XIII JORNADA DE JÓVENES INVESTIGADORES/AS DEL I3A

Implementación de una PUF basada en osciladores digitales no-lineales reconfigurables para la autenticación de dispositivos

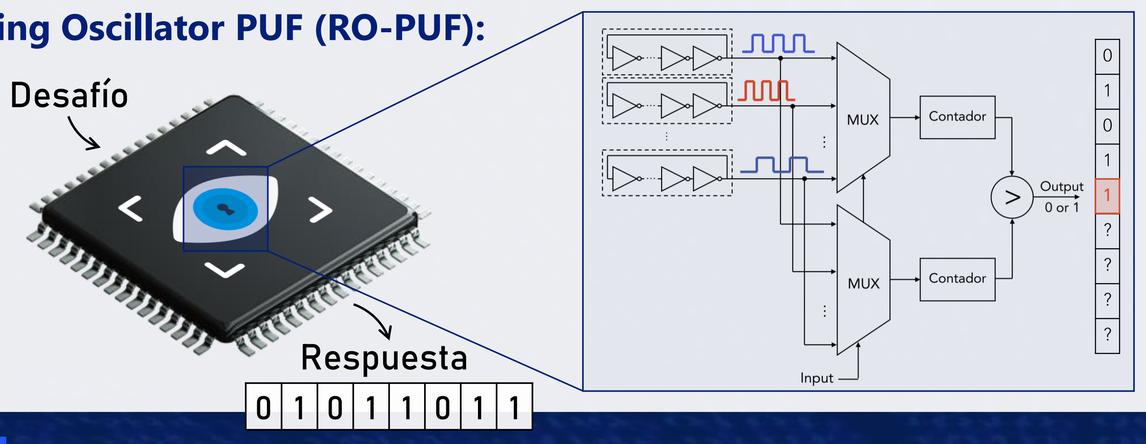
Raúl Aparicio-Téllez, Miguel Garcia-Bosque, Guillermo Díez-Señorans y Santiago Celma

Grupo de Diseño Electrónico (GDE), I3A, Universidad de Zaragoza; r.aparicio@unizar.es

1 Introducción

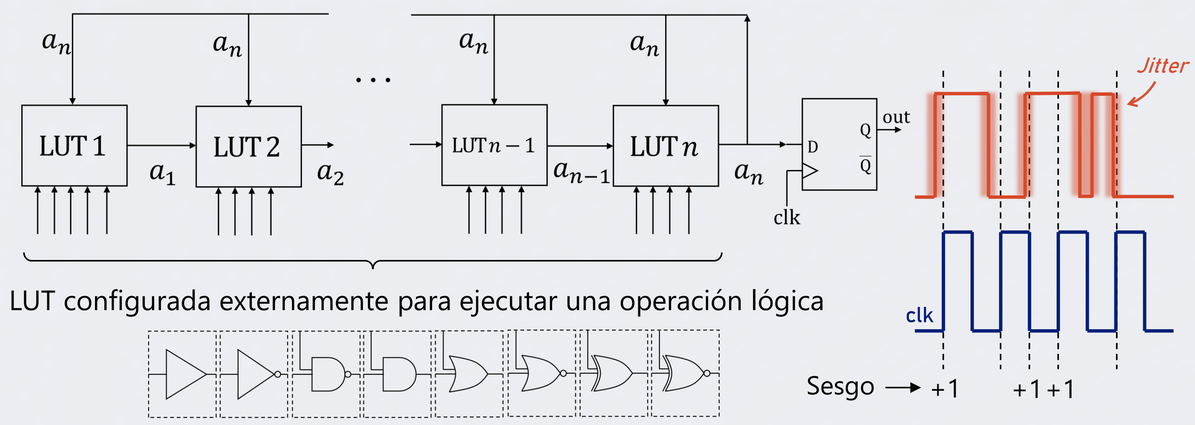
Physically Unclonable Function (PUF): genera clave única a partir de variaciones estocásticas del proceso de fabricación del dispositivo.

Ring Oscillator PUF (RO-PUF):



2 Propuesta

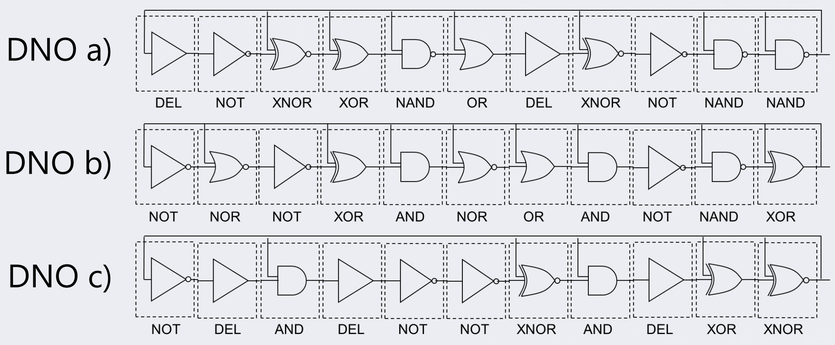
Reconfigurable Digital Nonlinear Oscillator (DNO):



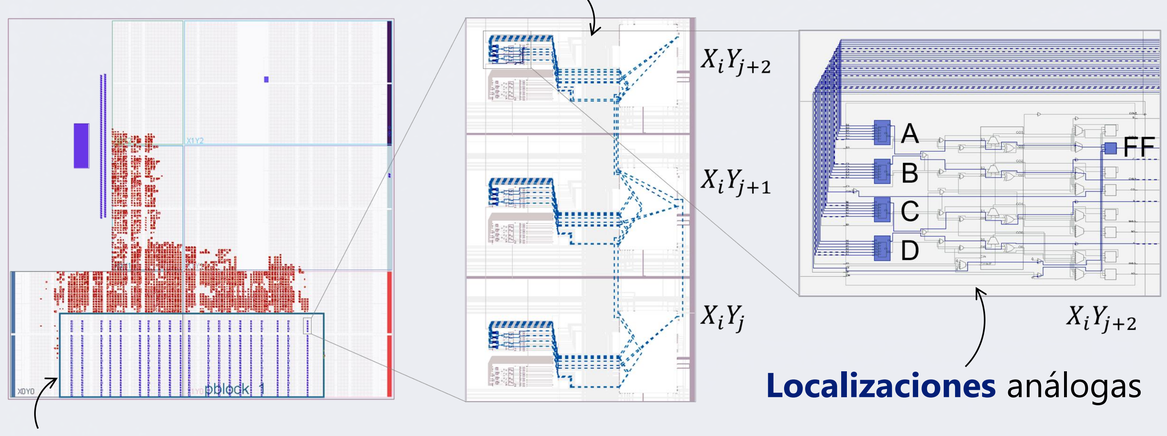
LUT configurada externamente para ejecutar una operación lógica

3 Implementación en FPGA

- Implementación de **200 DNO** de **11-LUT** en **40 FPGA Artix-7**.
- Comparación según la **topología *1-out-of-2***.
- Selección de tres **configuraciones** con buenas propiedades:



Ruteado idéntico



Localizaciones análogas

pblock: restricción de los DNO a una zona de la FPGA

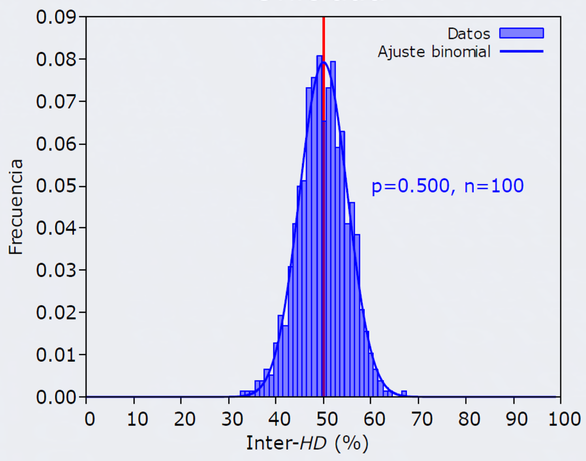
4 Análisis de las propiedades de la PUF

Propiedades

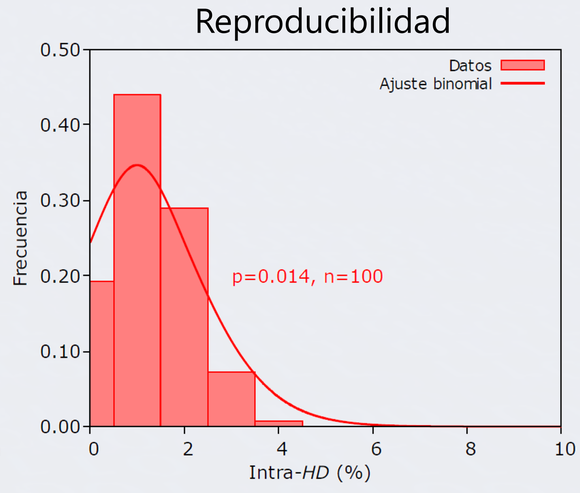
- **Unicidad:** generar respuestas distintas en dispositivos distintos. Medida con Inter-*HD* (idealmente 50%, en promedio).
- **Reproducibilidad:** generar en todo momento la misma respuesta. Medida con Intra-*HD* (idealmente 0%).
- **Identificabilidad (*EER*):** probabilidad del intento de autenticación de resultar simultáneamente en falso rechazo/aceptación.
- **Correlación espacial:** medida con la I de Moran. En una disposición aleatoria, I=0.
- **Resistencia a ataques de Machine Learning:** predicción del bit de salida de pares de DNO con una red neuronal.

Caso	<Intra-*HD*>	<Inter-*HD*>	*EER*	I de Moran	Resistencia ML
Ideal	0.00%	50.0%	0.00	0.00	✓
RO	0.63%	42.0%	10^{-11}	0.63	✗
DNO a)	1.34%	49.3%	10^{-13}	-0.05	✓
DNO b)	1.37%	48.9%	10^{-12}	-0.04	✓
DNO c)	1.47%	49.3%	10^{-12}	0.05	✓

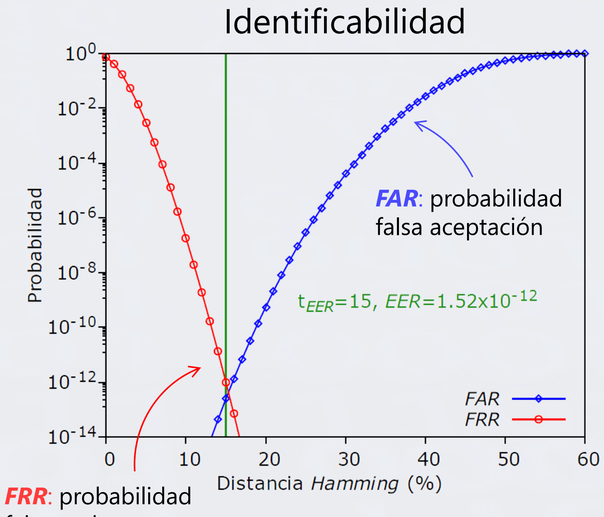
Unicidad



Reproducibilidad



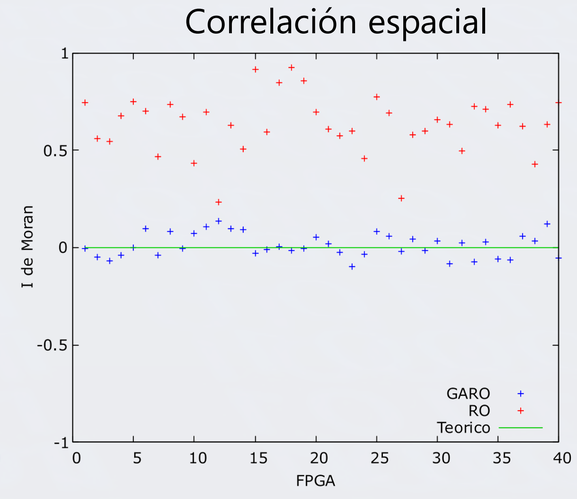
Identificabilidad



FAR: probabilidad falsa aceptación

FRR: probabilidad falso rechazo

Correlación espacial



5 Conclusiones

- Nuevos DNO combinan propiedad **aleatoriedad verdadera** debido al ***jitter*** de RO con **pseudo-aleatoriedad** de los **LFSR**.
- PUF con baja **correlación espacial**, alta **reproducibilidad, unicidad, identificabilidad** y **resistencia** a ataques de **Machine Learning**.
- Abre la puerta a la implementación de una PUF con **múltiples pares desafíos-respuestas** (PUF Fuerte).