Implementación de arquitectura ROPUF en FPGA para identificación segura de dispositivos

G. Díez-Señorans, M. Garcia-Bosque, C. Sánchez Azqueta, S. Celma

Afiliación: 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: gds@unizar.es

Resumen

En este trabajo se propone la implementación de una arquitectura de funciones físicas no clonables (PUF) de osciladores de anillo en FPGA, y se proporciona un ejemplo de uso en la identificación de dos FPGA Zynq 7000.

Introducción

El incremento continuo en la capacidad de almacenar, procesar y transmitir información digital está transformando de un modo radical nuestro entorno en un ecosistema de información. El acceso masivo de dispositivos cotidianos a la red (*internet de las cosas* o IoT) tiene importantes aplicaciones potenciales en ámbitos tan diversos como la logística, la industria o la sanidad. Sin embargo, la naturaleza distribuida de esta tecnología y las severas restricciones en silicio y potencia introducen un nuevo paradigma de vulnerabilidad, en el que la capa física emerge como el eslabón más débil de unos sistemas donde la criptografía clásica resulta excesivamente cara para ser práctica. En este contexto surge una innovadora estrategia de seguridad basada en el uso de *Funciones Físicas no Clonables* (PUF), capaces de explotar las variaciones estocásticas del proceso de fabricación microelectrónica de dispositivos y circuitos para producir secuencias binarias con interés criptográfico: identificación unívoca de dispositivos idénticos en diseño y generación de claves [1].

En este estudio se ha diseñado una topología PUF basada en osciladores de anillo (ROPUF) y se ha demostrado su utilidad en la identificación de dos FPGAs Zynq 7000.

Topología ROPUF

Un oscilador de anillo es una sucesión impar de inversores realimentada, de tal modo que se genera un sistema astable alternando constantemente entre los valores “0” y “1” lógicos. Esta estructura puede utilizarse en la construcción de un circuito PUF (fig. 1), disponiendo una serie de osciladores idénticos en diseño, cuyas frecuencias de oscilación se espera que difieran ligeramente debido a variaciones aleatorias introducidas en el proceso de fabricación del circuito. De este modo puede obtenerse una palabra binaria única para cada circuito comparando parejas de osciladores entre sí, incluso si estos circuitos han sido producidos en serie a partir de un mismo diseño [4].

A pesar de que los osciladores deben ser genuinamente idénticos en la implementación, esta topología PUF resulta particularmente robusta a asimetrías en el resto de la circuitería: cualquier variación sistemática introducida por diseño más allá de los osciladores tendrá un impacto arbitrariamente pequeño frente a las variaciones *entre* osciladores, siempre que se mida durante períodos de tiempo suficientemente largos [4]. Esta circunstancia hace de ROPUF una arquitectura idónea para el diseño *semi-custom* en FPGA

Metodología propuesta

El diseño ROPUF propuesto ha sido implementado en dos FPGA Zynq 7000 CMOS de 28 nm (idéntico modelo); consta de una serie de 33 osciladores de anillo de cinco inversores cada uno, cuyas frecuencias son medidas y comparadas sucesivamente (osciladores *i-ésimo* vs. *i+1-ésimo*) para obtener una palabra de 32 bits, la cual identifica unívocamente a cada FPGA.

Para controlar la identidad de cada oscilador se han programado las placas a nivel de LUT (fig. 2) en lenguaje Verilog, utilizando el software Vivado; cada bit producido es recogido por un microcontrolador Arduino utilizado como interfaz. La comparación entre osciladores sucesivos se realiza mediante un juego de dos registros contadores *a* y *b*, de tal modo que con cada oscilación el contador correspondiente aumenta en una unidad. Una vez el primer contador *a* llega a *N* unidades, el proceso se detiene y se devuelve “0” si

$b < N$, y “1” en otro caso; en esta implementación se ha utilizado un valor elevado de repeticiones N = 10^7, lo cual garantiza la reproducibilidad de la clave *inter-chip*. En la tabla 1 se muestran las claves hexadecimales obtenidas para cada placa.

Conclusiones

Este trabajo describe una estrategia de diseño y aplicación de una PUF con prometedoras propiedades en seguridad a nivel de hardware; se ha demostrado cómo una estrategia de diseño *semi-custom* en FPGA controlada a bajo nivel (LUTs) puede resultar adecuada para la síntesis e implementación de estructuras PUF, así como la simplicidad y robustez de una arquitectura en particular basada en osciladores de anillo (ROPUF).

Tabla 1. Comparativa de las claves obtenidas para un diseño idéntico de ROPUF en dos FPGA Zynq 7000

FPGA	Clave (hexadecimal)
1	D69BC397
2	70D6422A

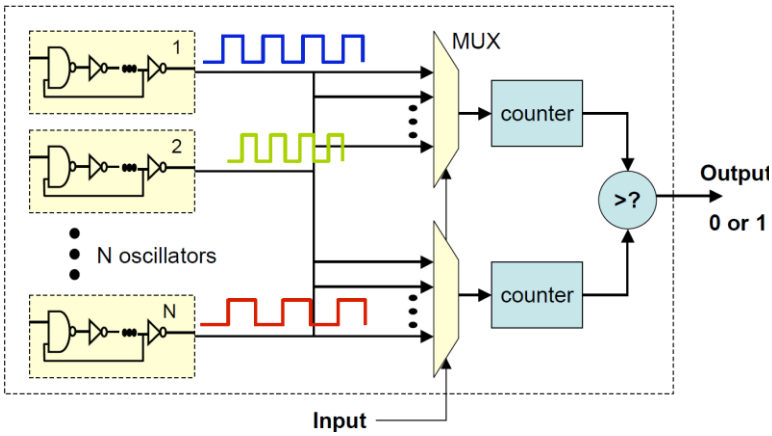

Fig. 1 Esquemático Diagrama conceptual de un circuito PUF de osciladores de anillo (ROPUF)

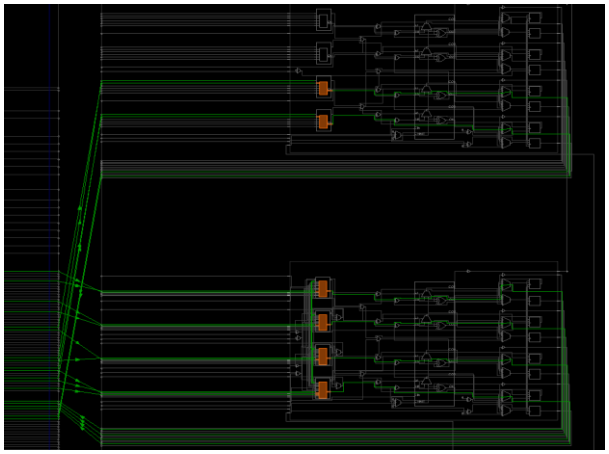

Fig. 2 Detalle del ruteado de un oscilador de anillo implementado sobre la FPGA. El circuito ROPUF se compone de la repetición de 33 estructuras idénticas.

REFERENCIAS

[1]. Handschuh H., Schrijen GJ., Tuyls P. *Hardware Intrinsic Security from Physically Unclonable Functions.* In: Sadeghi AR., Naccache D. (eds) Towards Hardware-Intrinsic Security. Information Security and Cryptography. Springer, Berlin, Heidelberg; 2010
.

[2]. G. Edward Suh, Srinivas Devadas, *Physical Unclonable Functions for Device Authentication and Secret Key Generation*, 2007, 44th ACM/IEEE Design Automation Conference, San Diego, CA, 2007, pp. 9-14.

[3]. Charles Herder *et.al*; *Physical Unclonable Functions and Applications: A Tutorial*; Proceedings of the IEEE; Vol. 102; No 8; 2014

[4]. Roel Maes; *Physically unclonable functions: constructions, properties and applications*, (2012), Universidad Católica de Lovaina, Bélgica, pp. 3-10