PUF-enabled Security Challenge, European Cyber Security Awareness Week (CSAW) 2023

Proposal of a new PUF based on sensors for the identification of IoT smart mobile devices

Authors: **Raúl Aparicio-Téllez**, **Jorge Fernandez-Aragon**, **Abel Naya-Forcano** and **Guillermo Diez-Señorans**

Supervisors: **Miguel Garcia-Bosque, Santiago Celma**

Universidad Zaragoza

Group of Electronic Design (GDE), I3A, University of Zaragoza, Pedro Cerbuna 12, Zaragoza, Spain

PUF PROPOSAL

Parameters

N, k, δ

Response

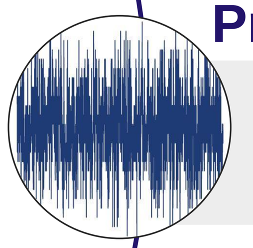
11010110

Own-developed app to measure and obtain the binary key.

Justification

Sensors of smart mobile devices provide an **inherent non-zero acceleration**, **angular velocity** and **noise** level when stationary.

Proposal



Use the **non-zero measured parameters** obtained to generate a **unique fingerprint**.

PUF

Results provide a **valid identification and authentication system. Already integrated in IoT system.**

TECHNICAL DESCRIPTION

Selection of the parameters

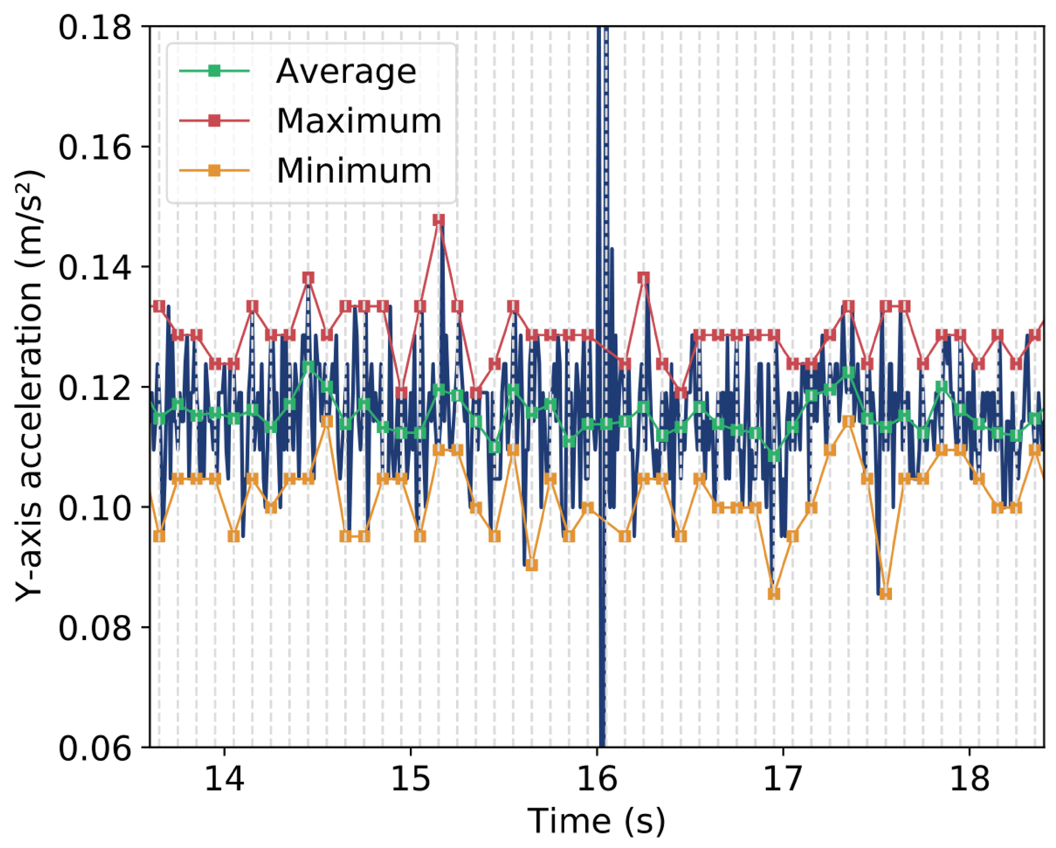
- Split in N intervals.
- Average (γ^i_{ave}), maximum (γ^i_{max}) and minimum (γ^i_{min}) values for every interval i.
- Average (μ) and standard deviation (σ).
- Valid range: $\{\Omega\} = \{\gamma_i \,|\, |\gamma_i - \mu| \leq k \cdot \sigma\}$.

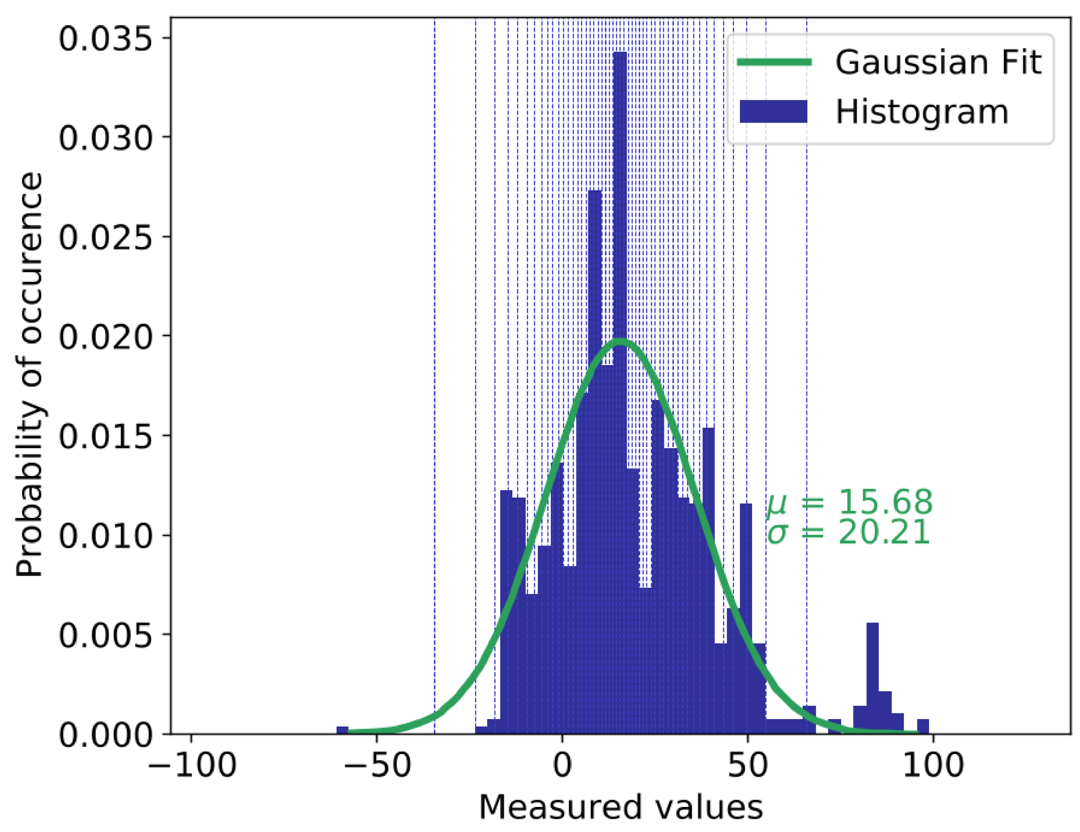
Encoding process

- Average ($\bar{s}$) and noise (s_{noise}) of the signal: $\bar{s} = \overline{\Omega_{aver}}$; $s_{noise} = |\overline{\Omega_{max}} - \overline{\Omega_{min}}|$.
- Narrow the interval $\mathbf{s} \rightarrow \boldsymbol{\alpha}$.
- **Fitted data** to a Gaussian distribution with **intervals of equal probability**.

PUF response

- Transform $\boldsymbol{\alpha}, \boldsymbol{\alpha_{noise}}$ into binary sequence using **Gray Code**.
- **Sequence of 6 bits** for each parameter, axis and device.
- Join all values to obtained **final response → 108-bit word**.





Accelerometer:

x	101101	y	011011	z	111010	μ
x	001011	y	011001	z	110101	*noise*
x	110101	y	001011	z	110111	μ
x	000101	y	110101	z	111010	*noise*

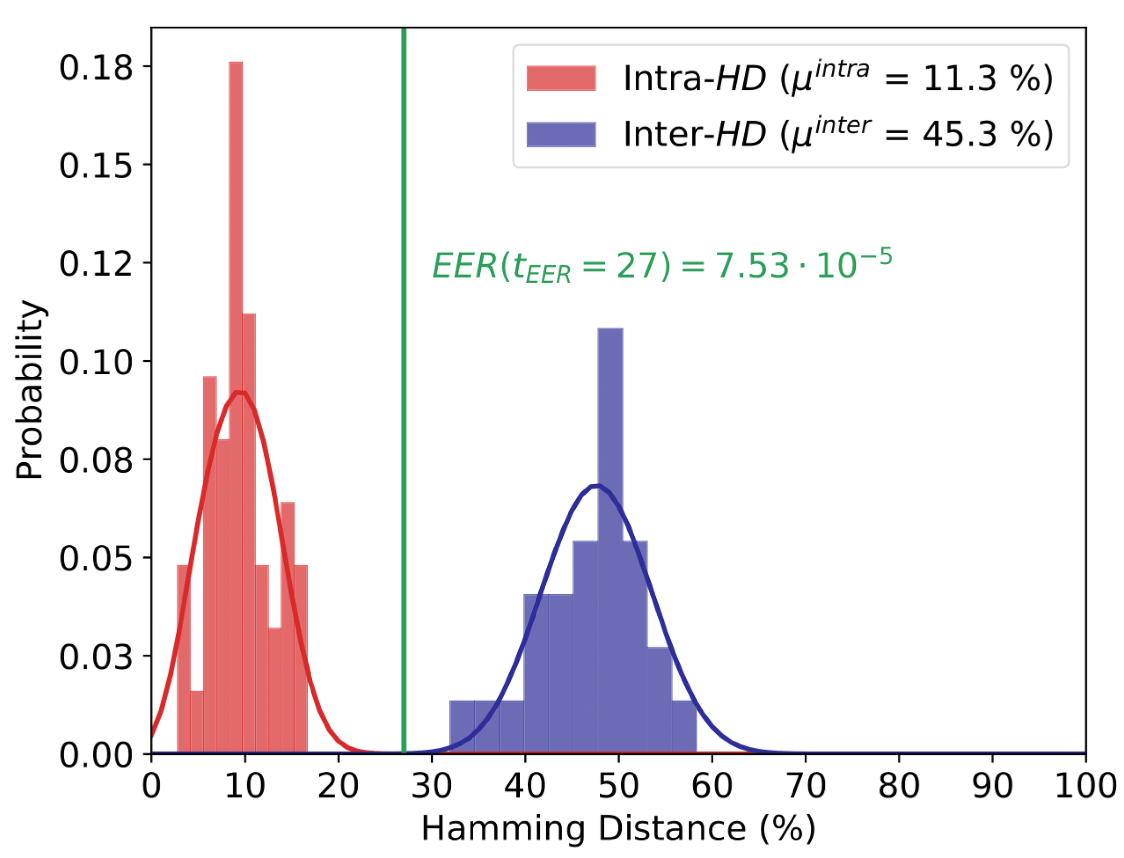
Gyroscope:

x	000101	y	001011	z	110101	μ
x	111101	y	110101	z	000100	*noise*

PUF response: 36-bit response + 36-bit response + 36-bit response

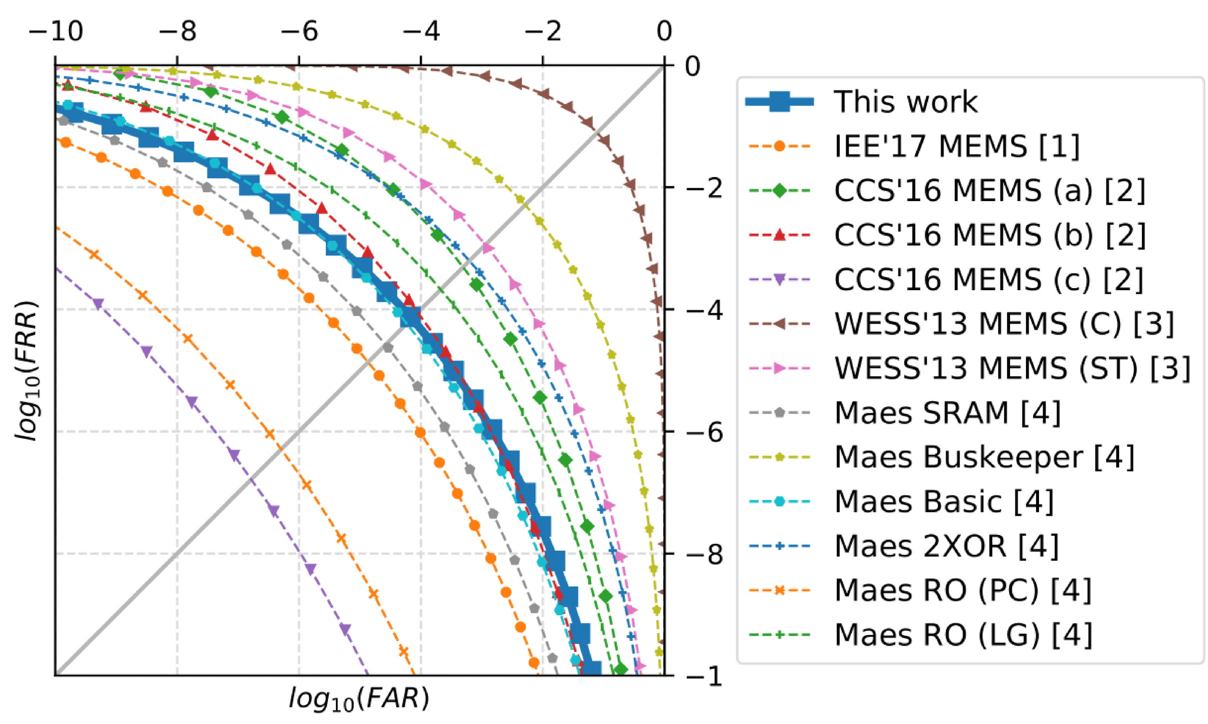
RESULTS

Uniqueness and reproducibility



Inter-*HD* and Intra-*HD* distributions, identification threshold (t_{EER}) and equal error rate (EER) obtained with 8 devices through 30 measurements.

Identifiability



Receiver Operating Characteristic (ROC) curves obtained and comparison with other PUFs.

[1] Ma, H. (2017). "A PUF sensor: Securing physical measurements".
[2] Willers, O. (2016). "MEMS Gyroscopes as Physical Unclonable Function".
[3] Aysu, A. (2013). "Digital fingerprints for low-cost platforms using MEMS sensors".
[4] Maes, R. (2012). "Physically Unclonable Functions: Concept and Constructions".

CONCLUSIONS

- ✓ **Good identifiability based on state-of-the-art PUFs.**
- ✓ **Results validate the feasibility of the PUF.**
- ✓ **Cost reduction (already integrated).**
- ✓ **Resistant to some common IoT attacks.**
- ✓ **Future lines: study more sensors and parameters.**

Generate the PUF key downloading our app

Google Play

Read the full paper