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)
Instituto de Investigación en Ingeniería de Aragón (I3A)
Universidad de Zaragoza, Mariano Esquillor s/n, 50018, Zaragoza, Spain.
Tel. +34-976762707, e-mail: r.aparicio@unizar.es

Abstract

Las Funciones Físicamente No-Clonables (PUF) basadas en osciladores de anillo (RO-PUF) son una de las implementaciones de PUF en FPGA más utilizadas actualmente. Sin embargo, la arquitectura de la FPGA afecta a la aleatoriedad de la respuesta. En este trabajo, proponemos algunas formas de optimizar una RO-PUF implementada en FPGA.

Introducción

El desarrollo del Internet de las cosas (IoT) ha dado lugar al intercambio de grandes cantidades de datos que deben ser encriptados. Esta información se almacena en memorias no volátiles (NVM) que pueden ser vulnerables a ataques físicos. Las Funciones Físicamente No-Clonables (PUF) aprovechan variaciones estocásticas inherentes al proceso de fabricación de los dispositivos para generar una secuencia binaria que identifica de forma unívoca a cada objeto, pudiéndose interpretar como la huella dactilar del dispositivo. Esta aproximación evita almacenar información secreta en NVMs, aumentando la seguridad y reduciendo el coste de los sistemas. Una de las PUFs más utilizadas debido a su simplicidad para ser implementada en FPGA es la PUF de oscilador de anillo (RO-PUF), que compara las frecuencias de los osciladores por parejas para generar el *bit* de salida. Para generar una respuesta aleatoria, estas frecuencias deben ser lo más similares posibles. Sin embargo, hemos observado que la arquitectura de la FPGA afecta a las frecuencias de los osciladores, produciendo *bits* predecibles en lugar de aleatorios. En este trabajo, proponemos algunas estrategias para reducir estos efectos y aumentar la aleatoriedad de la respuesta de la RO-PUF.

Métricas clave de una PUF

Se pueden realizar tres métricas para determinar la calidad de una RO-PUF: unicidad, reproducibilidad e identificabilidad. Estas métricas utilizan la Distancia Hamming (HD) como figura de mérito, que se define como la operación XOR entre dos secuencias de *bits* Y, Y': $HD = \sum_{i=1}^{n} Y_i \; XOR \; Y_i'$.

- **Unicidad:** compara las respuestas de diferentes dispositivos. Se mide con la Inter-*HD*. Idealmente, debería ser del 50%.
- **Reproducibilidad:** compara las respuestas del mismo dispositivo en diferentes condiciones. Se mide con la Intra-*HD*. Idealmente, será del 0%.
- **Identificabilidad:** combina las propiedades de unicidad y reproducibilidad. Mide la probabilidad de que un intento de identificación resulte en una falsa aceptación o en un falso rechazo. Se mide con el *equal error rate* (*EER*), que da la probabilidad de que el intento resulte en ambas situaciones simultáneamente.

Metodología

En este trabajo, hemos utilizado la placa PYNQ Z2, que cuenta con una FPGA Artix 7. La FPGA se divide en Bloques Lógicos Configurables (CLB). Cada CLB cuenta con dos *slices*. Cada *slice* se expresa con una coordenada X_iY_j y cuenta con cuatro LUTs de 6 entradas. En este trabajo, hemos analizado cuatro parámetros que normalmente no se consideran en la implementación de un diseño en una FPGA, pero que podrían ser decisivos para una RO-PUF:

- ***Routeado* de los RO (R_0):** al implementar el diseño, el software Vivado ejecuta un *routeado* automático que reduce el tiempo de compilación y la congestión del cableado. Esto podría ser un inconveniente ya que esperamos que todos los osciladores sean lo más similares posibles. Se utiliza la notación: R_0=0 (*routeado* automático) y R_0=1 (los ROs utilizan un *routeado* análogo).
- **Ubicación de la *slice* (R_1):** cada CLB contiene dos *slices*: Slice(0) (R_1=0) y Slice(1) (R_1=1), situadas en la parte inferior y en la parte superior del CLB respectivamente.
- **Tipo de *slice* (R_2):** hay dos tipos de *slices*: tipo L (solo para funcionalidades lógicas, R_2=1) o tipo M (también para memoria distribuida, R_2=0).
- **Localización de los CLB (R_3):** los CLBs situados en la parte derecha de las *switchboxes* de la FPGA se identifican como CLB-R (R_3=1) y los situados a la izquierda se identifican como CLB-L (R_3=0).

Resultados

En este trabajo, hemos implementado 4000 osciladores en anillo de 3-LUT en una matriz 40x100 partiendo de la *slice* $X_0\,Y_0$ (oscilador 0) a la *slice* $X_{99}\,Y_{39}$ (oscilador 4000). En primer lugar, hemos analizado el efecto del *routeado* de los osciladores en su frecuencia. Con este propósito, hemos medido las frecuencias de los osciladores utilizando el *routeado* automático realizado por Vivado (R_0=0) y utilizando un *routeado* manual realizado por el diseñador (R_0=1). Como se puede ver en la Figura 1, al fijar el *routeado* de los osciladores, uno de los dominios frecuenciales desaparece. Además, algunos efectos relacionados con separaciones físicas y efectos de borde también desaparecen. En conclusión, al fijar el *routeado*, los osciladores tienen frecuencias claramente similares. Sin embargo, todavía se observan dos dominios frecuenciales. Por este motivo, hemos fijado el *routeado* de los osciladores para estudiar cuáles son las localizaciones óptimas para implementar los ROs. Como se puede ver en la Tabla 1, los osciladores ubicados en Slices(0) tienen frecuencias más bajas en comparación con los de Slices(1). Además, también hay una pequeña diferencia entre las frecuencias de los osciladores implementados en *slices* de tipo M y tipo L. Finalmente, la diferencia entre CLB-L y CLB-R es insignificante. Además, la menor dispersión ($\widehat{\sigma_{\bar{f}}}/\bar{f}$) se obtiene para los osciladores situados en Slices(1)

Tabla 1. Frecuencias de los osciladores según la restricción aplicada. Esta FPGA no cuenta con Slices(1) de tipo M.

R_1	R_2	R_3	$\bar{f}$(MHz)	$\widehat{\sigma_{\bar{f}}}$	$\widehat{\sigma_{\bar{f}}}/\bar{f}$
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 %

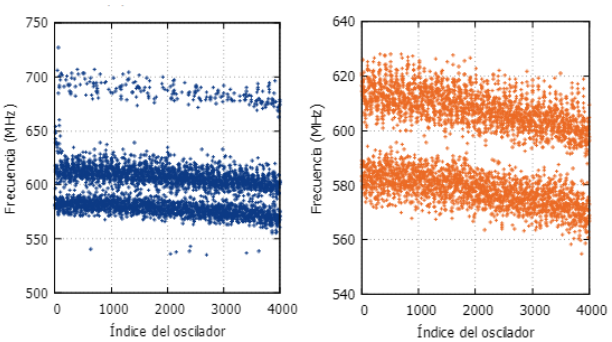

Figura 1. Frecuencias de los osciladores obtenidas fijando el *routeado* (naranja) y sin fijar el *routeado* (azul).

de tipo L implementadas en CLBs L (R_1=1, R_2=1, R_3=0). Estas serán las mejores localizaciones para implementar los osciladores.

Finalmente, hemos implementado una RO-PUF con 200 osciladores de 11-LUT fijando su *routeado* y localización (R_0=1, R_1=1, R_2=1), y hemos comparado sus propiedades con las de una RO-PUF no optimizada. Como se puede ver en la Tabla 3, nuestra optimización contribuye a un aumento considerable en la unicidad (Inter-*HD*) de la RO-PUF mientras que no reduce casi la reproducibilidad (Intra-*HD*). También mejora la identificabilidad (menor *EER*) de la PUF en seis órdenes de magnitud, lo que hace que la RO-PUF optimizada sea adecuada para propósitos de identificación y autenticación de dispositivos.

Tabla 2. Comparación entre las propiedades de la RO-PUF optimizada y la RO-PUF no optimizada.

Métrica	RO-PUF optimizada	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	$1.07\cdot10^{-11}$	$6.56\cdot10^{-5}$

Conclusiones

En este trabajo hemos mostrado que la arquitectura de la FPGA puede afectar a la frecuencia de los osciladores y, por lo tanto, a la calidad de la PUF. Con este propósito, hemos analizado qué parámetros se deben considerar para construir una RO-PUF en una FPGA y hemos propuesto algunas estrategias para aumentar la identificabilidad de la RO-PUF.

Agradecimientos

Este trabajo ha sido financiado por la Diputación General de Aragón (LMP197_21).

REFERENCIAS

[1]. APARICIO-TÉLLEZ, R., GARCIA-BOSQUE, M., DÍEZ-SEÑORANS, G., and CELMA, S. Oscillator Selection Strategies to Optimize a Physically Unclonable Function for IoT Systems Security. *Sensors*, 23(9), 2023.

[2]. MAES R. Physically Unclonable Functions: Constructions, Properties and Applications. *Springer Berlin Heidelberg, Berlin, Heidelberg.* 2013.

[3]. BÖHM C., and HOFER M. Physical Unclonable Functinos in Theory and Practice. *Springer, NY,* 2013.

[4]. GARCIA-BOSQUE M., APARICIO, R., DÍEZ-SEÑORANS, G., SÁNCHEZ-AZQUETA C., and CELMA, S. An Analysis of the Behaviour of a PUF based on Ring Oscillators Depending on their Locations. *17th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME).*