Extracción de entropía en PUFs de medida compensada

G. Díez-Señorans[1], M. Garcia-Bosque[1,2], C. Sánchez Azqueta[1], S. Celma[1]

[1]Grupo de Diseño Electrónico (GDE) - Instituto de Investigación en Ingeniería de Aragón (I3A)
[2]Centro Universitario de la Defensa de Zaragoza
e-mail: gds@unizar.es

Resumen

En este trabajo proponemos algunas técnicas novedosas para maximizar la entropía extraída de una matriz de osciladores de anillo, utilizada como función física no-clonable (PUF) en FPGA para la identificación segura de dispositivos y generación de claves con interés criptográfico. Todos los resultados han sido obtenidos mediante la evaluación experimental en una FPGA Zynq 7000.

Introducción

Las funciones físicas no-clonables son primitivas criptográficas que obtienen sus propiedades de seguridad de la *capa física* sobre la cual están construidas. Estos objetos tienen las propiedades de ser *identificables* y *físicamente no-clonables* [1]: cuando una instancia PUF se expone a un cierto estímulo (i.e., se evalúa la PUF), esta proporciona una respuesta que es exclusiva de dicha instancia y es reproducible en el tiempo; además, dicha respuesta es extraída a partir de las variaciones estocásticas introducidas en cada instancia durante el proceso de fabricación, por lo que resulta imposible de replicar a nivel de hardware. Una de las alternativas PUF más estudiadas, por su facilidad de implementación tanto en ASIC como en FPGA, es la PUF de osciladores de anillo (RO-PUF), que utiliza como identificador los retardos relativos de una serie de osciladores de anillo idénticos por diseño [2]. De este modo, para extraer una respuesta binaria, se seleccionan algunas parejas de osciladores y se construye la respuesta escribiendo *0* o *1* en función de qué oscilador de la pareja tiene una mayor frecuencia característica; esta técnica se conoce como *medida compensada*, y además de proporcionar un mecanismo sencillo de digitalización, también aumenta la robustez de las respuestas de un chip inmerso en un entorno variable. La elección de qué parejas comparar (*topología* de RO-PUF) para producir una palabra binaria con una correlación mínima entre bits (*extracción de entropía*) es un problema no trivial de un evidente interés criptográfico; en este trabajo proponemos algunas topologías novedosas para maximizar el número de bits independientes manteniendo un consumo de recursos hardware moderado, y hacemos una comparación con las topologías más utilizadas en la práctica del diseño de RO-PUF.

Topologías propuestas

Dado un arreglo de N osciladores de anillo, las topologías que aparecen con más frecuencia en el diseño de RO-PUFs son [3]:

(i) 1-out-of-2: en este esquema se comparan todos los osciladores sin repetición: el primero con el segundo, el tercero con el cuarto, etc., produciendo $\boldsymbol{N/2}$ bits de respuesta.

(ii) N-1: aquí se comparan todos los osciladores repitiendo un oscilador en cada comparación: primero con el segundo, segundo con el tercero, etc., produciendo $\boldsymbol{N-1}$ bits.

(iii) All-pairs: se comparan todos los osciladores entre sí, dando lugar a respuestas de $\frac{\boldsymbol{N(N-1)}}{\boldsymbol{2}}$ bits.

Por otro lado, en este trabajo proponemos las siguientes topologías:

(i) 3-modular: el arreglo de osciladores se divide en conjuntos (disjuntos) de tres osciladores, y cada uno de estos se evalúa siguiendo una estrategia *All-pairs*, dando lugar a $\boldsymbol{N}$ bits.

(ii) 4-modular: se opera como en el caso anterior, pero dividiendo el conjunto de osciladores en grupos de cuatro elementos, lo que da lugar a palabras de $\boldsymbol{3/2N}$ bits.

Montaje experimental

Para evaluar la entropía asociada a la distribución de probabilidad de cada topología es necesaria una gran cantidad de instancias RO-PUF, lo cual resulta impracticable; en su lugar, hemos implementado un gran número de osciladores de anillo (782 elementos en una matriz de 34×23) en una FPGA Zynq 7000, que utilizaremos como reserva (Fig. 1);

para evaluar una topología concreta utilizando un arreglo de N osciladores seleccionamos aleatoriamente N elementos de la reserva y los comparamos de acuerdo con el dictado de la topología correspondiente, dando lugar a un valor numérico (en formato binario). Repetimos este proceso hasta que el histograma $\{p_i\}$ de la distribución de valores permanece estacionario, y calculamos después la entropía asociada como $S = -\sum p_i \log_2(p_i)$.

Resultados

En la Fig. 1 hemos representado: (a) la entropía por oscilador (S/N) y (b) la entropía por bit (S/bit) respectivamente. La primera de estas curvas puede relacionarse con una medida de la eficiencia en términos de recursos hardware (potencia y silicio) que cabría esperar de cada topología, mientras que la segunda mide la resistencia al criptoanálisis exhibido por las mismas. En la Fig. 2 se puede apreciar la existencia de una relación inversa entre el uso eficiente de recursos y el potencial de seguridad de la topología. A este respecto, las topologías que hemos propuesto en este trabajo (especialmente la alternativa *4-modular*) ocupan un lugar central en ambos gráficos (Fig. 2.a y 2.b), lo cual la convierte en una candidata prometedora para el diseño de RO-PUFs con un buen compromiso entre ambas propiedades.

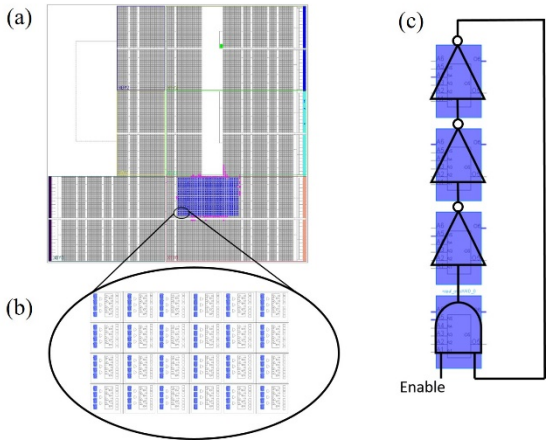

Figura 1. (a) Implementación del sistema de medida en la FPGA, (b) detalle de la matriz de osciladores de anillo, (c) esquema de un oscilador de anillo de tres inversores en FPGA.

Conclusiones

En este trabajo hemos diseñado un procedimiento para evaluar la entropía extraíble de una matriz de osciladores de anillo en FPGA, probando su viabilidad como primitiva para construir aplicaciones de interés criptográfico. Además, se han propuesto y probado de utilidad algunas estrategias de diseño alternativas al estado del arte.

AGRADECIMIENTOS

MINECO-FEDER (TEC2017-85867-R) y Beca Predoctoral DGA a G. Díez-Señorans.

REFERENCIAS

[1]. R. Maes, "Physically unclonable functions: Constructions, properties and applications", PhD thesis, 2012.

[2]. T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A puf taxonomy," Applied Physics Reviews, vol. 6, no. 1, p. 011303, 2019.

[3]. M. Garcia-Bosque, G. Díez-Señorans, C. Sánchez-Azqueta, and S. Celma, "Introduction to physically unclonable fuctions: Properties and applications," ECCTD. IEEE, 2020.

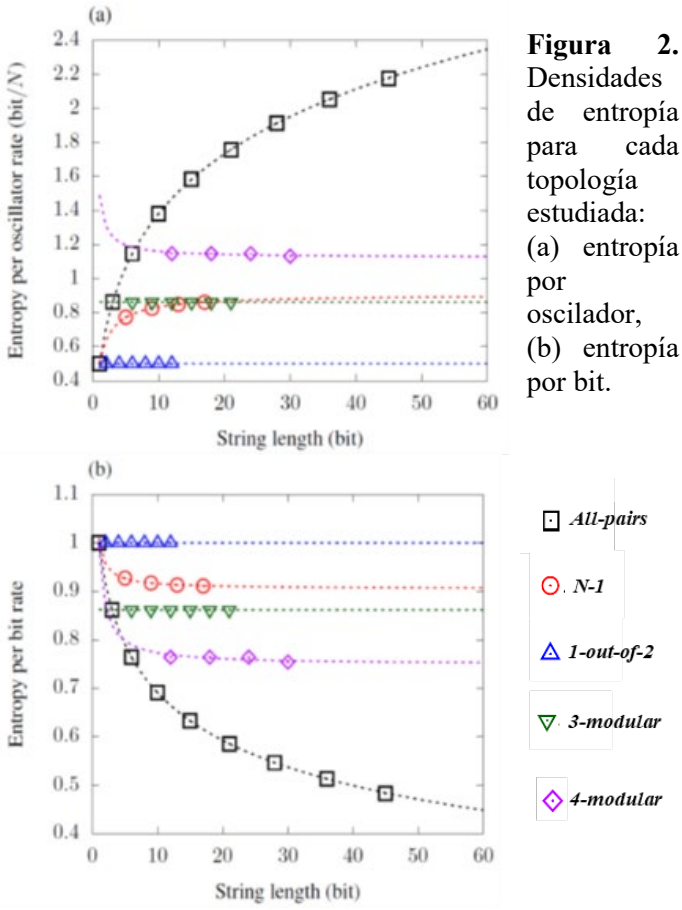

Figura 2. Densidades de entropía para cada topología estudiada: (a) entropía por oscilador, (b) entropía por bit.