Ring Oscillator PUF on FPGA: Design and Characterisation by Using Second-Order Compensated Measurement

Jorge Fernandez-Aragon, Guillermo Diez-Señorans, Miguel Garcia-Bosque, Santiago Celma

Grupo de Diseño Electrónico (I3A), Universidad de Zaragoza, Mariano Esquilor s/n 50018, España

Instituto Universitario de Investigación **en Ingeniería de Aragón** **Universidad** Zaragoza

Universidad Zaragoza

GDE GRUPO DE DISEÑO ELECTRÓNICO
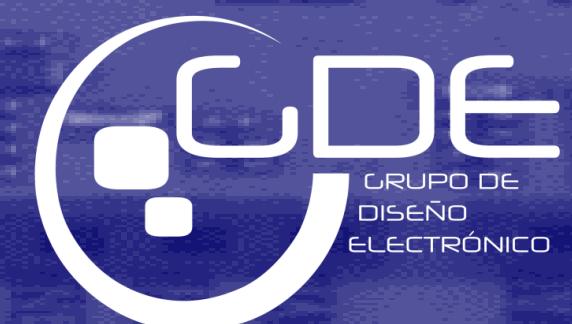
INTRODUCTION

Stochastic variations **inherent** to manufacturing process

Challenge → **PUF** → Response

PUF ↔ **IDENTIFIABILITY**

PUF ↔ **PHYSICALLY UNCLONABLE**

RO-PUF

Enable — [NAND] — [INV][INV][INV] — **Counter**

osc_i

$frequency(osc_i, osc_j)$ ← **>?**

Enable — [NAND] — [INV][INV][INV] — **Counter**

osc_j

IMPLEMENTATION

a) FPGA: *Zynq 7000 SoC*

b)

c)

Enable
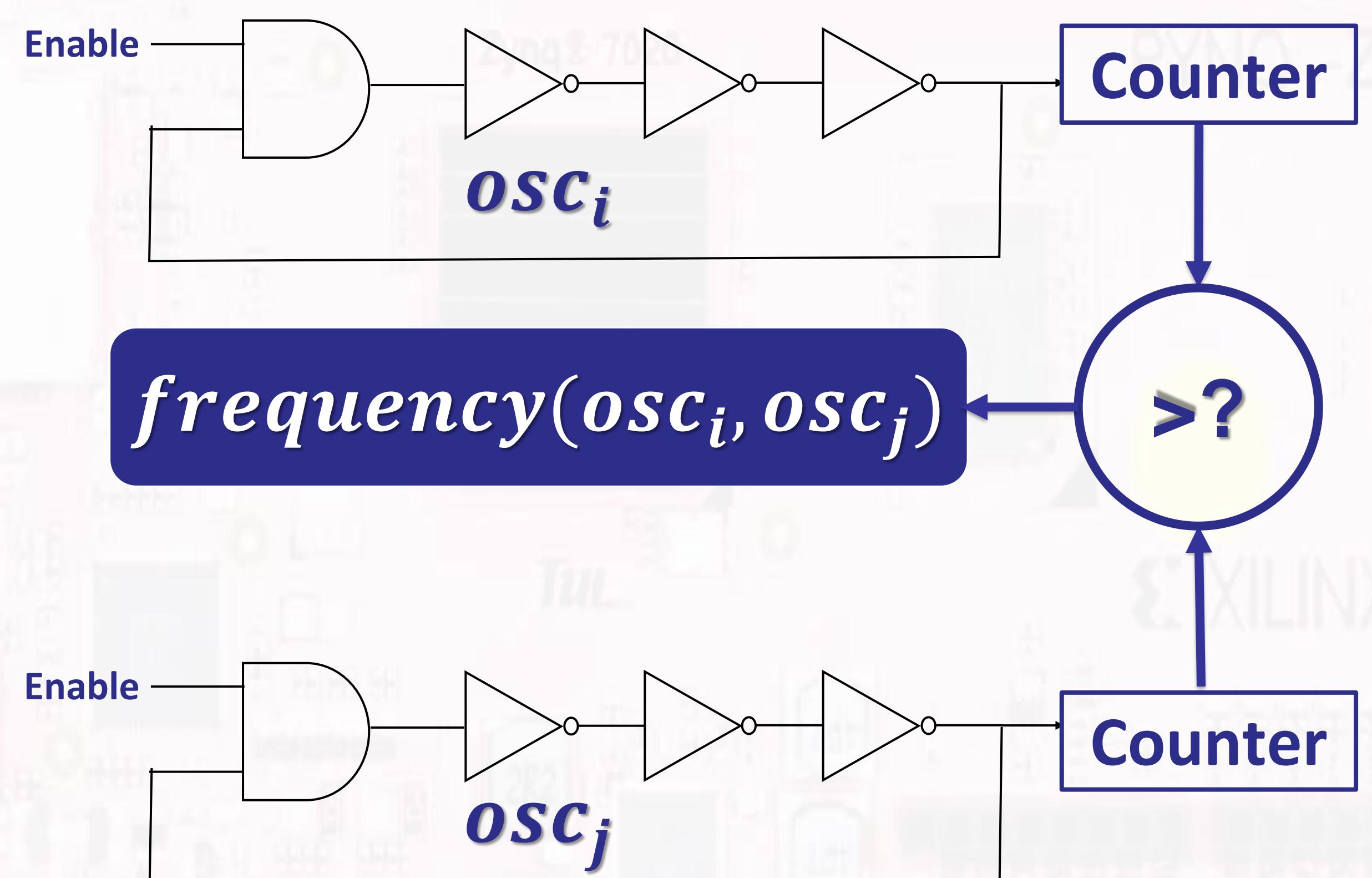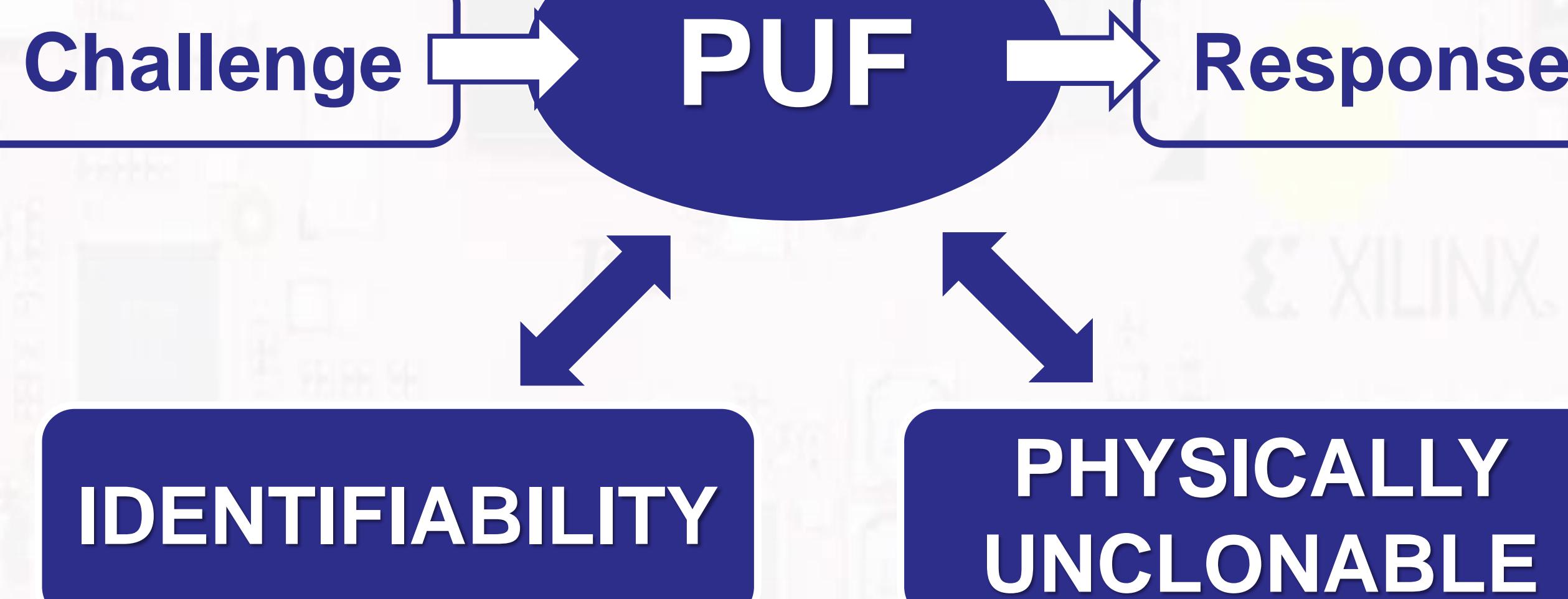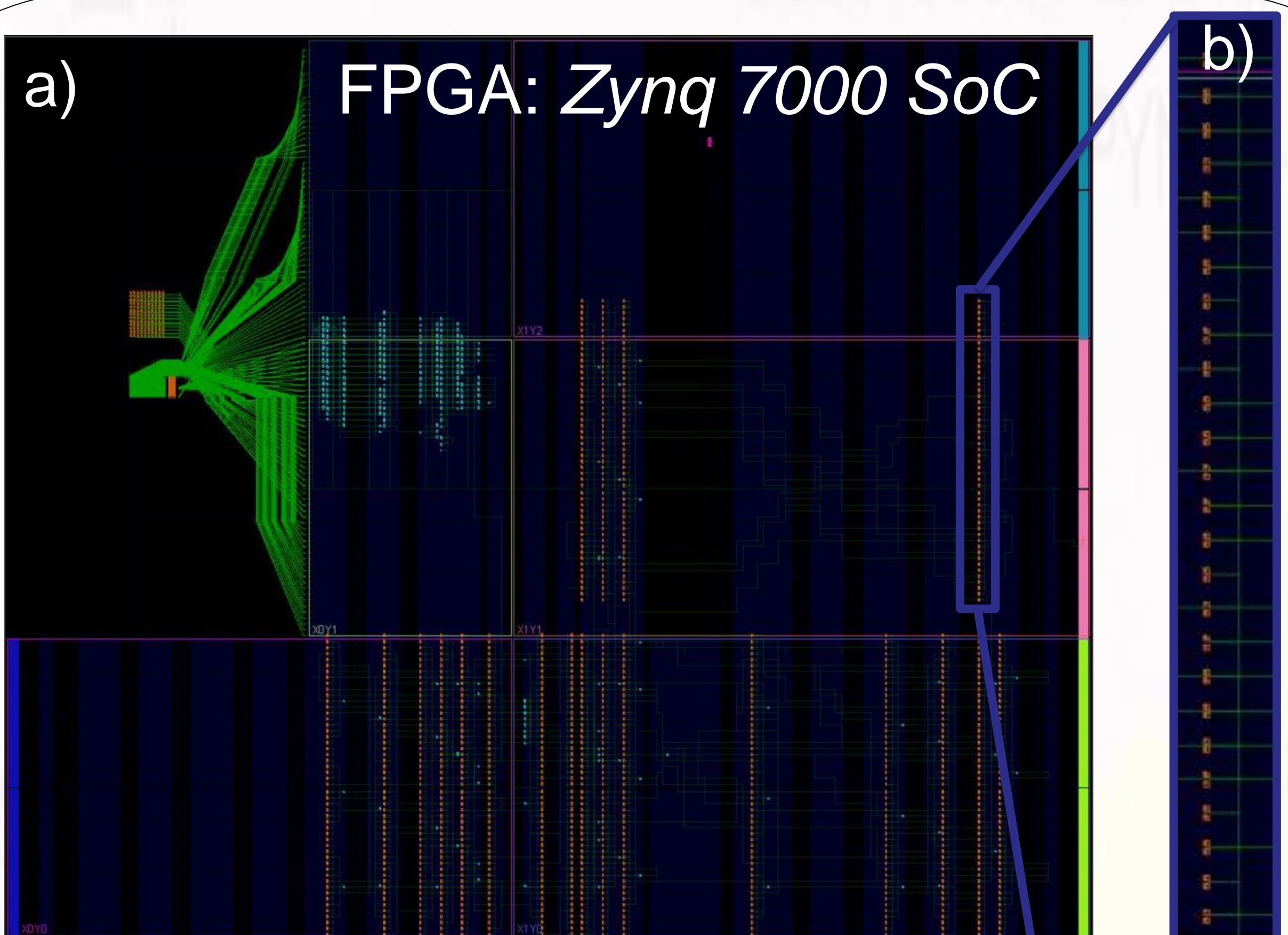
a) **FPGA-implemented RO array**

b) **51 RO reproduced in 20 different positions**

c) **RO ≡ 3 inverters + 1 AND gate**

METHODOLOGY

Extract oscillation frequency

⬇

Compare the frequencies of pairs of oscillators

⬇

32-bit array: sign bit (1 bit) + subtraction of frequencies in binary format (31 bits)

Sign bit

$$f_i > f_j \rightarrow 1 \; or$$
$$f_i < f_j \rightarrow 0$$

Remaining bits

$$Binary\{|f_i - f_j|\}$$

Create a 50-bit word corresponding to the bit we select in each case and study the reliability with the Hamming distance

RESULTS

Intra-distance and inter-distance

Legend:
- Ideal: Intra-distancia
- Ideal: Inter-distancia
- Sign bit: Intra-distance
- Sign bit: Inter-distance
- Bit 14: Intra-distance
- Bit 14: Inter-distance
- Bit 15: Intra-distance
- Bit 15: Inter-distance
- Bit 16: Intra-distance
- Bit 16: Inter-distance
- Bit 17: Intra-distance
- Bit 17: Inter-distance

Y-axis: Probabily
X-axis: Response Hamming Distances (%)
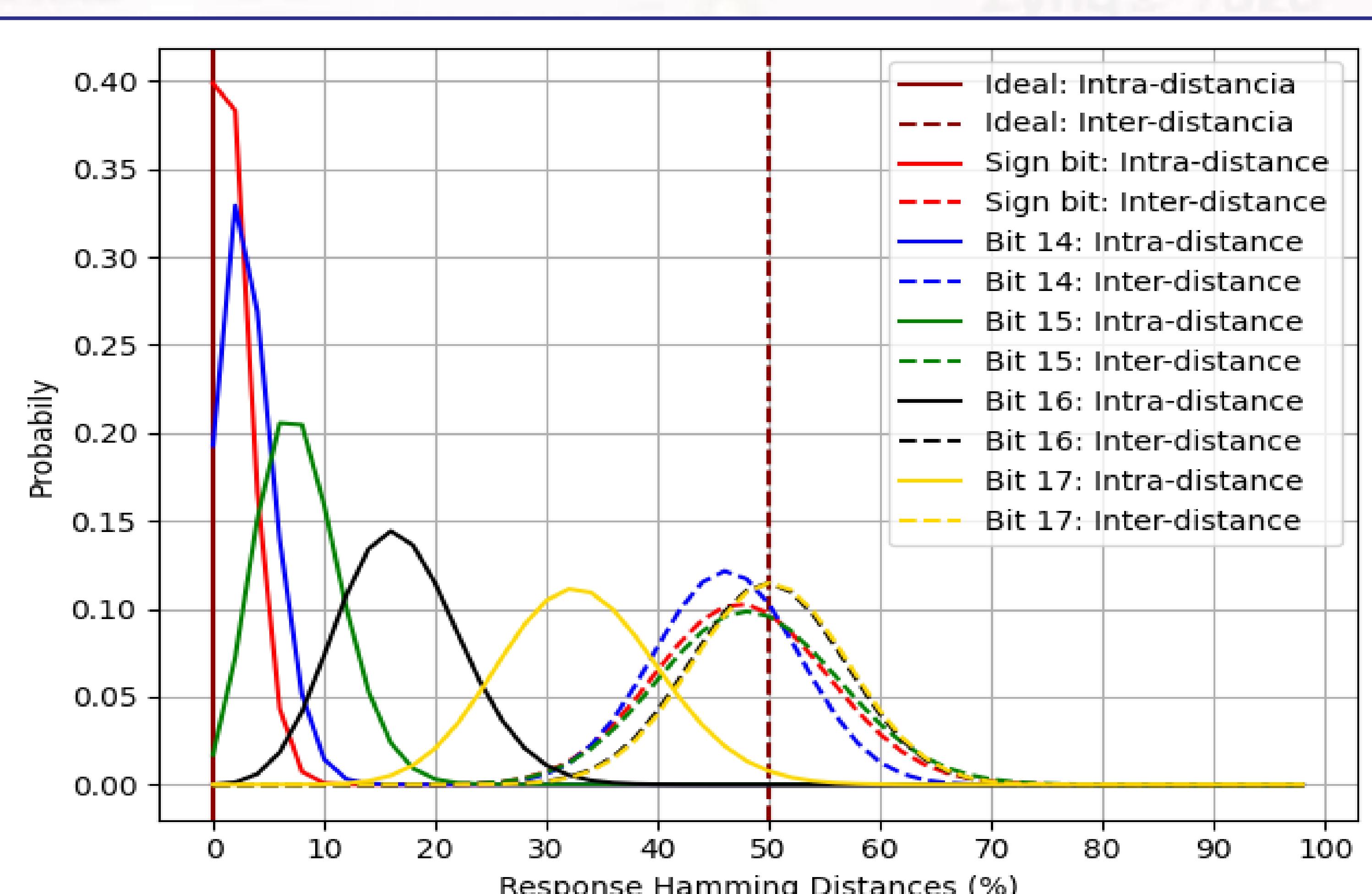
Receiver Operation Characteristic (ROC)

More secure

Better Identification

More robust

Legend:
- Sign bit
- Bit 14
- Bit 15
- Bit 16
- Bit 17

Y-axis: log_{10}(False Rejection Rate)
X-axis: log_{10}(False Acceptance Rate)