# Extracción de entropía en funciones físicas no-clonables de medida compensada

**Guillermo Díez-Señorans, Miguel Garcia-Bosque, Carlos Sánchez-Azqueta, Santiago Celma**

*Grupo de Diseño Electrónico (I3A), Universidad de Zaragoza, Mariano Esquilor s/n 50018, España*

Instituto Universitario de Investigación en Ingeniería de Aragón Universidad Zaragoza

Universidad Zaragoza 1542

GDE Grupo de Diseño Electrónico

## INTRODUCCIÓN

**Retos**

1011

**Respuestas**

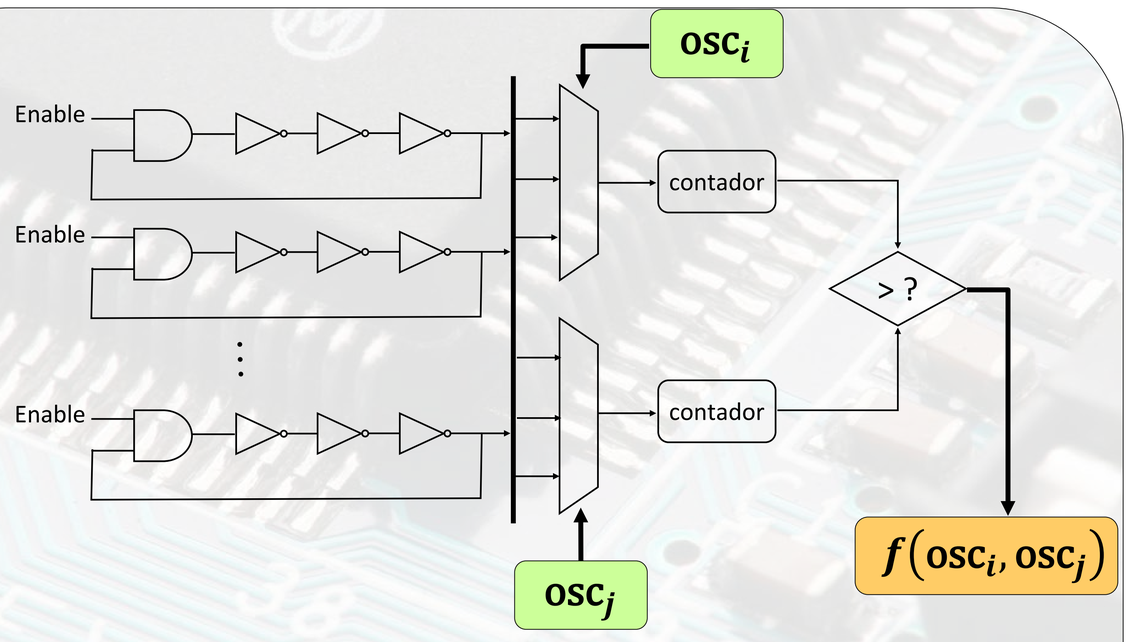
00101100

**PUF**

**IDENTIFICABLE**

**FÍSICAMENTE NO-CLONABLE**

## RO-PUF




$$f(osc_i, osc_j) = \begin{cases} 1, & \text{si } osc_i \text{ es más rápido que } osc_j \\ 0, & \text{en otro caso} \end{cases}$$

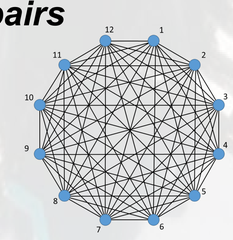
## TOPOLOGÍAS

$osc_i > osc_j$ y $osc_j > osc_k$ $\Rightarrow$ $osc_i > osc_k$

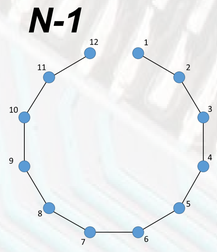
¡Correlación entre bits!

Topología (e.g. $N = 12$)

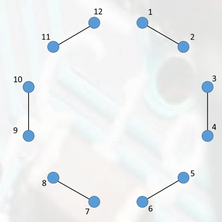
***All-pairs***



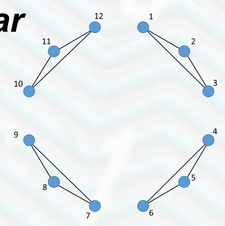
***N-1***



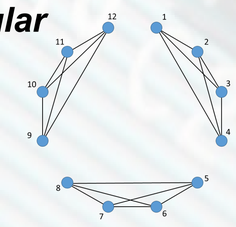
***1-out-of-2***



***3-modular***

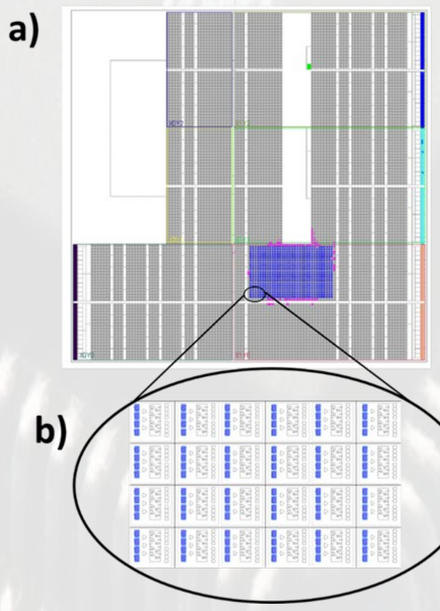


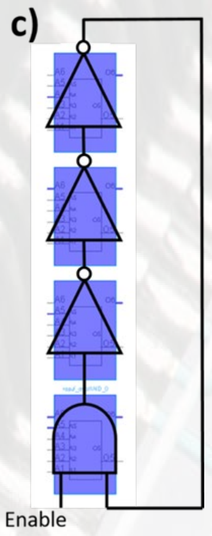
***4-modular***



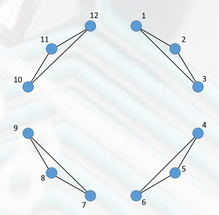
**Nueva propuesta**

## EXPERIMENTO




**Tomamos $N$ osciladores aleatoriamente**



**Se evalúa utilizando una cierta topología**

**Distribución de probabilidad**

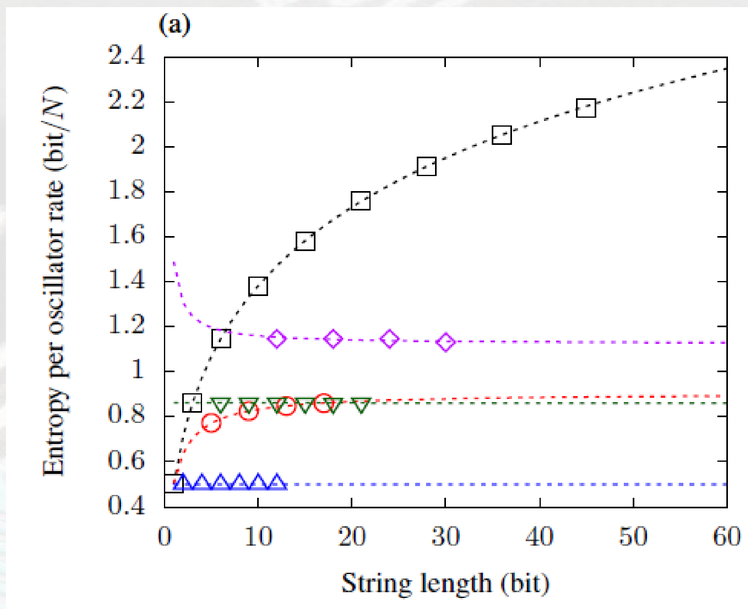
**Cálculo de entropía:**

$$S = -\sum p \log(p)$$

## RESULTADOS

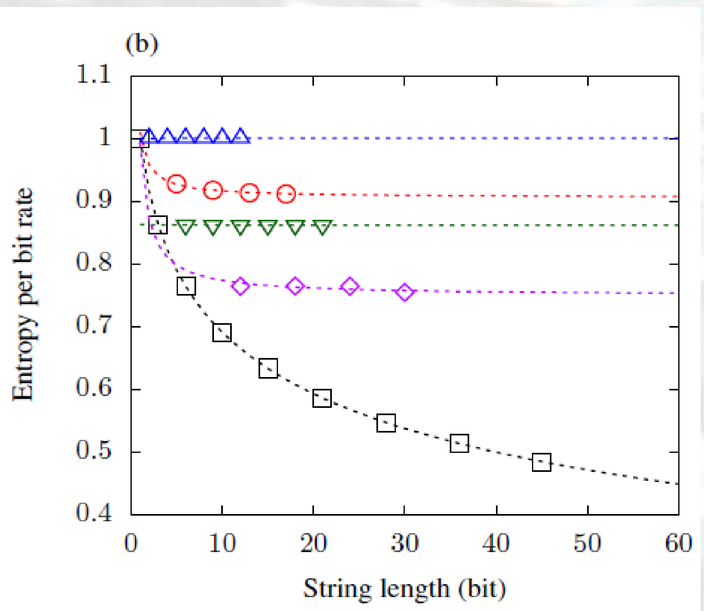
***a)* Entropía por oscilador: $S/N$**

**Eficiencia en consumo de recursos hardware: potencia y silicio**




***b)* Entropía por bit: $S$/bit**

**Resistencia frente al criptoanálisis**




*All-pairs* *N-1* *1-out-of-2* *3-modular* *4-modular*