XII JORNADA DE JÓVENES INVESTIGADORES/AS DEL I3A

Optimización de una PUF de oscilador en anillo en una FPGA

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

Grupo de Diseño Electrónico (GDE), I3A, Universidad de Zaragoza, Pedro Cerbuna 12, 50010, España, r.aparicio@unizar.es

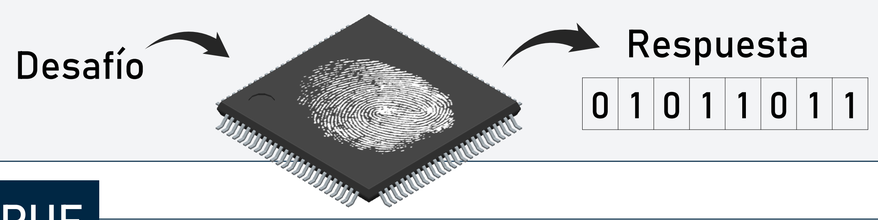
Universidad Zaragoza 1542

Instituto Universitario de Investigación en Ingeniería de Aragón Universidad Zaragoza

GDE Grupo de Diseño Electrónico

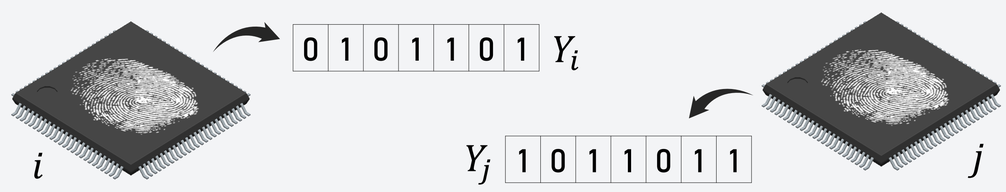
1 ¿Qué es una PUF?

Función Físicamente no-Clonable (PUF): entidad física con una funcionalidad desafío-respuesta que depende de las variaciones estocásticas inherentes al proceso de fabricación de los dispositivos.

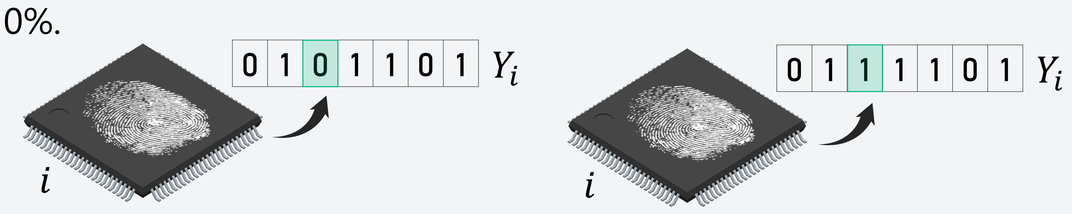


2 Métricas de calidad

Unicidad: se comparan las respuestas de dos PUF en dos dispositivos distintos. Se mide con la Inter-*HD*. Idealmente será 50%.

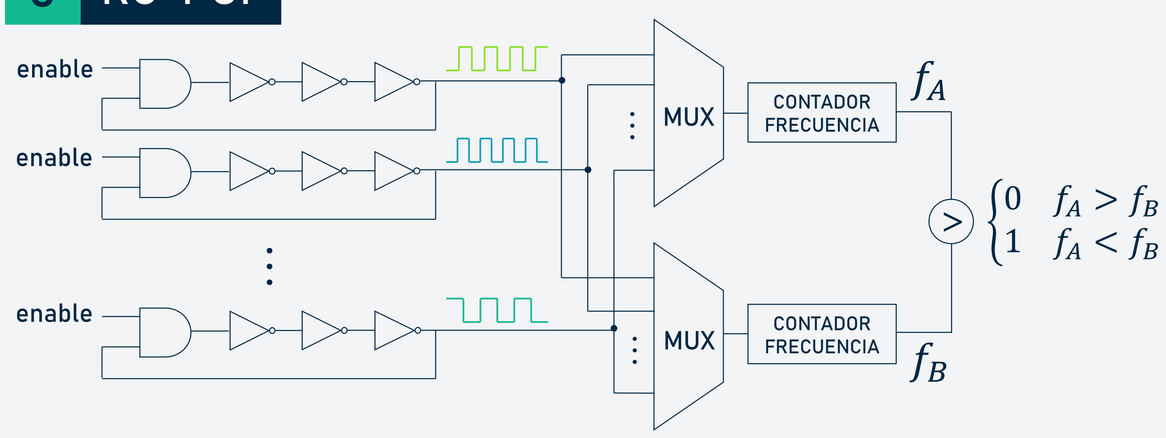


Reproducibilidad: compara la respuesta de una PUF en un mismo dispositivo en distintos instantes. Se mide con Intra-*HD*. Idealmente será 0%.



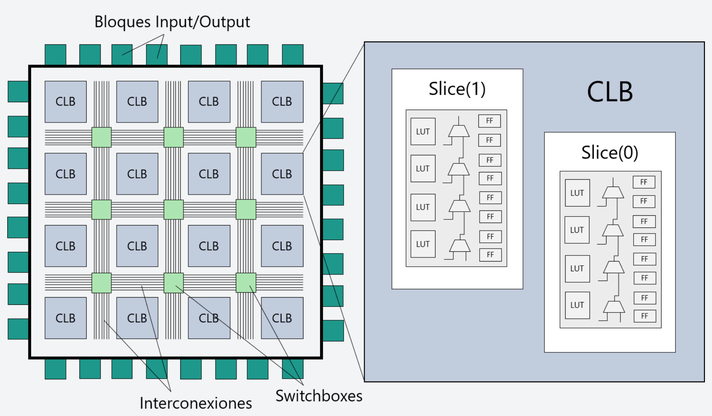
Identificabilidad (*EER*): probabilidad simultánea de que un intento de identificación resulte en falsa aceptación (*FAR*) o falso rechazo (*FRR*).

3 RO-PUF



4 Implementación en FPGA

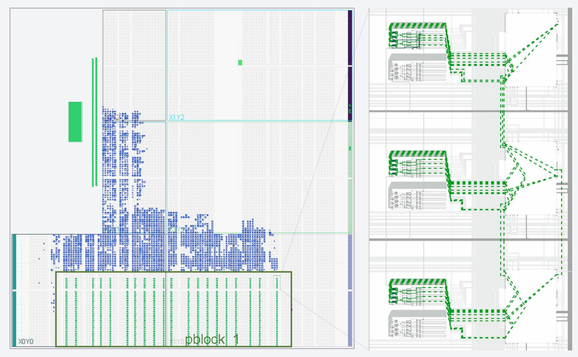
En casi todas las aplicaciones, se considera que las *slices* de la FPGA son iguales en funcionalidad, velocidad y potencia. Sin embargo, hemos observado que al implementar una **RO-PUF** en una **FPGA** algunos parámetros resultan **críticos**. Se estudian **cuatro restricciones**:



+ crítico

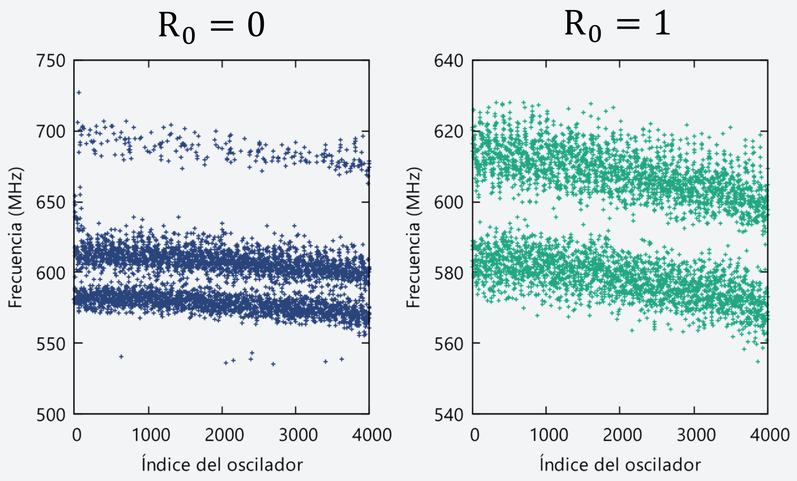
- R_0 Conexionado RO: automático (R_0=0) o idéntico (R_0=1)
- R_1 Ubicación *slice*: *Slice*(0) (R_1=0) o *Slice*(1) (R_1=1)
- R_2 Tipo *slice*: M (R_2=0) o L (R_2=1)
- R_3 Ubicación CLB: L (R_3=0) o R (R_3=1)

- crítico



5 Resultados

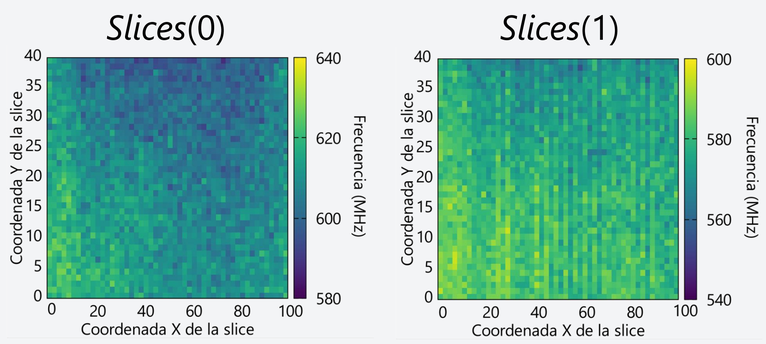
Efecto del conexionado (R_0)



- Desaparece un dominio frecuencial.
- Desaparecen efectos de borde.
- Dos dominios frecuenciales (*Slices* 0 y 1).
- Se mantiene la correlación espacial.

Efecto de la *slice* y el CLB (R_1, R_2, R_3)

R_1	R_2	R_3	$\bar{f}$(MHz)	$\widehat{\sigma_{\bar{f}}}/\bar{f}$
0	0 (M)	0 (L)	585.70 ± 0.22	0.037 %
		1 (R)	586.54 ± 0.26	0.044 %
	1 (L)	0 (L)	593.20 ± 0.25	0.043 %
		1 (R)	592.45 ± 0.23	0.039 %
1	**1 (L)**	**0 (L)**	**620.04 ± 0.22**	**0.035 %**
		1 (R)	620.03 ± 0.24	0.039 %

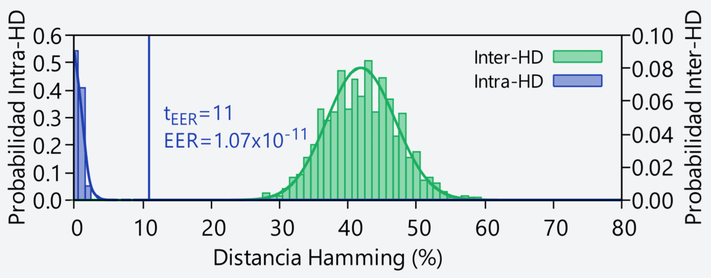


Propuesta de optimización

- Optimización (R_0=1, R_1=1, R_2=1 y R_3=0):

Métrica	RO-PUF Opt.	RO-PUF No-Opt.
<Inter-*HD*> (%)	42.0 ± 0.2	18.7 ± 0.2
<Intra-*HD*> (%)	0.66 ± 0.07	0.32 ± 0.05
EER	**$1.07 \cdot 10^{-11}$**	**$6.56 \cdot 10^{-5}$**

- La optimización mejora notablemente la identificabilidad de la PUF (↓ *EER*).



6 Conclusiones

- La **arquitectura** de la **FPGA** y el **conexionado** de los osciladores modifica su frecuencia y, por tanto, afecta a la **calidad** de la **PUF**.
- La **optimización** propuesta (R_0=1, R_1=1, R_2=1 y R_3=0) **disminuye** notablemente la **probabilidad** de errores **falso rechazo** y errores de **falsa aceptación.**