# Autenticación de smartphones mediante huellas digitales de silicio

Raúl Aparicio-Téllez, Miguel Garcia-Bosque, Guillermo Díez-Señorans, Abel Naya, 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

## Resumen

En este trabajo se implementa una nueva forma de autenticar dispositivos móviles que consiste en la construcción de una Función Física no-Clonable (PUF) que aprovecha las variaciones estocásticas de los acelerómetros y giroscopios inherentes al proceso de fabricación de un *smartphone* para identificarlo, obteniendo errores de falsa identificación $< 0.01\%$.

## Introducción

Una Función Física no-Clonable (PUF) explota las variaciones estocásticas que se producen durante el proceso de fabricación de un dispositivo para generar una "huella dactilar" de silicio que lo identifica, surgiendo como una solución óptima para la autenticación de dispositivos y la generación segura de claves [1], [2]. Los acelerómetros y giroscopios están presentes en una gran cantidad de dispositivos del día a día, incluyendo dispositivos móviles, vehículos, relojes inteligentes, etc. Por este motivo, aprovechando que estos sensores ya están integrados en estos dispositivos, resulta especialmente interesante construir una PUF basada en ellos evitando así diseñar un ASIC para autenticar al dispositivo. En este sentido, algunos trabajos previos han investigado la posibilidad de construir una PUF basada en MEMS [3].

Se ha observado que la señal que producen los acelerómetros y giroscopios en *smartphones* del mismo modelo y fabricante tienden a ser diferentes (Fig. 1) debido a variaciones intrínsecas al proceso de fabricación. En este trabajo, se propone utilizar algunas características extraídas de estas señales para generar claves para identificarlos (Fig. 2).

## Metodología

Se ha utilizado un conjunto de ocho *smartphones* incluyendo: dispositivos del mismo modelo y fabricante, diferentes modelos del mismo fabricante y de distintos modelos y fabricantes. Se ha medido la señal del acelerómetro y del giroscopio en reposo en cada uno de los tres ejes ortogonales con y sin vibración. Después, se han extraído algunas características de las señales (promedio y ruido) y se ha llevado a cabo un proceso de corrección de errores. Seguidamente, se realizado un proceso de reescalado de los parámetros y se han definido condiciones de contorno para que todos ellos tuviesen dos dígitos. Tras este proceso, se han obtenido 6 parámetros por cada eje, es decir, 18 parámetros en total. En la Fig. 3 se ha representado uno de esos parámetros: el ruido de la señal del acelerómetro sin activar la vibración del dispositivo en el eje *y*, frente al número de repeticiones, para varios dispositivos. Este parámetro muestra una aceptable reproducibilidad y unicidad, ya que parámetros de dispositivos distintos son distintos.

A continuación, se ha llevado a cabo un proceso de codificación. Los parámetros obtenidos no están uniformemente distribuidos en el intervalo de enteros de dos dígitos (-100,100) (Fig. 4). Por tanto, se ha seleccionado un subconjunto de parámetros, obtenido la distribución de los mismos y ajustado a una distribución gaussiana. Posteriormente, se ha dividido la gaussiana en intervalos de igual probabilidad y se ha asignado a cada uno de esos intervalos un número en código Gray. La decisión de utilizar el código Gray en lugar de directamente transformar los números de decimal a binario viene motivada porque en código Gray dos números consecutivos solo difieren en un bit, haciendo que la respuesta en bits sea más robusta frente a posibles errores de reproducibilidad. Este proceso se resume en la Fig. 4. Tras este proceso, se obtienen secuencias de 108 bits en dispositivos con acelerómetro y giroscopio, y de 72 bits en los que únicamente tienen acelerómetro. Todo este proceso de extracción de características y construcción de la respuesta de la PUF se realiza íntegramente en una app propia compatible con Android [4].

## Resultados

Para que la cadena de bits obtenida se pueda utilizar para autenticar dispositivos, ésta debe ser

reproducible, es decir, que en distintos instantes proporcione la misma respuesta; y única, es decir, que la respuesta de un dispositivo sea distinta a la que genera otro dispositivo idéntico. Para medir la reproducibilidad, se comparan respuestas generadas por un mismo dispositivo en instantes distintos. En particular, en este caso, se han tomado 10 medidas de cada uno de los 18 parámetros. Para medir la unicidad, se comparan respuestas de dispositivos distintos. Para comparar ambas respuestas se utiliza como métrica la Distancia Hamming (*HD*) que mide el número de bits distintos entre las dos secuencias. Una unicidad perfecta supondrá una intra-*HD* = 0 % y una reproducibilidad perfecta supondrá una inter-*HD* = 50 %, en promedio. Adicionalmente, en el contexto de identificación de dispositivos, se utiliza como métrica estándar el *Equal Error Rate* (*EER*), que combina las propiedades de reproducibilidad y unicidad simultáneamente. Éste es el parámetro más importante ya que mide la probabilidad de que un intento de identificación del dispositivo resulte simultáneamente en un falso rechazo (*FRR*) o una falsa aceptación (*FAR*), e idealmente será 0.

La PUF construida presenta una inter-*HD* del 45,37 %, muy próxima al 50 % ideal y una intra-*HD* del 12,69 %. Además, se ha obtenido un *EER* de $9{,}42 \cdot 10^{-5}$ (Fig. 5), lo que indica que aproximadamente solo el 0,009 % de los intentos de autenticación del dispositivo resultarán en un error.

# Conclusiones

En este trabajo se propone una PUF para autenticar *smartphones* usando las señales del acelerómetro y giroscopio, sin necesidad de hardware adicional. Se ha medido un *EER* $\sim 10^{-5}$, mostrando su viabilidad para propósitos de identificación de *smartphones*. Futuros estudios pasarán por utilizar un mayor número de sensores y parámetros.

# Agradecimientos

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

## REFERENCIAS

[1]. BÖHM C., and HOFER M. Physical Unclonable Functions in Theory and Practice. Springer, New York, NY, 2013.

[2]. MCGRATH T., BAGCI I.E., WANG Z.M., ROEDIG U., YOUNG R.J. A PUF taxonomy. Applied Physics Reviews, 6(1):011303, 02, 2019.

[3]. RAHIM K., TAHIR H., and IKRAM N. Sensor Based PUF IoT Authentication Model for a Smart Home with Private Blockchain. *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, pages 102–108, 2018.

[4]. NAYA-FORCANO, A. GDE PUF Authentication App. Available in Play Store: https://goo.su/BImphA5.

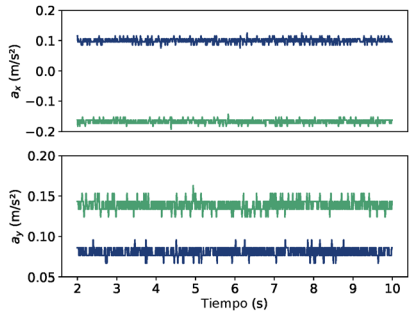


Figura 1. Señal del acelerómetro en los ejes X ($a_x$) e Y ($a_y$) de dos *smartphones* idénticos.

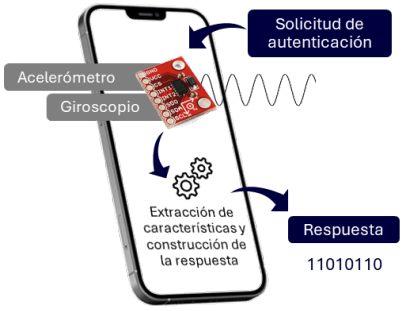


Figura 2. Esquema de funcionamiento de la MEMS-PUF propuesta.

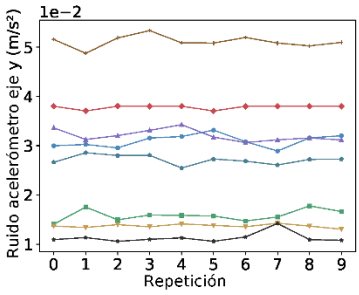


Figura 3. Ruido del acelerómetro en el eje Y sin vibración en ocho dispositivos.

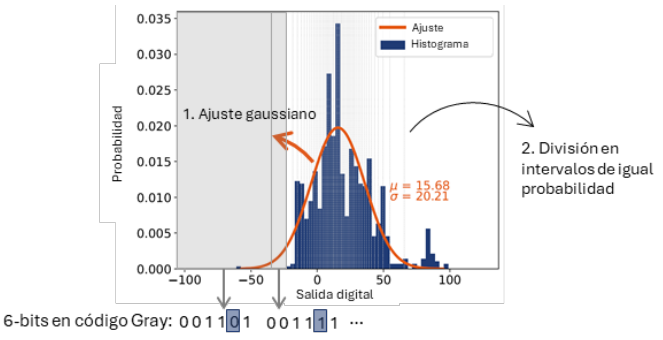


Figura 4. Codificación de las características de la señal en cadenas de 6 bits.

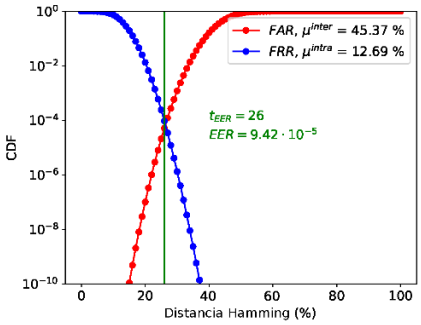


Figura 5. Probabilidad de falso rechazo (*FRR*), falsa aceptación (*FAR*) y *EER*.