge



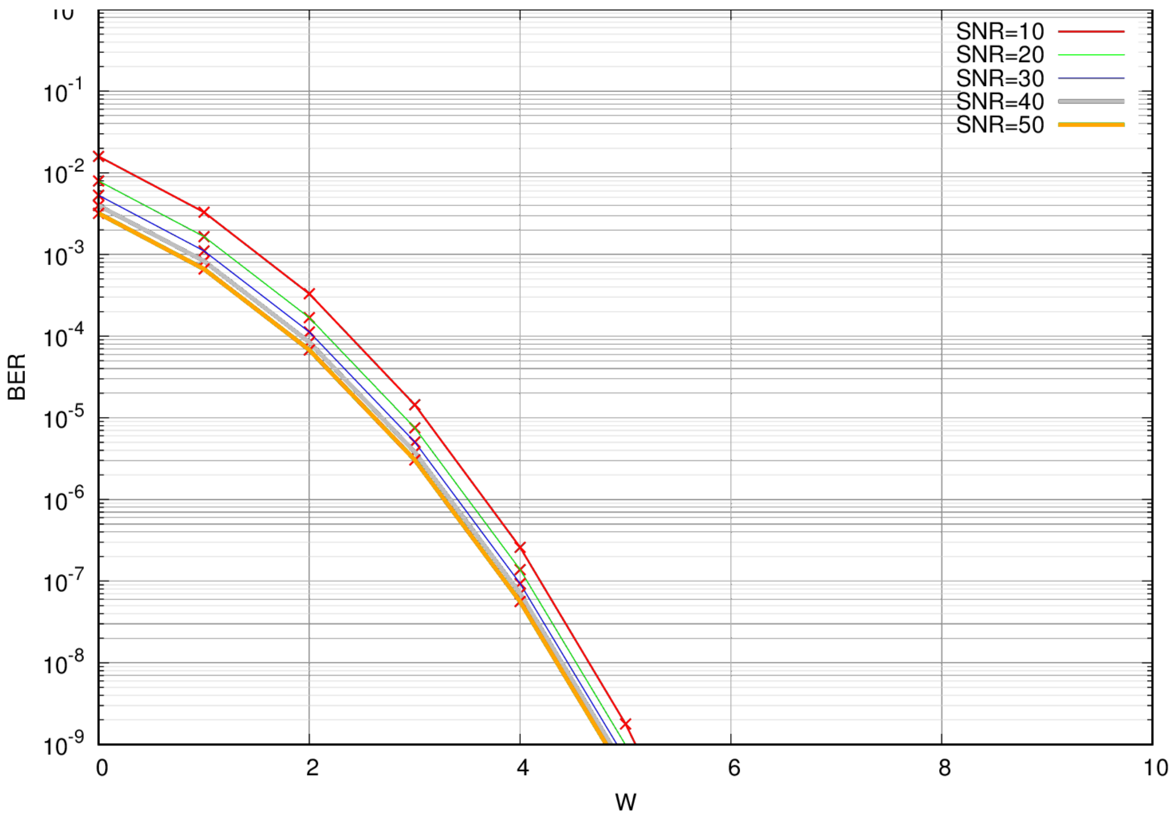
Bit unreliable ⇔ |delay| < Th

Th= Wσ

The bits in the unreliable area "B" are discarded
The helper data indicates the unreliable bits

New BER with filtered bits

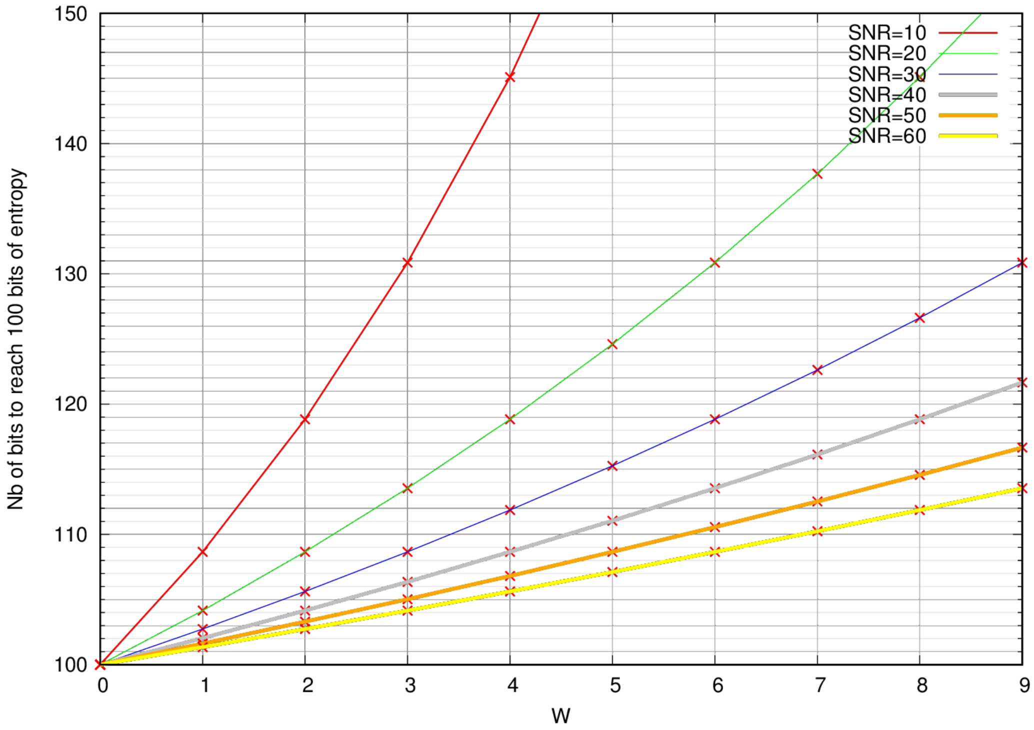
$$\widehat{BER_{filt}} = T(W, \frac{1}{SNR}) + \frac{1}{4}\,\mathrm{erf}(\frac{W}{\sqrt{2} \cdot SNR})(\mathrm{erf}(\frac{W}{\sqrt{2}}) - 1)$$



Entropy after bit filtering

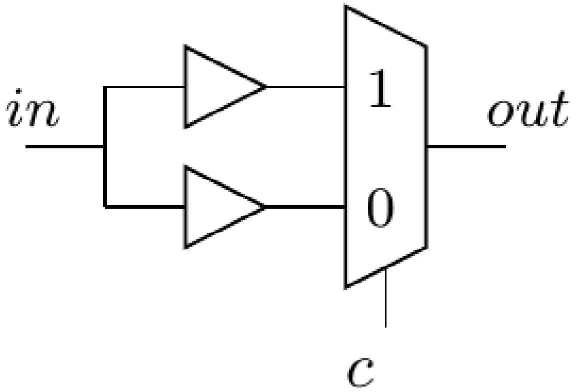
Number of delay elements to reach n bits of entropy with Hadamard codes

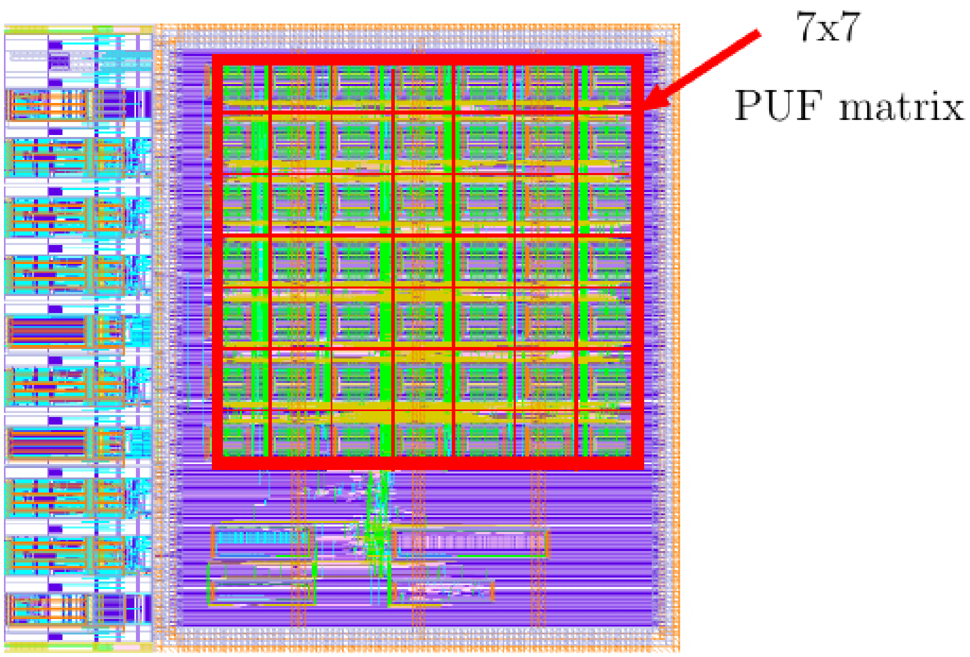
$$n' = \frac{n}{1 - \mathbb{P}(Bit\ unreliable)}) = \frac{n}{\mathrm{erfc}(\frac{W}{SNR})}$$



Results on real silicon

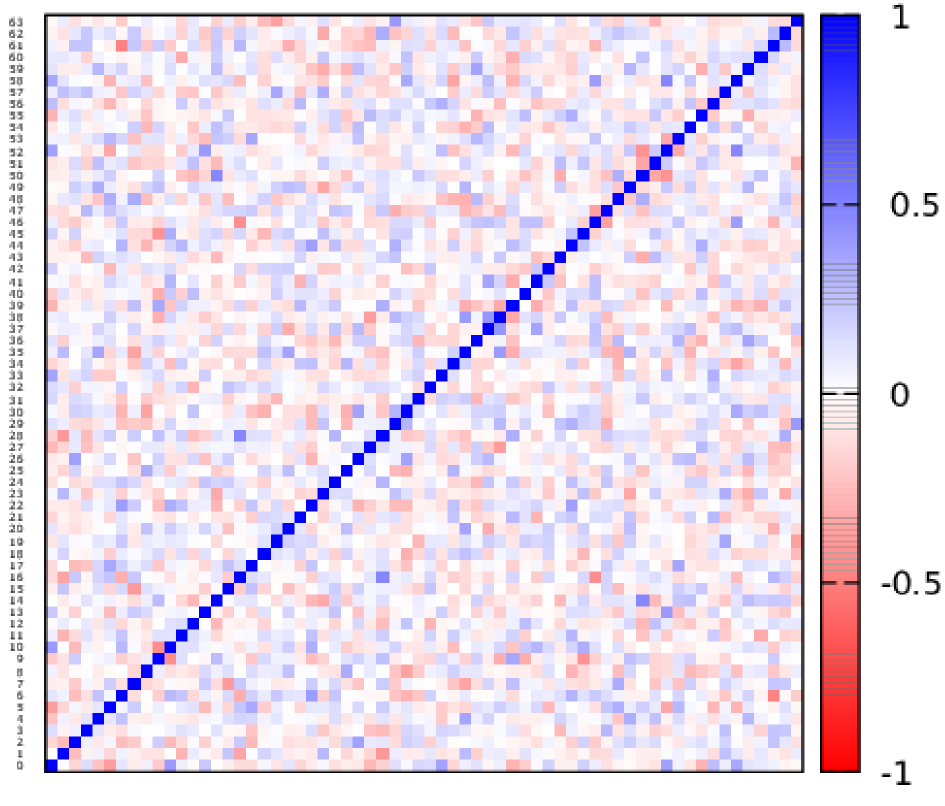
- n=54 cells, 65nm technology





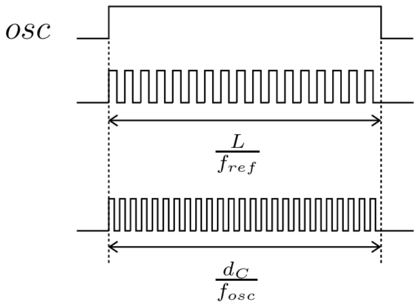
i..i.d. check

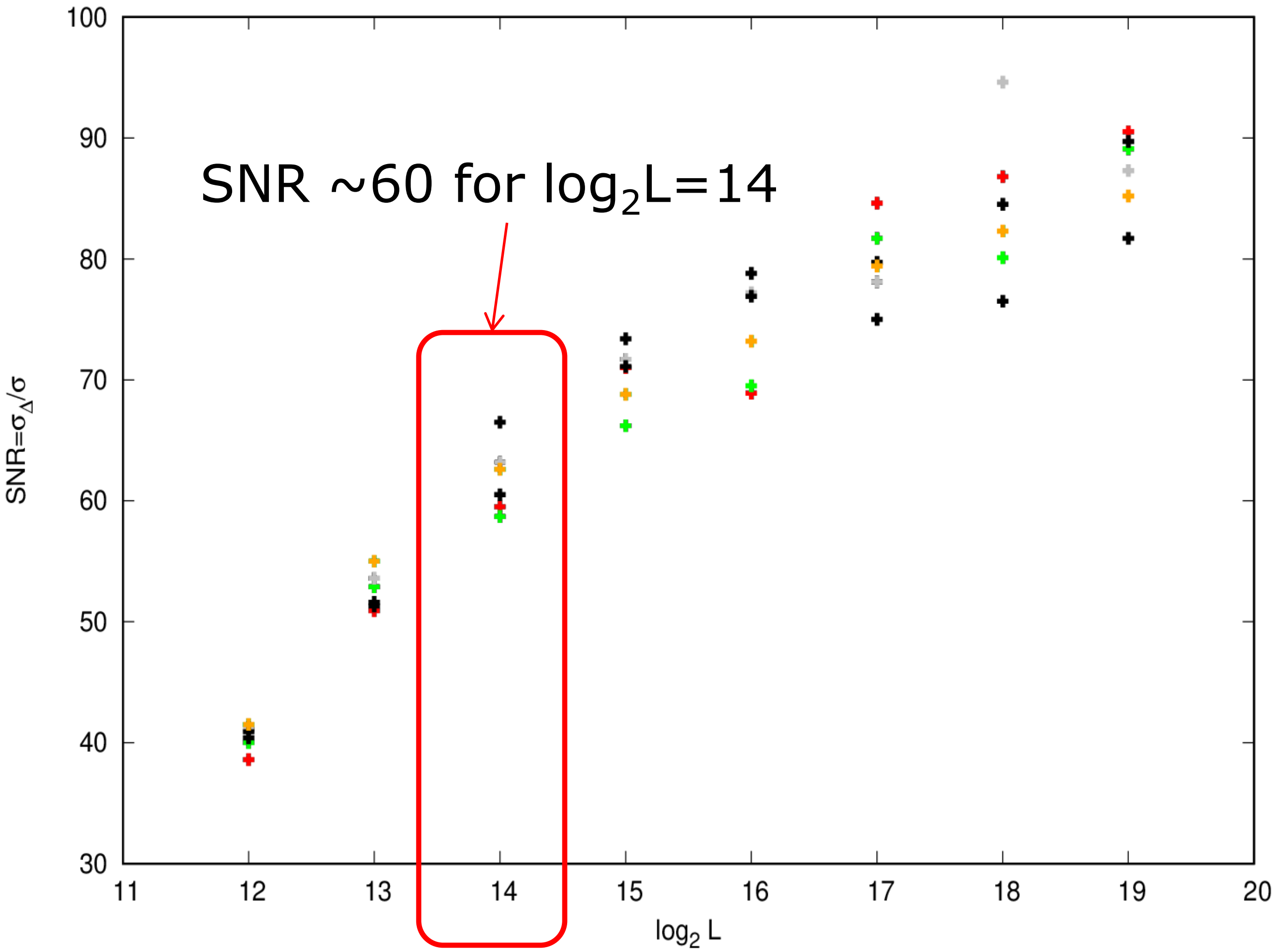
Correlation matrix on the 64 elements of the 49 PUFs



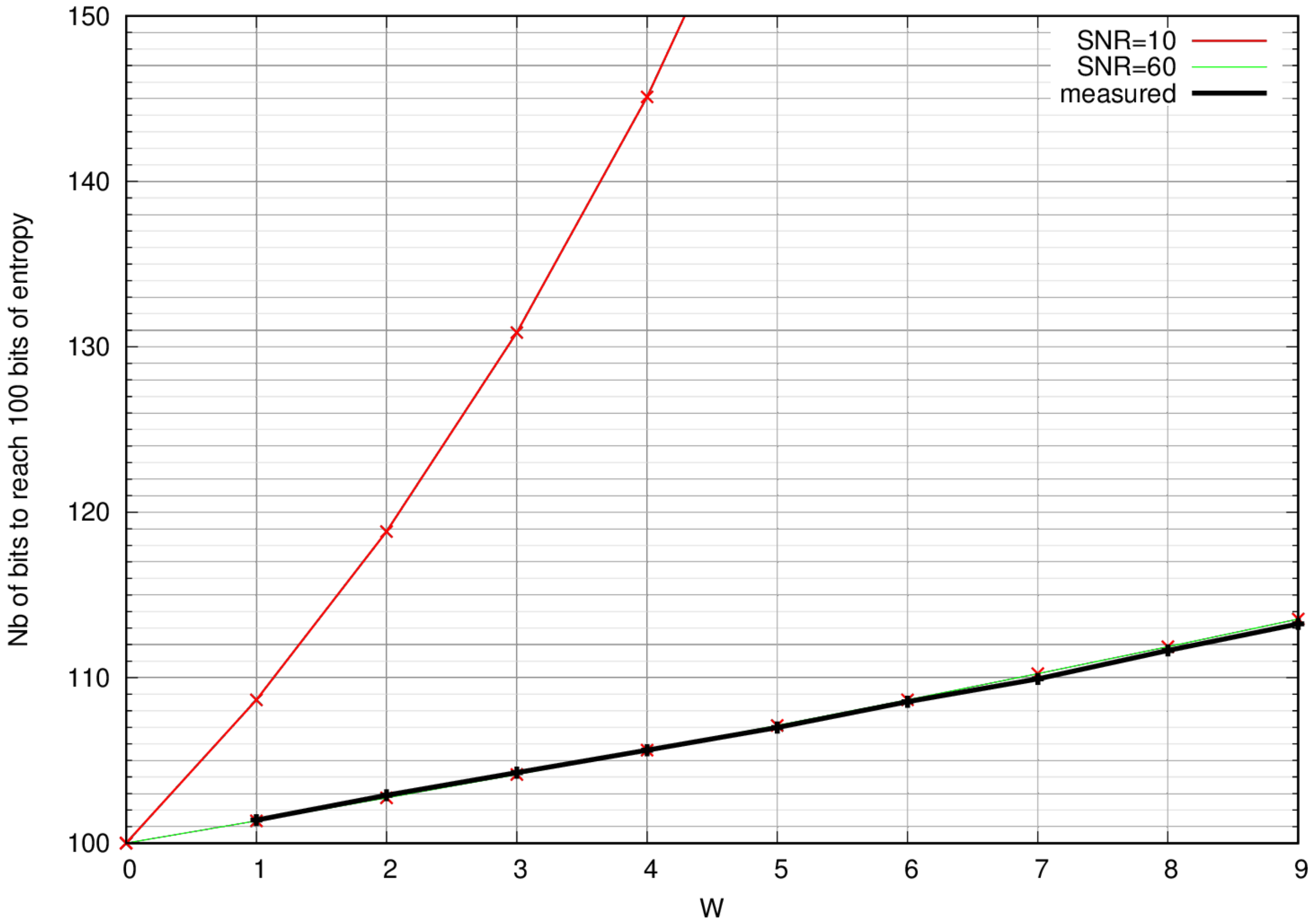
No correlation between the 64 delay elements
=> entropy ~ 64 with Hadamard codes

Impact of the measurement window on the SNR



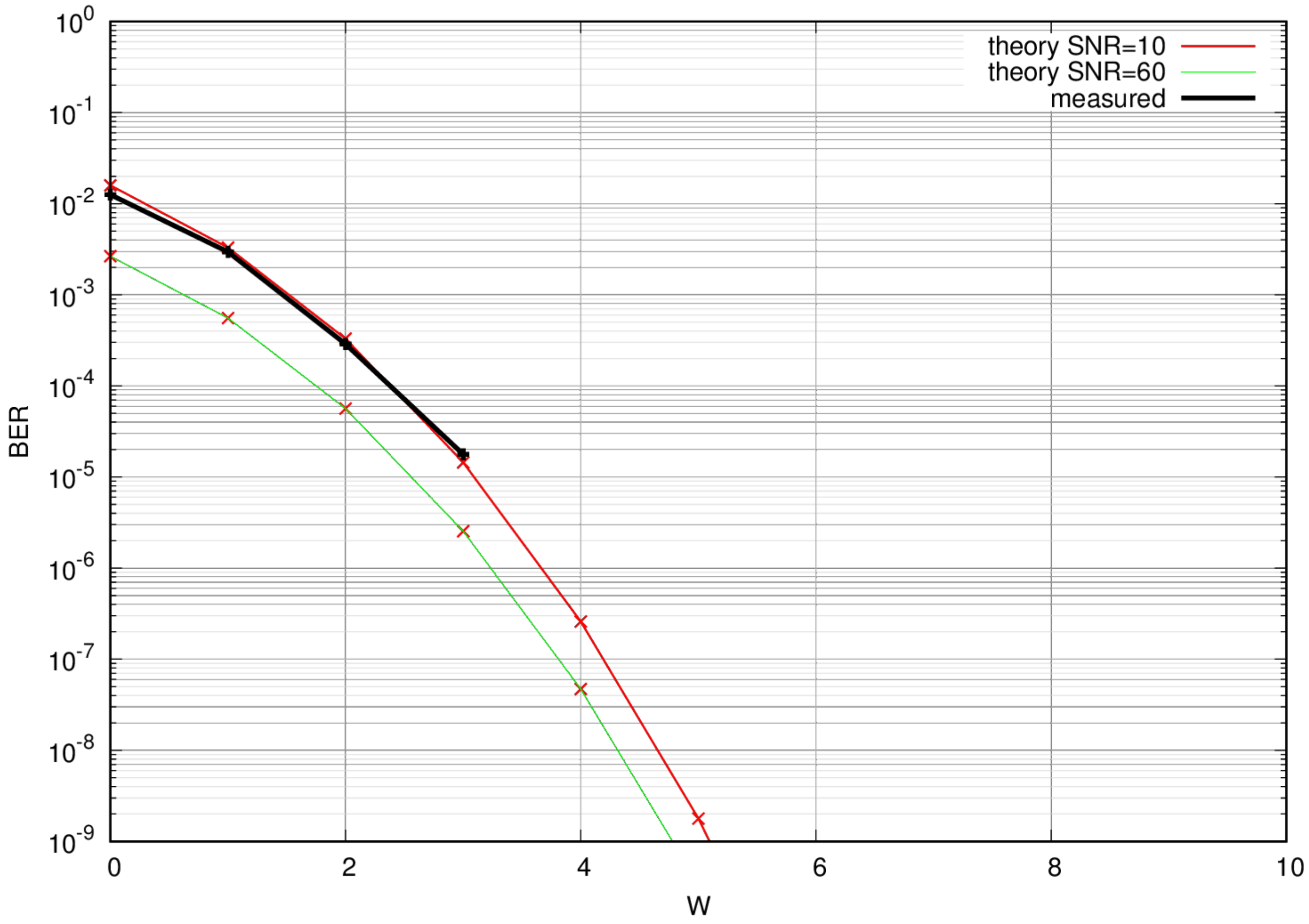


Entropy



SNR=10
SNR=60
measured
Nb of bits to reach 100 bits of entropy
W
150
140
130
120
110
100
0
1
2
3
4
5
6
7
8
9

Reliability: BER results



Conclusions

- **The Entropy of the Loop PUF can be formally obtained if Hadamard codes are used:**
  - Entropy = number of delay elements n
  - The entropy increases non linearly if M > n

N=Number of challenges

- **The reliability of the Loop PUF is low (BER ~10^{-3})**
- **It can be easily improved by exploiting the delay knowledge**
  - The unreliable bits are discarded
  - BER can go down 10^{-9}
  - But more bits are needed to reach the same entropy

THANK YOU
FOR YOUR ATTENTION