# Técnica novedosa para obtener respuestas multi-bit en funciones físicamente no-clonables (PUF)

Jorge Fernández-Aragón, Guillermo Díez-Señorans, Miguel Garcia-Bosque, 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: jorgefa@unizar.es

## Resumen

Las funciones físicamente no-clonables (PUF) se han convertido en una de las primitivas criptográficas más importantes y en este artículo se ha desarrollado una nueva técnica, denominada medida compensada de segundo orden, que consigue obtener respuestas multi-bit mejorando así el rendimiento de la PUF en términos de identificabilidad y entropía por área.

## Introducción

La conexión de un gran número de dispositivos y usuarios conduce a un intercambio masivo de datos sensibles y confidenciales. Esto lleva a la necesidad de generar sistemas tecnológicos presentes en aplicaciones de autenticidad y generación de claves de seguridad. Hoy en día las funciones físicamente no-clonables (PUFs) son las primitivas criptográficas más demandadas [1] debido a su bajo coste de fabricación y su sencillez para ser implementadas. Una de las PUFs más empleadas [2] son las PUFs de oscilador de anillo (RO-PUFs). Estas se basan en medir las variaciones estocásticas inherentes a su fabricación para generar una respuesta específica del dispositivo. Mediante la comparación de las frecuencias de parejas de osciladores de anillo se obtiene la respuesta de la PUF. Este método de comparación se denomina medida compensada y, a pesar de ser fiable a la hora de generar la respuesta, está limitado a obtener un único bit en cada comparación, por lo que el área del dispositivo debe ser lo suficientemente grande para obtener respuestas robustas y seguras. A raíz de esto, proponemos la medida compensada de segundo orden que permite obtener varios bits de una única comparación permitiendo así generar respuestas multi-bit que mejoren el rendimiento de la PUF. Esta técnica fue introducida en [3], donde se probó la posibilidad de obtener varios bits de una única comparación y en este artículo se demuestra su rendimiento, así como la posibilidad de obtener respuestas multi-bit.

## Medida compensada de 2º orden

La nueva técnica propuesta se basa en la medida compensada convencional donde se comparan parejas de osciladores de anillo de forma que, si la frecuencia del primer oscilador es mayor que la del segundo, se le asigna un '1' lógico; y en el caso de que la frecuencia del primer oscilador sea menor, se le asigna un '0'. De esta forma al signo (mayor o menor) de la comparación se le asocia un bit (1 o 0) denominándose el bit de signo. Para obtener más bits de la comparación de osciladores se ha propuesto emplear el valor absoluto de la resta de frecuencias en formato binario. De esta forma la diferencia entre las frecuencias está representada por un número de 32 bits, donde el primer bit es el bit de signo y el resto corresponde al valor absoluto de la resta. Con esta nueva técnica obtendremos respuestas que dependerán del bit que seleccionemos dentro de la cadena de 32 bits. Por un lado, si seleccionamos el bit de signo, obtendremos la misma respuesta que utilizando la medida compensada convencional; esto nos servirá para comparar la calidad de las respuestas del resto de bits. Por otro lado, si seleccionamos cualquiera de los otros 31 bits para generar la respuesta, obtendremos respuestas que pueden o no ser útiles como PUF. En los casos en los que obtengamos nuevos bits que generen respuestas válidas, yuxtapondremos las cadenas generadas por el bit de signo y uno o varios de estos nuevos bits, generando así respuestas multi-bit. Para diseñar la RO-PUF se ha implementado una matriz de osciladores de anillo en una FPGA, concretamente en una placa PYNQ-Z2 que incluye una FPGA *Artix-7* integrada en 28 nm. Además, para comprobar el rendimiento de la técnica propuesta, se han estudiado las propiedades y parámetros característicos que definen una PUF [4]. Entre ellos destaca la identificabilidad, cuya figura de mérito es la curva característica operativa del receptor (ROC) que muestra el compromiso entre seguridad y robustez de las respuestas a través de la tasa de error (EER).

# Resultados

De los 32 bits del vector que se obtiene en cada comparación, se ha demostrado que generan una respuesta válida como PUF cuatro de ellos: el bit de signo y tres nuevos bits situados en las posiciones 16, 17 y 18 del vector. El resto de los bits tienen una tasa de error muy alta que deriva en una identificabilidad muy baja y por tanto no pueden considerarse válidos. La figura 1 muestra que el bit de signo (utilizado en la medida compensada convencional) posee el menor EER con solo 1 error cada $10^{10}$ evaluaciones. También vemos que para el bit 16 y 17 obtenemos resultados similares al bit de signo, con 1 error cada $10^{8}$ evaluaciones y en el caso del bit 18 se obtiene 1 error cada $10^{5}$ evaluaciones. Estos buenos resultados indican que es posible generar respuestas con bits diferentes al del signo y abren la posibilidad de generar respuestas multi-bit. Para realizar estas respuestas se yuxtapone la obtenida por el bit de signo con cada uno de los nuevos bits por separado y también en conjunto. Los resultados se muestran en la figura 2 donde vemos el gran aumento en la identificabilidad cuando generamos una respuesta con el bit de signo y el bit 16 o 17 consiguiendo mejorar la tasa de error en un 70% comparado con emplear únicamente el bit de signo. Además, si empleamos el bit de signo junto al bit 16 y 17, la mejora es del 90% en comparación al método habitual. Cabe destacar que si empleamos los cuatro bits para generar la respuesta la identificabilidad es menor que empleando tres y probablemente se deba a la correlación entre bits adyacentes.

# Conclusiones

El artículo muestra la posibilidad de obtener nuevos bits válidos para generar la respuesta de una PUF con una única comparación y además permiten generar respuestas multi-bit que mejoran la identificabilidad en varios órdenes de magnitud. Los resultados se pueden ver de dos maneras complementarias: con los mismos recursos mejoramos la identificabilidad de la PUF o podemos reducir el área de la PUF sin perder identificabilidad. Cabe añadir que se ha probado la fiabilidad de las respuestas frente a variaciones de temperatura y voltaje interno de la FPGA obteniendo resultados robustos en el uso de esta nueva técnica.

## AGRADECIMIENTOS

Este trabajo ha sido cofinanciado por Ministerio de Ciencia e Innovación-Agencia Estatal de Investigación (PID2020-114110RA-100) y Diputación General de Aragón (LMP197_21).

## REFERENCIAS

[1]. SUH, G. E. and DEVADAS, S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. *44th ACM/IEE Design Automation Conference*. 2007, pp. 37-39.

[2]. MAES, R. Physically Unclonable Functions: Concept and Constructions. 2012, pp. 11-48.

[3]. FERNANDEZ-ARAGON, J., *et al.* Oscilador de anillo PUF en FPGA: diseño y caracterización mediante el uso de la medición compensada de segundo orden. *XI Jornada. Jóvenes Investigadores del I3A, vol. 10*. 2022.

[4]. GARCIA-BOSQUE, M., *et al*. Introduction to Physically Unclonable Functions: Properties and Applications. *2020 European Conference on Circuit Theory and Design (EECTD)*. 2020, pp. 1-4.

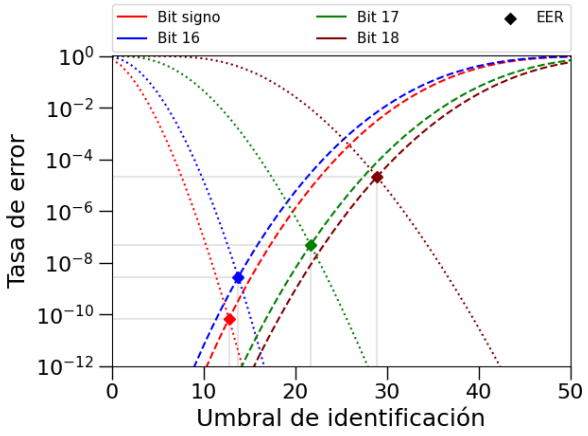


**Figura 1.** Representación de la tasa de error frente al umbral de identificación para la respuesta generada individualmente por el bit de signo y los tres nuevos bits, donde una tasa de error menor implica una mayor identificabilidad. El punto de intersección de las curvas de las tasas de error (EER) marca el mejor compromiso entre robustez y seguridad.

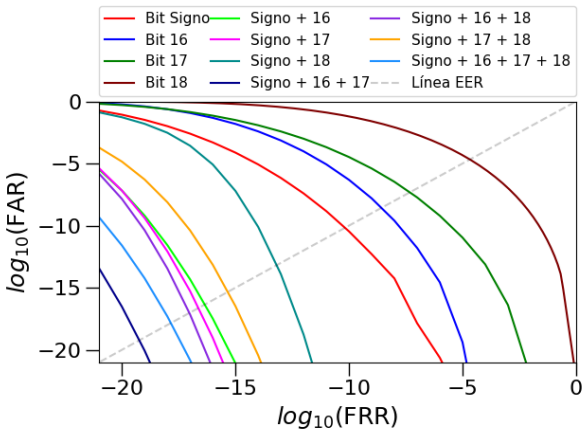


**Figura 2.** Curva característica operativa del receptor (ROC) que representa la tasa de falso rechazo (FRR) frente a la tasa de aceptación (FAR) para las respuestas generadas por el bit signo y los nuevos bits de forma individual y cada una de las respuestas multi-bit. Hay una gran mejora en la identificabilidad, obteniendo el mejor resultado combinando bit de signo, bit 16 y bit 17.