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, Santiago Celma

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

Resumen

En este trabajo se propone e implementa en FPGA una nueva PUF basada en osciladores no-lineales reconfigurables. Esta propuesta soluciona algunos problemas de la PUF de oscilador en anillo convencional, al mismo tiempo que presenta un excelente rendimiento en términos de unicidad y reproducibilidad, resultando óptima para la autenticación segura de dispositivos.

Introducción

A medida que el Internet de las Cosas (IoT) sigue creciendo, la necesidad de desarrollar nuevas medidas de seguridad que protejan los sistemas de accesos no autorizados resulta crítico. Uno de los elementos más débiles de estos sistemas son los *edge devices*, que operan en entornos no controlados, cuentan con recursos limitados y pueden ser vulnerables a diversos ataques [1]. En este contexto, las Funciones Físicamente No Clonables (PUF) son una solución óptima para proteger estos dispositivos. Una PUF es un elemento de circuito que asigna a un determinado reto c una única respuesta $r = F(c)$ [1] utilizando para ello variaciones estocásticas propias del proceso de fabricación de los dispositivos. Las dos principales aplicaciones de una PUF son la generación de claves y autenticación de dispositivos.

Una de las arquitecturas PUF más utilizadas es la PUF de Oscilador en Anillo (RO-PUF), en la que se comparan las frecuencias de N osciladores idénticos por parejas para obtener una respuesta binaria (Figura 1). Seleccionando distintas parejas de osciladores, se obtiene una respuesta de n bits que actúa como identificador del dispositivo. Sin embargo, esta arquitectura ha demostrado ser vulnerable frente a diversos ataques de *Machine Learning* [2], en parte debido a la existencia de una correlación entre las frecuencias de los osciladores y su localización espacial en el dispositivo [3].

Propuesta

En este trabajo, se propone una nueva arquitectura de PUF basada en osciladores digitales no-lineales (DNO). Este nuevo tipo de oscilador se ha construido uniendo un cierto número M de operaciones lógicas de hasta dos entradas en cascada, siendo una de las entradas la salida de la operación anterior y la otra entrada la señal de retroalimentación (Figura 2). Algunas de las combinaciones darán lugar a una salida estable mientras que otras darán lugar a una salida oscilante. Aunque la señal de salida de este oscilador es impredecible, se ha observado que existe un cierto sesgo o *bias* en el número de unos de la misma. De este modo, para construir la PUF, en lugar de comparar frecuencias se comparan los *bias*. Esta propuesta pretende definir nuevos osciladores que combinen las propiedades de aleatoriedad verdadera debido al *jitter* de los RO con la pseudo-aleatoriedad de los *Linear Feedback Shift Register* (LFSR).

Implementación

Para estudiar el rendimiento de una PUF construida a partir de estos osciladores, se han implementado 200 osciladores de longitud M=11 en 20 FPGA Artix-7. Cada operación lógica se ha implementado en una única LUT de 6 entradas. Cada LUT se ha inicializado de tal forma que dos líneas se puedan utilizar como las entradas de la operación lógica, mientras que las otras cuatro se puedan utilizar para seleccionar la operación lógica (Figura 2). Ya que las LUT se configuran externamente, una vez generado el *bitstream* con el diseño de la PUF, no es necesario volver a generar uno nuevo si se desea utilizar un oscilador con una configuración de operaciones lógicas diferente. Además, para que todos los osciladores sean idénticos, se han seleccionado las localizaciones de las LUT cuidadosamente, se ha fijado el *routeado* y se ha limitado la localización de los osciladores a una región de la FPGA, con el fin de evitar el posible acoplamiento de las señales de los osciladores con otros elementos del circuito.

Resultados

Para que una PUF se pueda utilizar para la autenticación de dispositivos, ésta debe proporcionar en todo momento la misma respuesta ante el mismo desafío (reproducibilidad) al mismo tiempo que la repuesta debe ser distinta a la que proporcionan el resto de dispositivos (unicidad). La reproducibilidad se mide con la Distancia Hamming (*HD*) intra-chip e idealmente será 0%. La unicidad se mide con la *HD* inter-chip e idealmente será en promedio 50% [4].

Se ha observado que ciertas combinaciones de puertas lógicas presentan mejores propiedades para ser utilizadas como PUF. En base a esto, se han definido tres DNO (Figura 3). En la Tabla 1 se muestran la unicidad y reproducibilidad de varias PUF construidas a partir de estos tres osciladores. Además, para determinar su rendimiento en un sistema de autenticación real, se ha obtenido el *Equal Error Rate* (*EER*) que mide la probabilidad de que un intento de autenticación resulte en un falso rechazo o falsa aceptación [4]. Asimismo, se muestran las métricas de calidad de una RO-PUF convencional implementada en las mismas localizaciones de la FPGA. Tal y como se observa, las nuevas propuestas de osciladores presentan una unicidad casi perfecta, mejorando considerablemente respecto de la RO-PUF convencional, al mismo tiempo que mantiene una alta reproducibilidad y mejoran la identificabilidad en uno o dos órdenes de magnitud (Figura 4). Además, se ha obtenido el índice I de Moran, que mide la correlación espacial de los osciladores en la FPGA. Idealmente $I = 0$. Tal y como se observa en la Tabla 1, la nueva propuesta de osciladores presenta una nula correlación espacial ($I \simeq 0$) a diferencia de la RO-PUF convencional ($I = 0.63$). Finalmente, se han llevado a cabo varios ataques de *Machine Learning* a las PUF propuestas, demostrando que los bits de salida de la respuesta de la PUF propuesta son impredecibles, al contrario que la RO-PUF.

Conclusiones

En este trabajo se proponen varias PUF construidas a partir de nuevos osciladores basados en operaciones lógicas de hasta dos entradas, demostrando que mejora el rendimiento de una RO-PUF convencional. Esta propuesta abre la puerta a la síntesis de una PUF con múltiples desafíos y respuestas utilizando como reto las líneas de configuración de los osciladores.

Agradecimientos

Este trabajo ha sido parcialmente financiado por una beca de la Diputación General de Aragón (DGA) de Raúl Aparicio-Téllez.

REFERENCIAS

[1]. GEBALI, Fayez; MAMUN, Mohammad. Review of Physically Unclonable Functions (PUFs): Structures, Models, and Algorithms. Frontiers in Sensors, 2022, vol. 2, p. 751748.

[2]. NOZAKI, Yusuke; YOSHIKAWA, Masaya. Security evaluation of ring oscillator PUF against genetic algorithm based modeling attack. En Innovative Mobile and Internet Services in Ubiquitous Computing: Proceedings of the 13th IMIS. Springer International Publishing, 2020. p. 338-347.

[3]. APARICIO-TÉLLEZ, Raúl, et al. Oscillator Selection Strategies to Optimize a Physically Unclonable Function for IoT Systems Security. Sensors, 2023, vol. 23, no 9, p. 4410.

[4]. SUH, G. Edward; DEVADAS, Srinivas. Physical unclonable functions for device authentication and secret key generation. En Proceedings of the 44th annual design automation conference. 2007. p. 9-14.

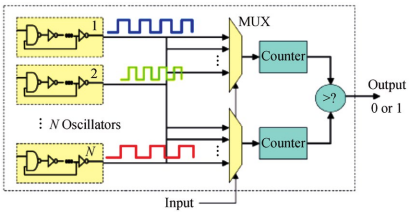

Figura 1. Arquitectura RO-PUF [4].

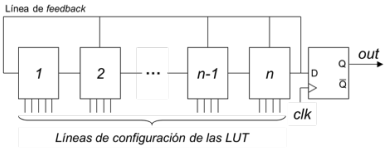

Figura 2. Propuesta de DNO.

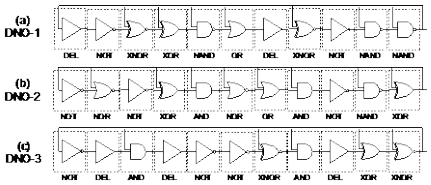

Figura 3. DNO seleccionados para construir las PUF propuestas.

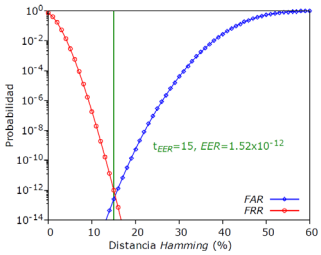

Figura 4. Identificabilidad del DNO-3.

Tabla 1. Intra-*HD* promedio (μ^{intra}), inter-*HD* promedio (μ^{inter}), *EER*, *I* de Moran y resistencia frente a ataques de Machine Learning.

Oscilador	μ^{intra}	μ^{inter}	*EER*	Moran's *I*	ML Resist.
Ideal	0.00%	50.00%	0.00	0.00	☑
RO	0.63%	42.00%	10^{-11}	0.63	☒
DNO-1	1.34%	49.31%	10^{-13}	-0.05	☑
DNO-2	1.37%	48.86%	10^{-12}	-0.04	☑
DNO-3	1.47%	49.31%	10^{-12}	0.05	☑