Enhanced TERO-PUF implementation and characterization on FPGAs

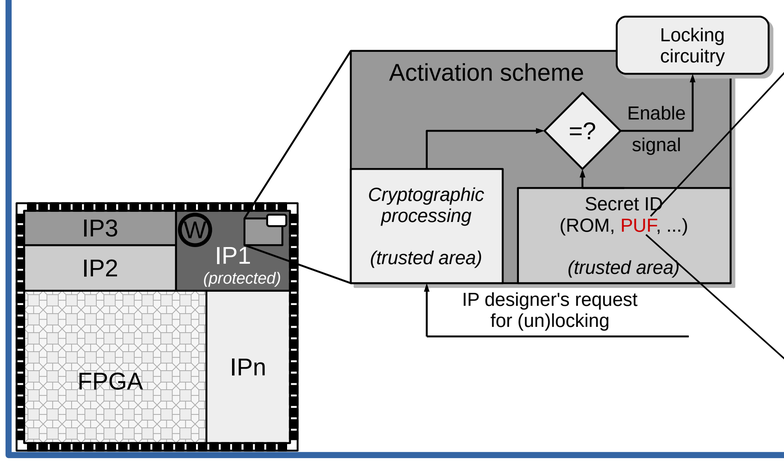
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Cédric Marchand and Lilian Bossuet
Hubert Curien lboratory, UMR CNRS 5516,
University of Lyon, Saint-Etienne, France,
{cedric.marchand, lilian.bossuet}@univ-stetienne.fr

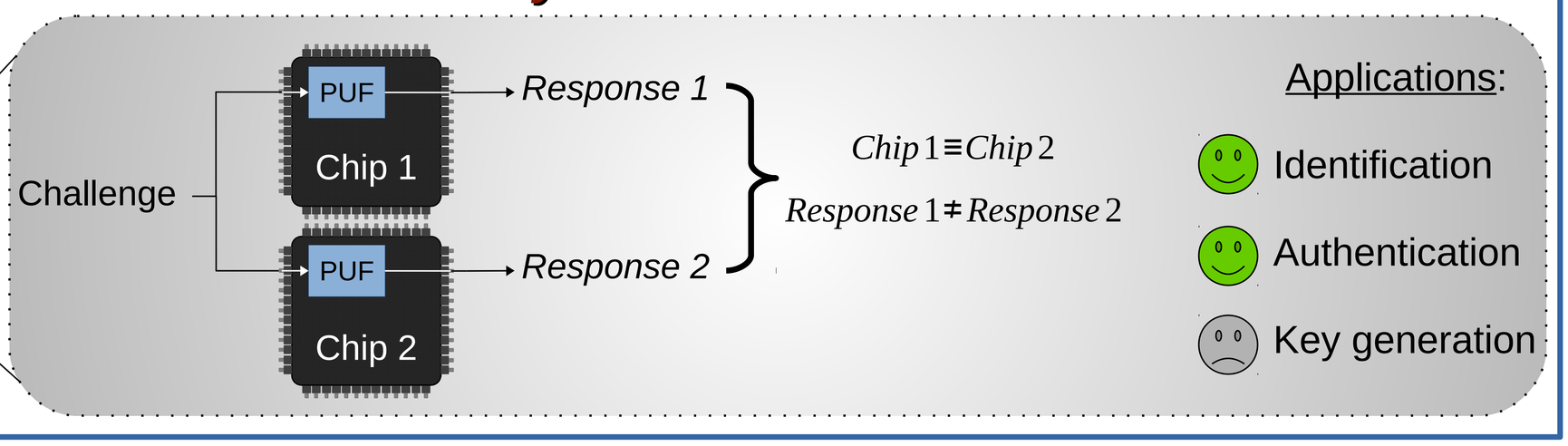
Abdelkarim Cherkaoui
TIMA laboratory
Grenoble, France
abdelkarim.cherkaoui@imag.fr

UNIVERSITÉ DE LYON
UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

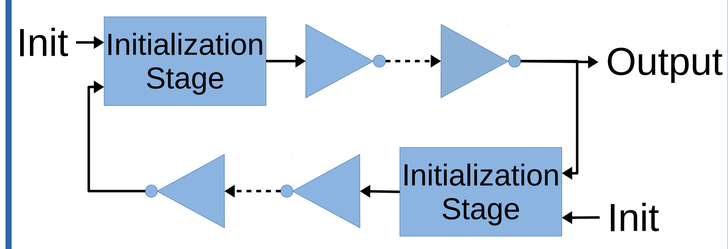
SALWARE project



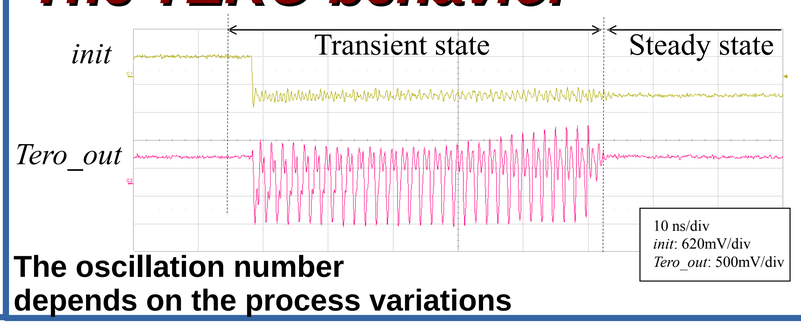
Physical Unclonable Function



The TERO cell

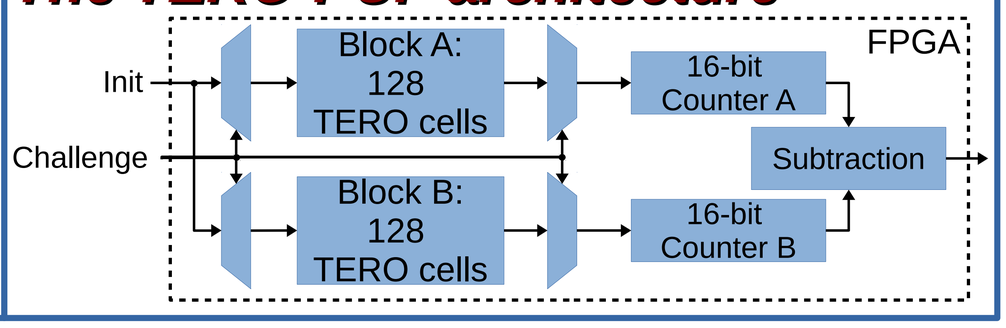


The TERO behavior



The oscillation number depends on the process variations

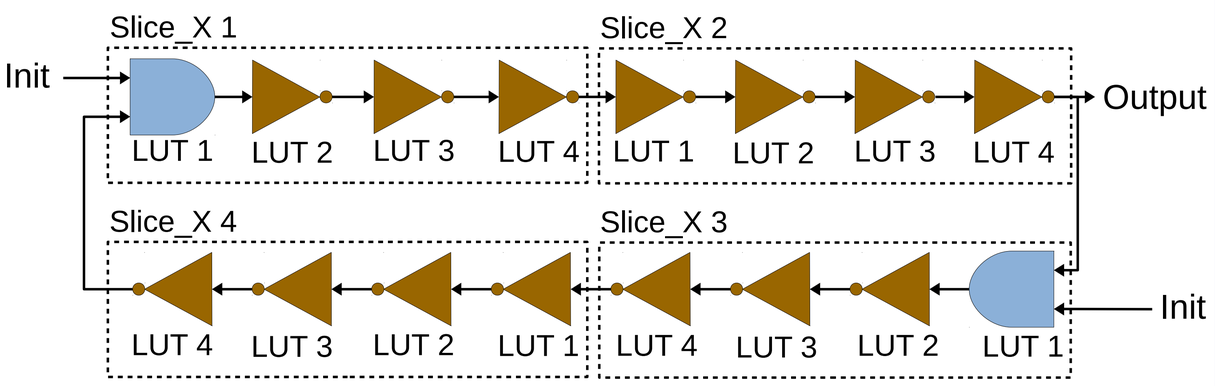
The TERO-PUF architecture



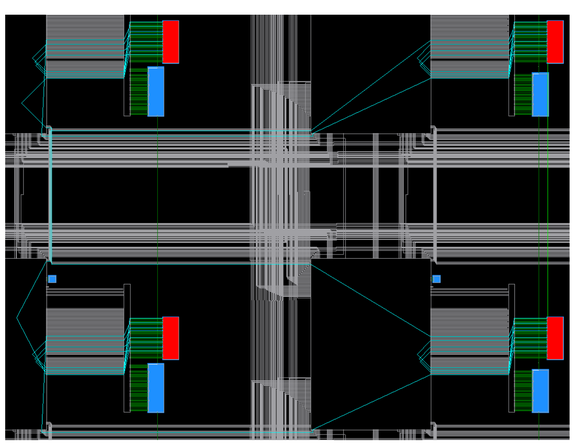
Design and Implementation of the TERO cell on SRAM FPGAs

Xilinx Spartan 6 FPGA (xc6slx16)

- LUT6 instantiation
- Placement by hand
- Hard Macro
- 4 Slices per cell
- Delays fully balanced



Xilinx FPGA Editor view

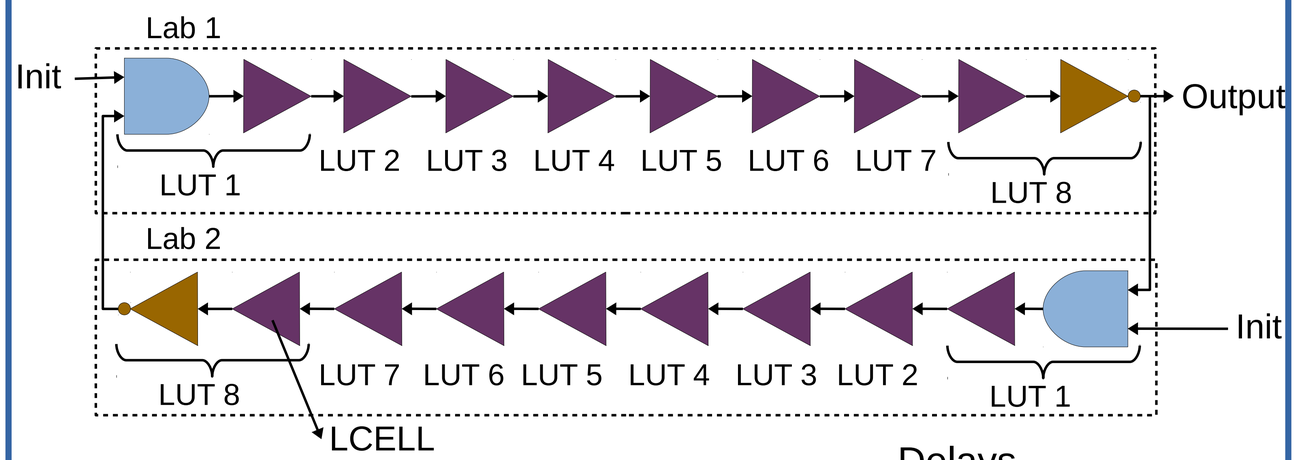


Delays

Starting Gate	Ending Gate	Branch 1	Branch 2
And	Not 1	0,143	0,143
Not 1	Not 2	0,352	0,352
Not 2	Not 3	0,230	0,230
Not 3	Not 4	0,494	0,494
Not 4	Not 5	0,143	0,143
Not 5	Not 6	0,352	0,352
Not 6	Not 7	0,230	0,230
Not 7	And	0,626	0,626

Altera Cyclone V (EP5CE BA4)

- LCELL: delay element
- Placement by hand
- Logic lock for the full system
- 2 LAB per cell
- 0,035ns delay difference



LAB configuration

LAB 1		LAB 2	
LCELL5	LCELL6	LCELL5	LCELL6
NOT		NOT	
AND		AND	
LCELL1	LCELL2	LCELL1	LCELL2
LCELL3	LCELL4	LCELL3	LCELL4

Delays

Starting Gate	Ending Gate	Branch 1	Branch 2
And	LCELL 1	0,257	0,257
LCELL 1	LCELL 2	0,259	0,259
LCELL 2	LCELL 3	0,249	0,249
LCELL 3	LCELL 4	0,254	0,254
LCELL 4	LCELL 5	0,220	0,220
LCELL 5	LCELL 6	0,260	0,260
LCELL 6	Not	0,242	0,242
Not	And	0,348	0,373

Characterization

Metrics:

- Steadiness (Intra-chip variations) :

$$IC_i(T,V)=\frac{1}{N}\sum_{j=1}^{N}\frac{HD(r_{i,j},r_{i,ref})}{n}\times 100$$

- Uniqueness (Extra-chip variations) :

$$EC=\frac{1}{M(M-1)N}\sum_{i=1}^{M}\sum_{k=1,k\neq i}^{M}\sum_{j=1}^{N}HD\frac{(r_{i,j},\overline{r_k})}{n}\times 100$$

- Randomness

Parameters:

- Temperature : -15 to 65°C
- Voltage : 1,1 to 1,3V for Spartan 6; 1,05 to 1,15V for Cyclone V
- Acquisition time : 6µs

Response bit per challenge	Steadiness (mean value over 30 chips)		Uniqueness (over 30 chips)	
	Xilinx Spartan 6	Altera Cyclone V	Xilinx Spartan 6	Altera Cyclone V
1	2,63%	1,80%	48,46%	47,62%
2	**2,36%**	**2,66%**	**47,22%**	**48,58%**
3	3,56%	3,73%	45,52%	47,39%

Response bit per challenge	Temperature range (10%)		Voltage range (10%)	
	Xilinx Spartan 6	Altera Cyclone V	Xilinx Spartan 6	Altera Cyclone V
1	2°C to 65°C	-	1,10V to 1,27V	1,05V to 1,15V
2	**2°C to 65°C**	**-**	**1,14V to 1,27V**	**1,05V to 1,15V**
3	5°C to 48°C	-	1,16V to 1,25V	1,06V to 1,13V

This work was carried out using the framework of the SALWARE project supported by the French “Agence Nationale de la Recherche” and by the French “Fondation de Recherche pour l’Aéronautique et l’Espace”.

SALWARE French ANR Project

PROJET FINANCÉ PAR L’ANR - PROJECT FUNDED BY THE ANR

Fondation de Recherche pour l’Aéronautique & l’Espace