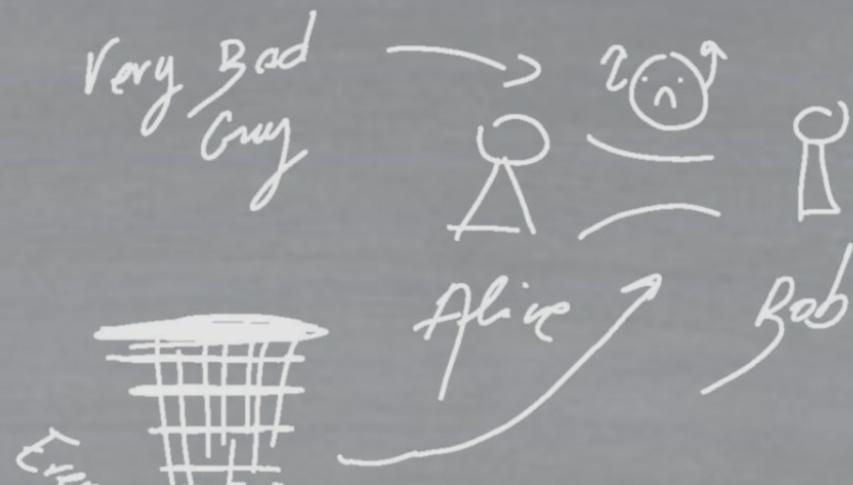


$(pk, sk) \leftarrow \text{Kyber.KeyGen}(\lambda)$   
 $(c, K) \leftarrow \text{Kyber.Encaps}(pk)$   
 $K' \leftarrow \text{Kyber.Decaps}(sk, c)$

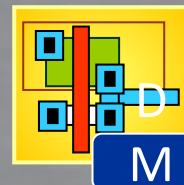
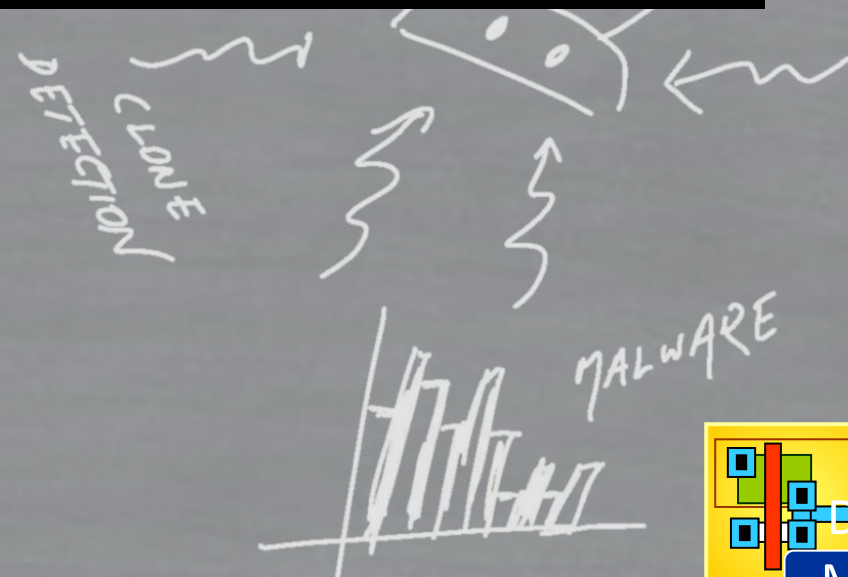
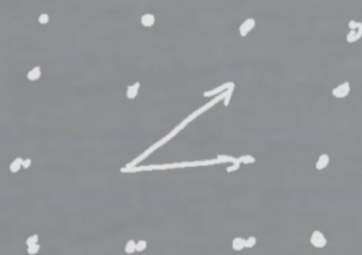


## Reto 5: El desafío del borrado seguro de claves

Fix  $u \in \mathbb{Z}_q^m$

$\{v \in \mathbb{Z}^m \mid v_i = \langle a_i, u \rangle \bmod q\}$

$E_1$  / Isogeny



# ¿Qué hacemos con las claves cuando los dispositivos alcanzan el final de su vida útil?



## Guía de Seguridad de las TIC CCN-STIC 804

### Dstrucción

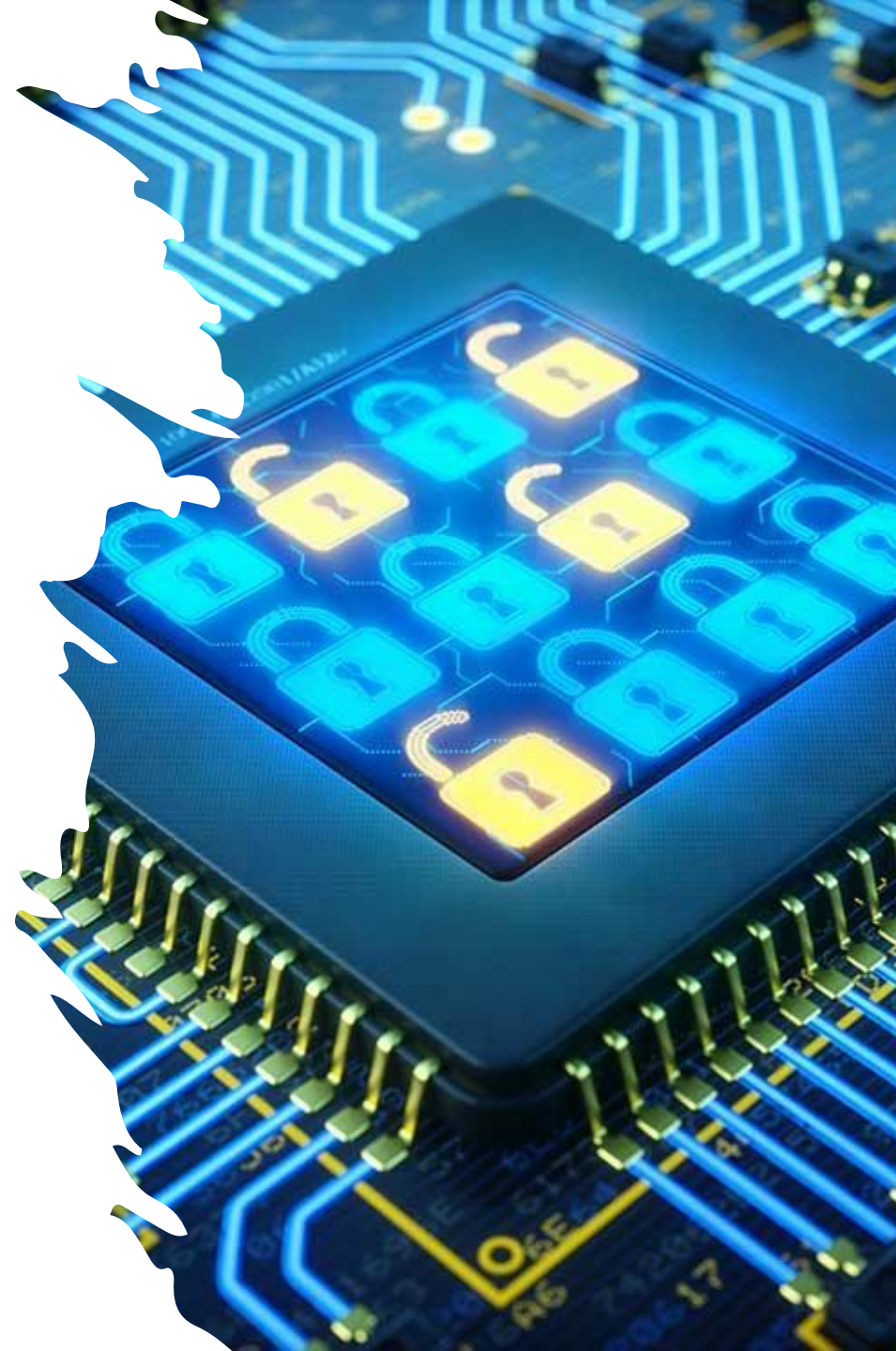
- ✓ eliminación de original y copias
- ✓ se debe garantizar su destrucción, aunque por política puede requerirse su retención durante un periodo a efectos de auditoría

## NIST Special Publication 800-88

- 1. Borrado lógico:** Uso de software o hardware para sobrescribir áreas de almacenamiento accesibles al usuario con datos no sensibles.
- 2. Purga:** Métodos como sobrescritura, borrado de bloques y borrado criptográfico. Incluye el uso de comandos especializados en el dispositivo para aplicar técnicas avanzadas.
- 3. Destrucción:** Métodos físicos que aseguran que los datos sean irrecuperables incluso con técnicas avanzadas de laboratorio. Ejemplos: pulverización, incineración, trituración y desintegración.



**Funciones Físicas  
No clonables  
(PUFs)**

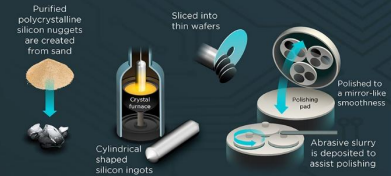




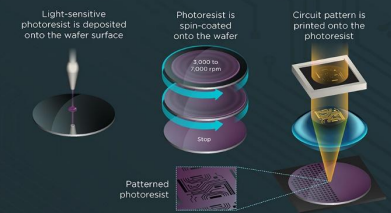
## How a Chip is Born

A glimpse into the manufacturing of a microchip, the tiny building block that runs complex technological devices

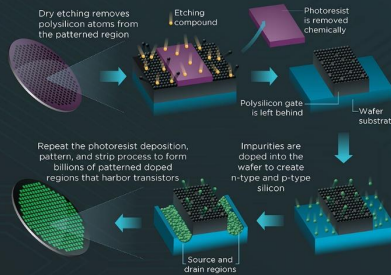
### 1. Laying the foundation: from sand to silicon wafers



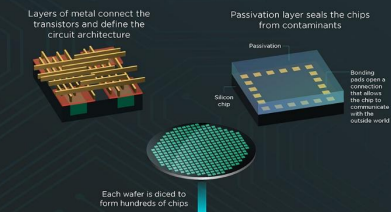
### 2. Creating circuit patterns with photolithography



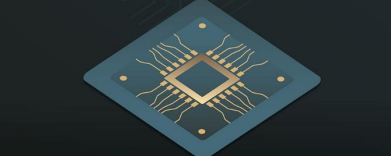
### 3. Building transistors: etching and doping



### 4. Packaging the final product



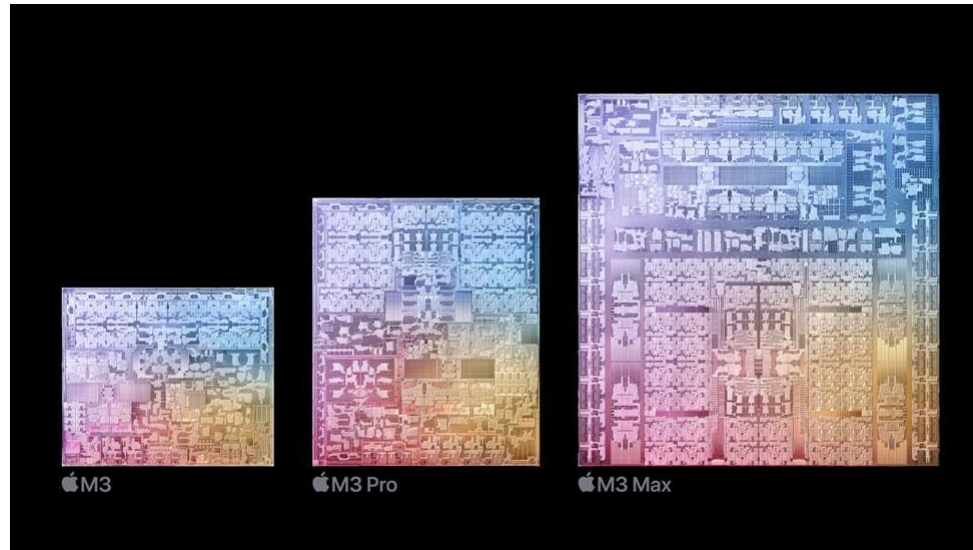
### 5. Connect the chip to the real world!



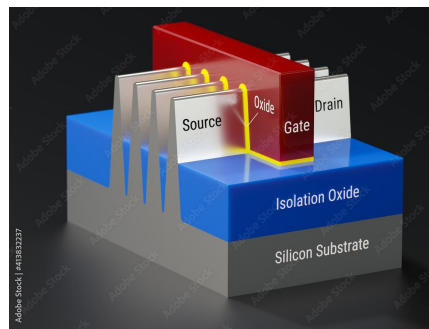
# ¿Qué es un PUF?

Una **función física no-clonable (PUF)** es un circuito digital que usa las **variaciones incontrolables** introducidas en los **procesos de fabricación** para generar una **huella digital única** de cada dispositivo

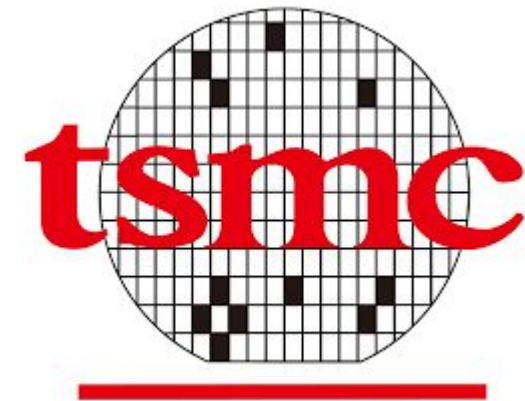
## Algunos datos interesantes



**M3MAX**  
**92.000 millones**  
de transistores



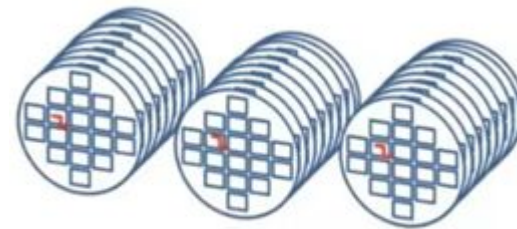
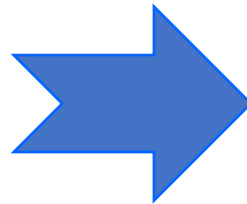
El proceso de fabricación de 3nm  
(marketing) tiene una CGP de 45 nm



# ¿Qué es un PUF?

Una **función física no-clonable (PUF)** es un circuito digital que usa las **variaciones incontrolables** introducidas en los **procesos de fabricación** para generar una **huella digital única** de cada dispositivo

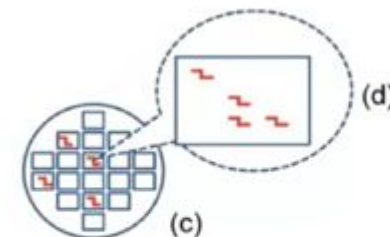
## Variaciones Procesos de Fabricación



a) Lot-to-lot variation



b) Wafer-to-wafer variation

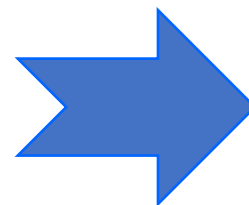


c) Chip-to-chip or across-wafer variation  
d) Within-chip variation

# ¿Qué es un PUF?

Una **función física no-clonable (PUF)** es un circuito digital que usa las **variaciones incontrolables** introducidas en los **procesos de fabricación** para generar una **huella digital única** de cada dispositivo

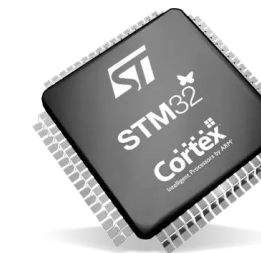
## Variaciones Procesos de Fabricación



ID:817483993377263



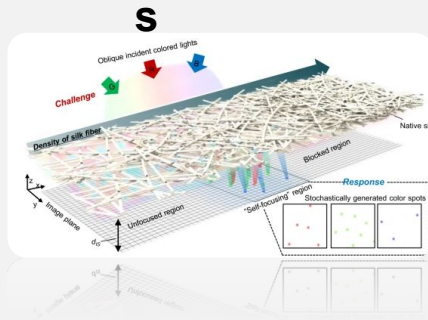
ID:293998874302939



ID:029388043903738

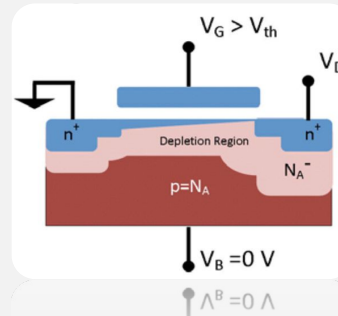
# Tipos de PUFs

## Óptico



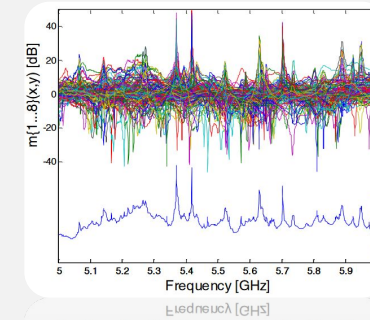
Patrones introducidos en encapsulado

## Electrónico



Explotación de Variaciones físicas y eléctricas

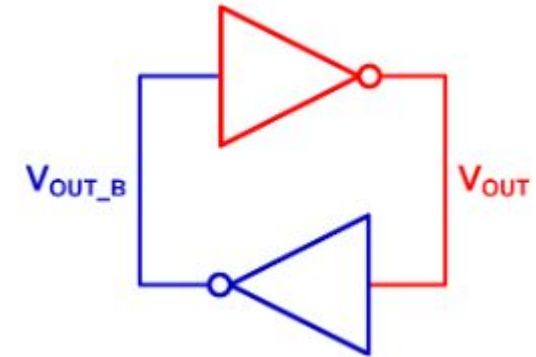
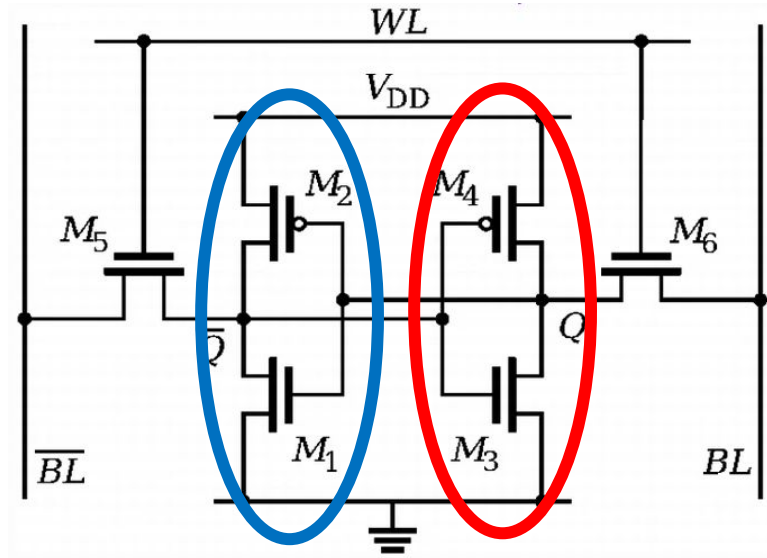
## Otro



Otros fenómenos como RF, magnetismo, etc.

# PUFs Electrónicos: SRAM-PUF

Celda SRAM 6T CMOS



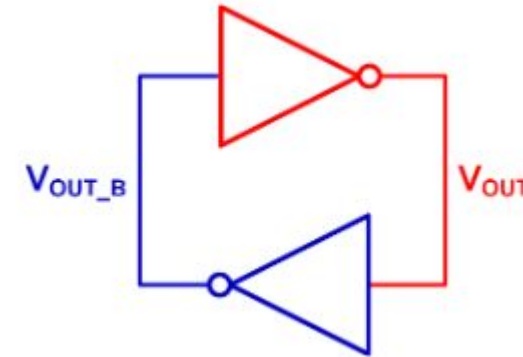
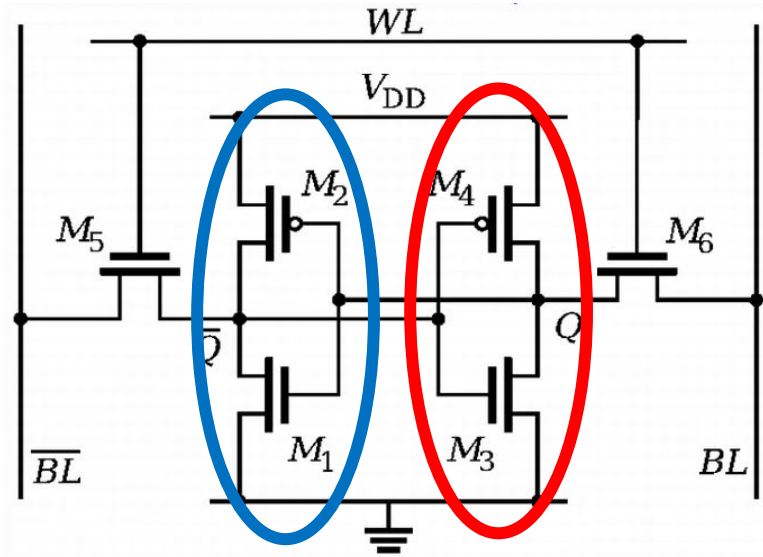
¿Cuál es su estado tras la inicialización (power-up)?

Depende del desajuste físico entre los transistores  $M_2$  y  $M_4$



# PUFs Electrónicos: SRAM-PUF

Celda SRAM 6T CMOS

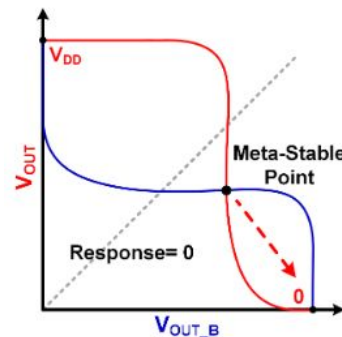


¿Cuál es su estado tras la inicialización (power-up)?

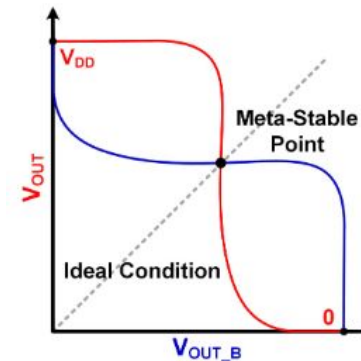
Depende del desajuste físico entre los transistores M2 y M4

Pregunta=>Dirección de memoria  
Respuesta=> Bit leído

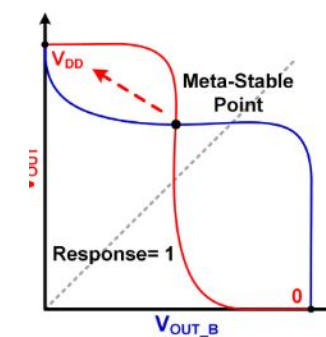
Genera un '0'



Ideal

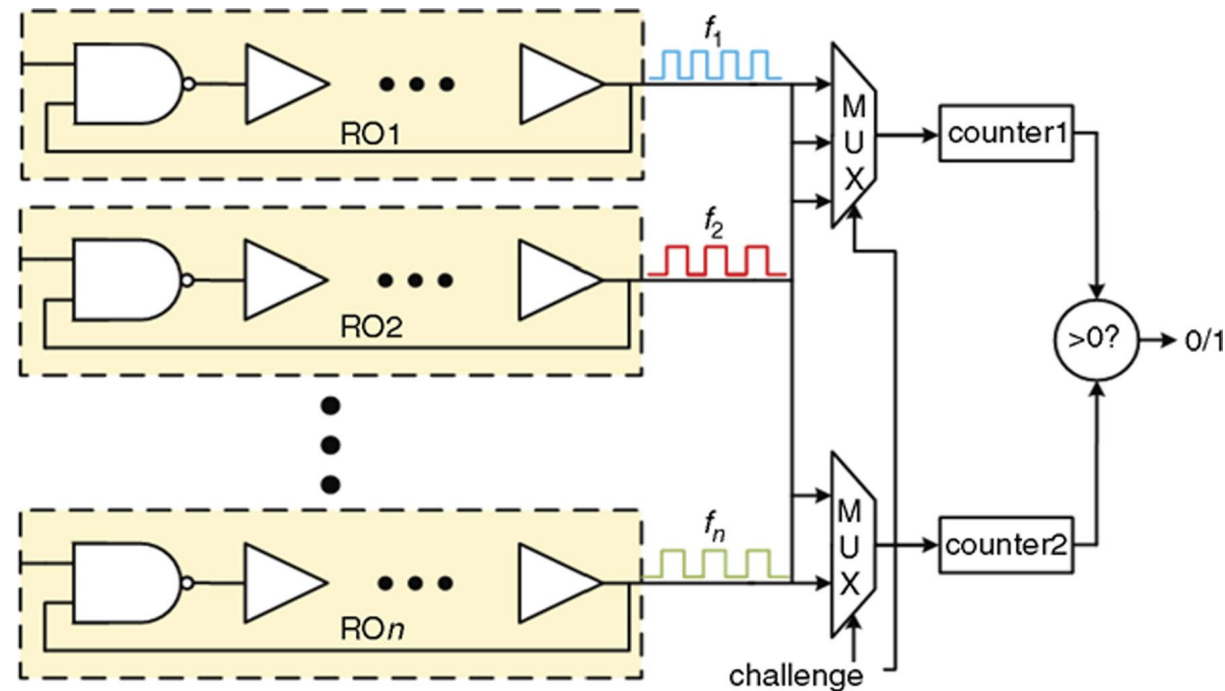


Genera un '1'



# PUFs Electrónicos: RO-PUF

Este PUF se basa en la **comparación de frecuencias de oscilación** entre anillos oscilantes (ROs) idénticos. La variabilidad de los procesos de fabricación hace que los retardos en los anillos sean diferentes



Pregunta=> Anillos a comparar

Respuesta=> Quien genera la frecuencia mayor

# RETO: ¿Cómo borramos los PUFs?

Al depender la clave de una característica física, el borrado lógico o los típicos mecanismos físicos (campos magnéticos) usados para el borrado de discos duros no son una solución a considerar.



En este reto se propone investigar sobre mecanismos de bajo coste y con posibilidad de ser utilizados de manera remota que permitan realizar un “borrado” seguro del PUF al final de su vida útil. Concretamente, se propone investigar el uso de fenómenos de envejecimiento (NBTI y HCI) para el borrado final del PUF.

Enviar ideas y propuestas a [hmartin@uc3m.es](mailto:hmartin@uc3m.es) con el asunto "CryptoClub - RETO 5"