Master thesis

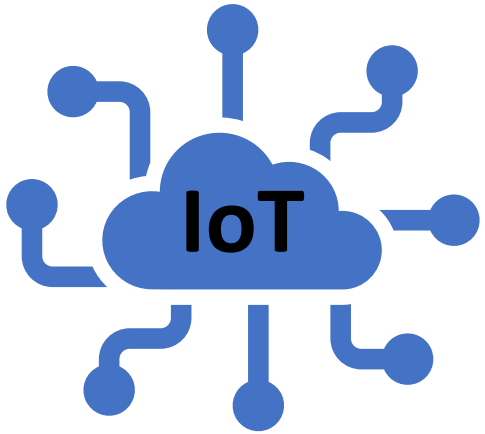
Physical layer security

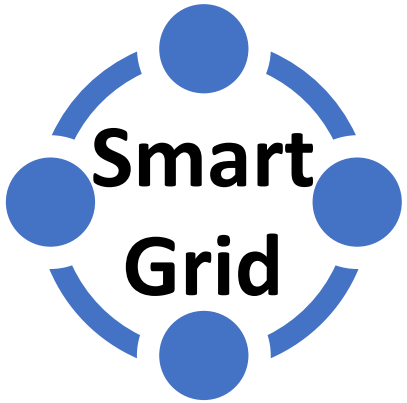
Authentication and ciphering using physical unclonable functions on FPGA

Oscar Van Slijpe
Supervisor: Dr. Pr. Jean-Michel Dricot
Co-supervisor: Dr. Pr. Dragomir Milojevic

IR-ELEC
2022-2023

Motivation



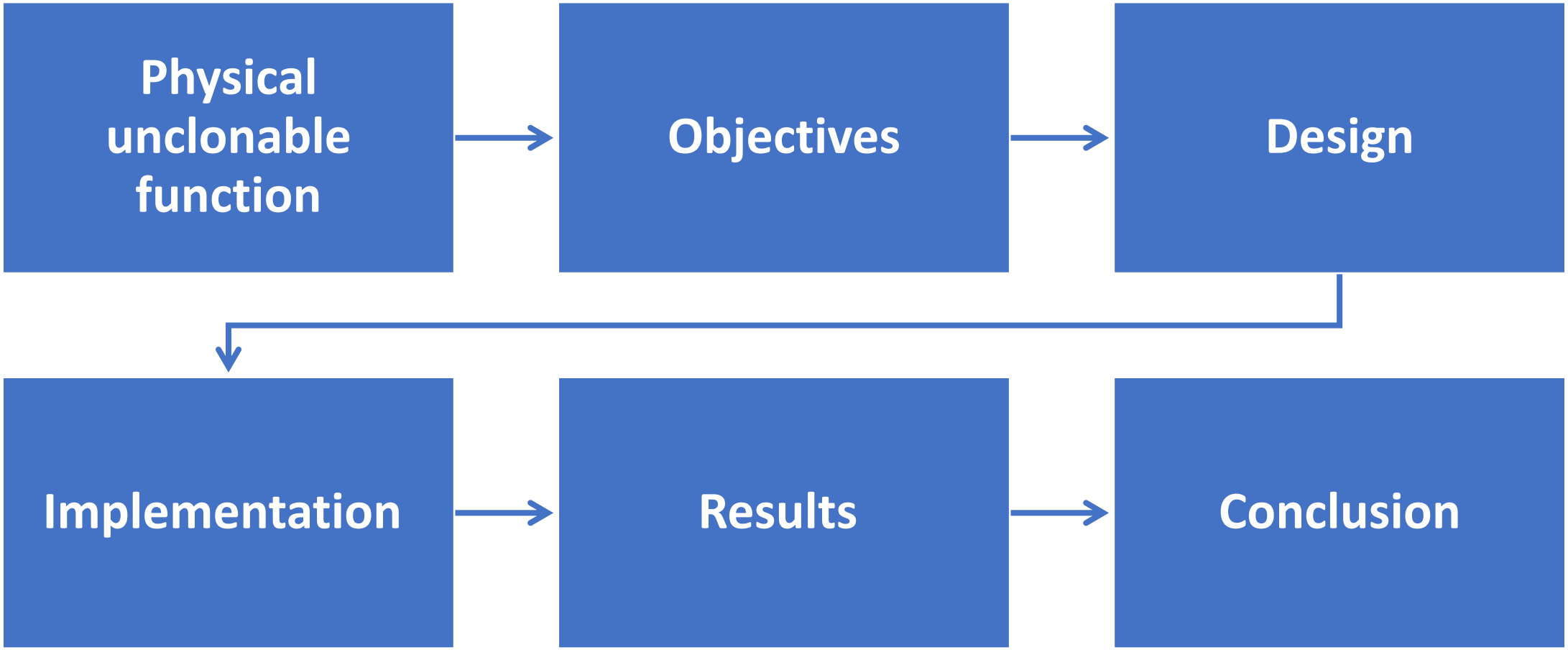


Own Security

Resistant to physical attack

Limited ressources

Table of content



PUF • Principles

Randomness

Key generation from random **intrinsic properties**

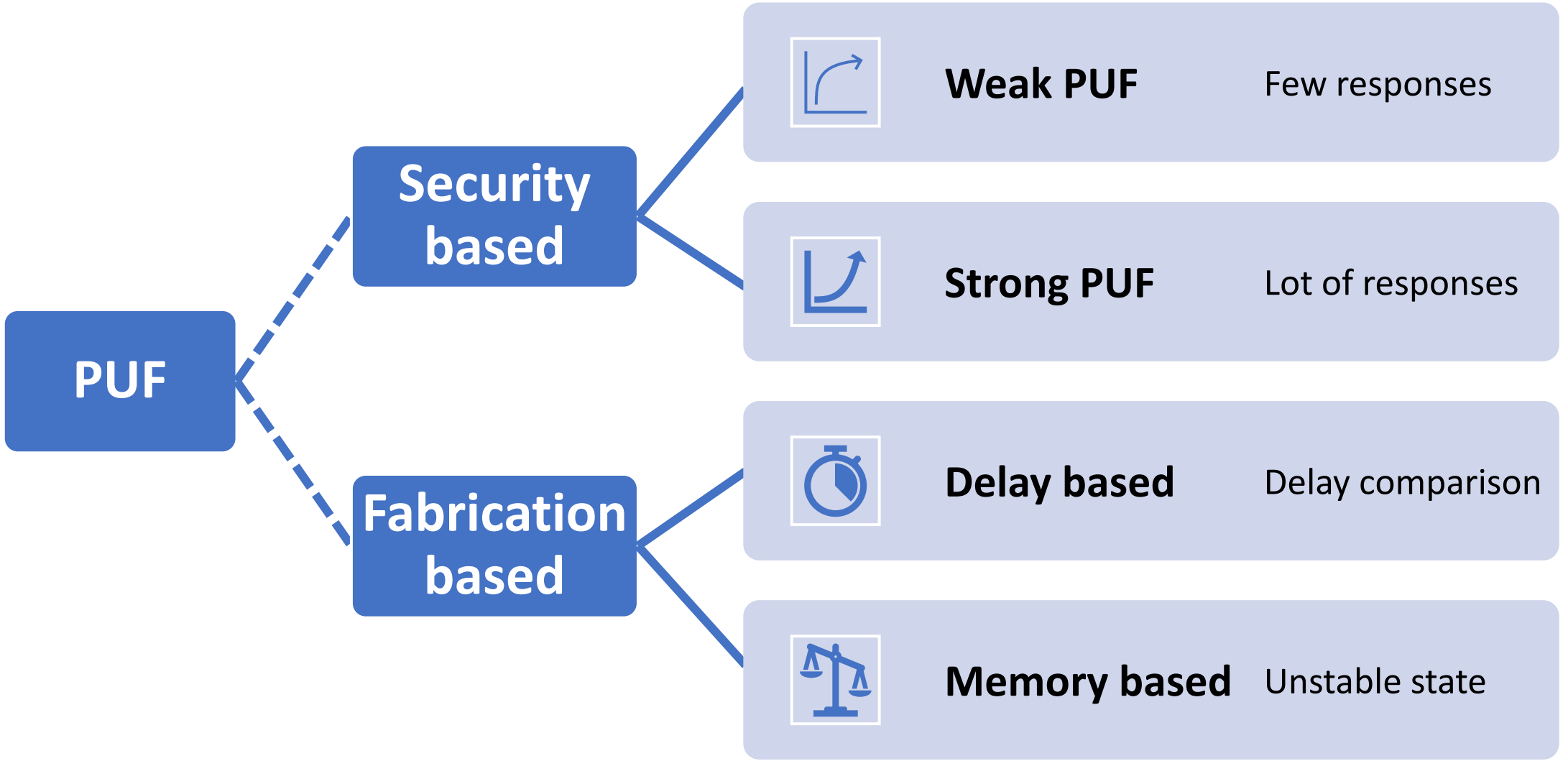
Unclonable

Due to **unreachable manufacturing precision**.

Usage

TRNG, key generation, identification, authentification

PUF • Classification



PUF • Examples • Arbiter

- Delay based
- One signal with 2 paths to a Latch
- Configurable paths using MUXs
- Response depend on the fastest path

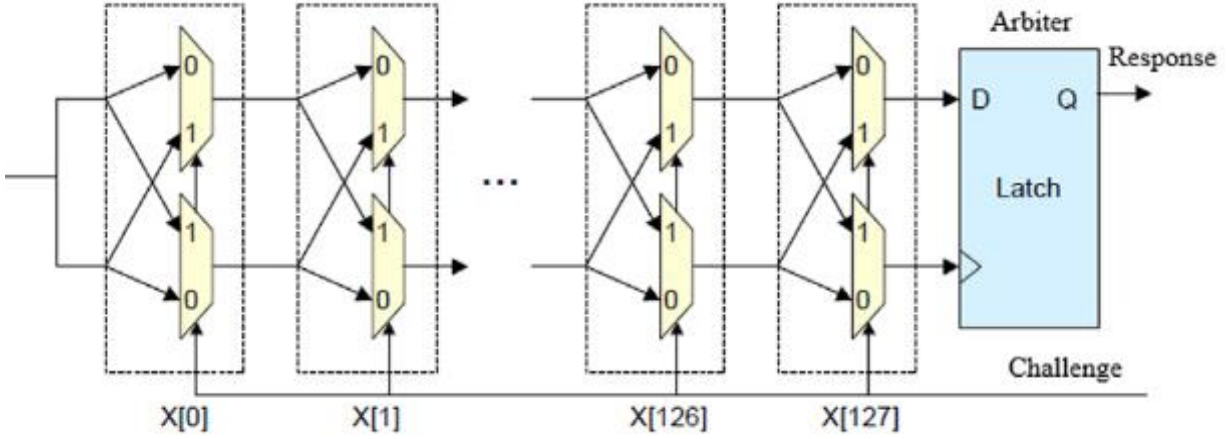


Figure 1: Arbiter PUF

PUF • Metrics

Uniformity

Repartition between 0 and 1.

Ideally equal to **50%** to maximise the entropy.

Reliability

Stability of the response over samples.

Ideally equal to **100%**

Uniqueness

Distance between the responses of different devices.

Ideally equal to **50%**

Bit-aliasing

Probability of each bit to be **1** over all devices

Ideally equal to **50%** for each bit.

PUF • Metrics

Method	APUF	FF-APUF	XOR-APUF	BST-APUF	RO-PUF	BST-ROPUF	M-ROPUF	TERO-PUF		PDL-TERO-PUF	SRAM-PUF	RWC-SRAM-PUF	FF-PUF
Reliability	**99.5%**	**90.2%**	**99.4%**	**99.9%**	**99.2%**	**99.9%**	*N/A*	**97.4%**	**98.2%**	**98.8%**	**98.2%**	**98.9%**	**99%**
Uniformity	**51.8%**	*N/A*	**50.7%**	*N/A*	**51.0%**	**46.7%**	**51.2%**	*N/A*	*N/A*	*N/A*	*N/A*	**55.4%**	**49.2%**
Uniqueness	**46.2%**	**38%**	**48.7%**	**49.1%**	**47.9%**	**48.6%**	**49.5%**	**48.5%**	**47.6%**	**49.3%**	*N/A*	**37.4%**	*N/A*
Bit-aliasing	*N/A*	*N/A*	*N/A*	**50.3%**	**51.0%**	*N/A*	**54.1%**	*N/A*	*N/A*	*N/A*	*N/A*	**46.9%**	**48.9%**
Device	Artix-7	ASIC	Artix-7	Artix-7	Artix-7	Artix-7	Kintex-7	Spartan-6	Cyclon-V	Spartan-3	Virtex-7	Artix-7	Artix-7

Objectives

Completing existing studies

Artix-7 FPGA

Transcient Ring Effect Oscillator

Test over multiple devices

33 boards

Small footprint

Easily integrated into existing systems

Fully working demonstration

Error correction

Key hashing

Ciphering

Design • TERO Cells

Oscillation	• 2 signals **propagating** • Output is **toggled**
Randomness	• **Intrinsic defects** affecting the signals propagation.
Stabilisation	• Signals **catch up** and **cancel** each other.
Observable results	• **Number of oscillations** before stabilisation

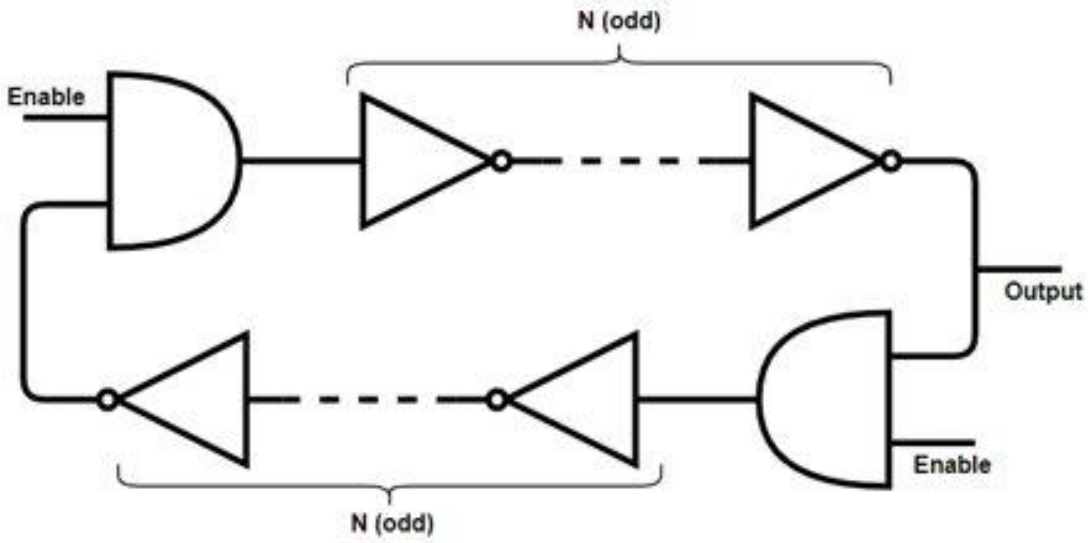


Figure 2: TERO cell

Design • Response generation

Cells	• Splitted in **2 arrays**
Pairs selection	• Using **LSFR** function
Stabilisation	• Reference **clock counter**
Comparison	• Number of **oscillations**

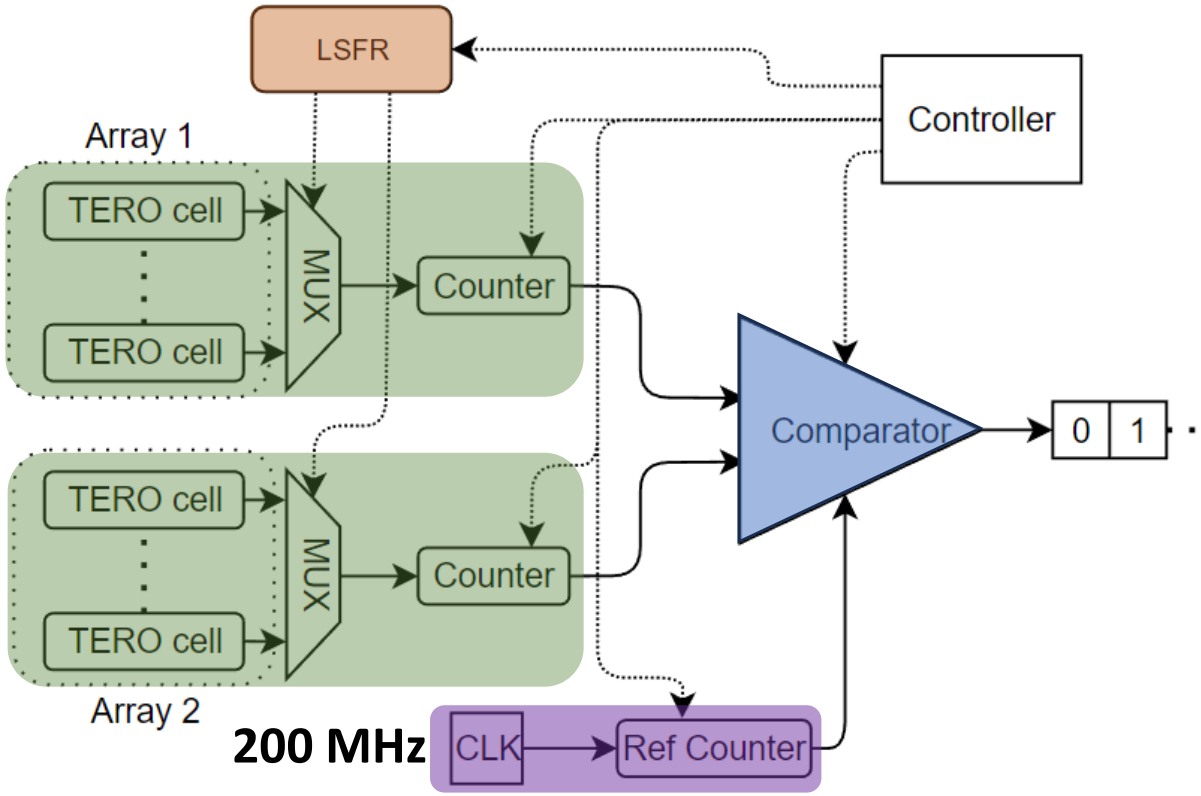


Figure 3: Response generation

Implementation • Artix-7 overview

LUT6

- Look up tables with **6** inputs.

Slice

- Containing **4x** LUT6.
- Two types
  - **Slice-L** (logic)
  - **Slice-M** (additionnal memory features)

Control Logic Block

- **2** slices that can be directly connected
- Inter CLB routing block for global routing

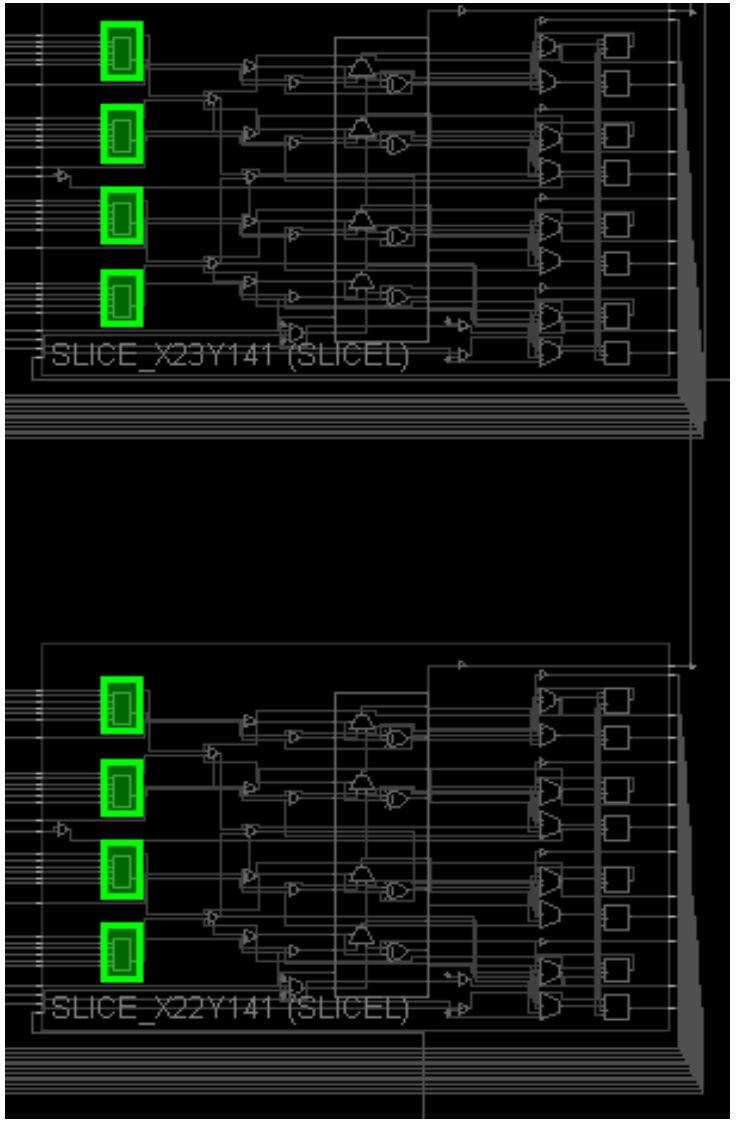


Figure 4: Artix-7 CLB

Implementation • Constraints

No optimisation

DONT_TOUCH

Disable automatique **optimisation**

Slice location

LOC

Only **Slice L**

LUTs usage

BEL & RLOC

Same **placement** of LUTs in the CLBs

Pins usage

LOCK_PIN

Same **routing** in the CLBs

Implementation • Cells

TERO-4

4 gates

1 slice

TERO-8

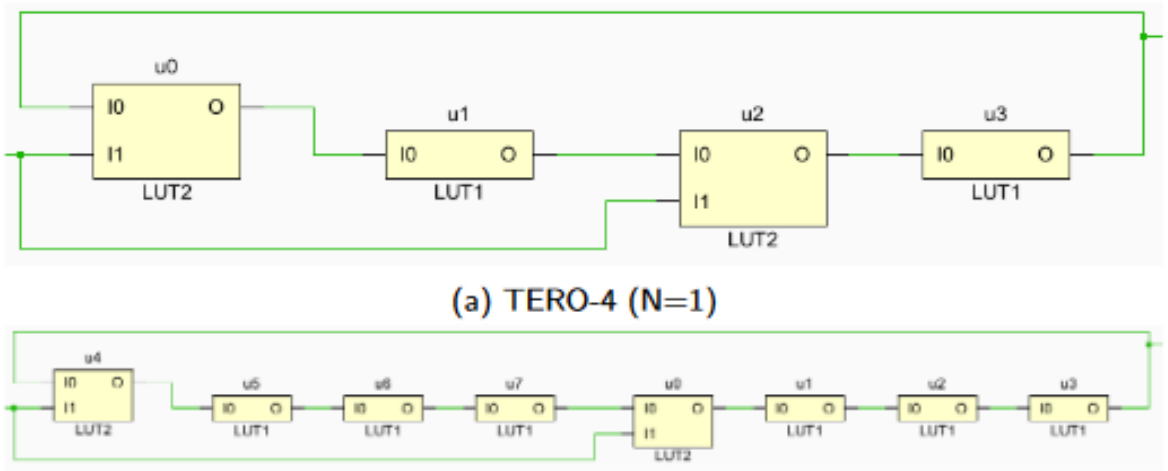
8 gates

1 CLB

Number of cells

2 x 32 cells

1023 bits



(a) TERO-4 (N=1)

(b) TERO-8 (N=3)

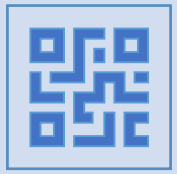
Figure 5: TERO cell

Implementation • Features

BCH decoder

Error correction code

From previous Master Thesis



SHA-256

Key hashing

Open source | Padding block

Results

1 device

Oscillation

Equalities

Uniformity

Reliability

33 devices

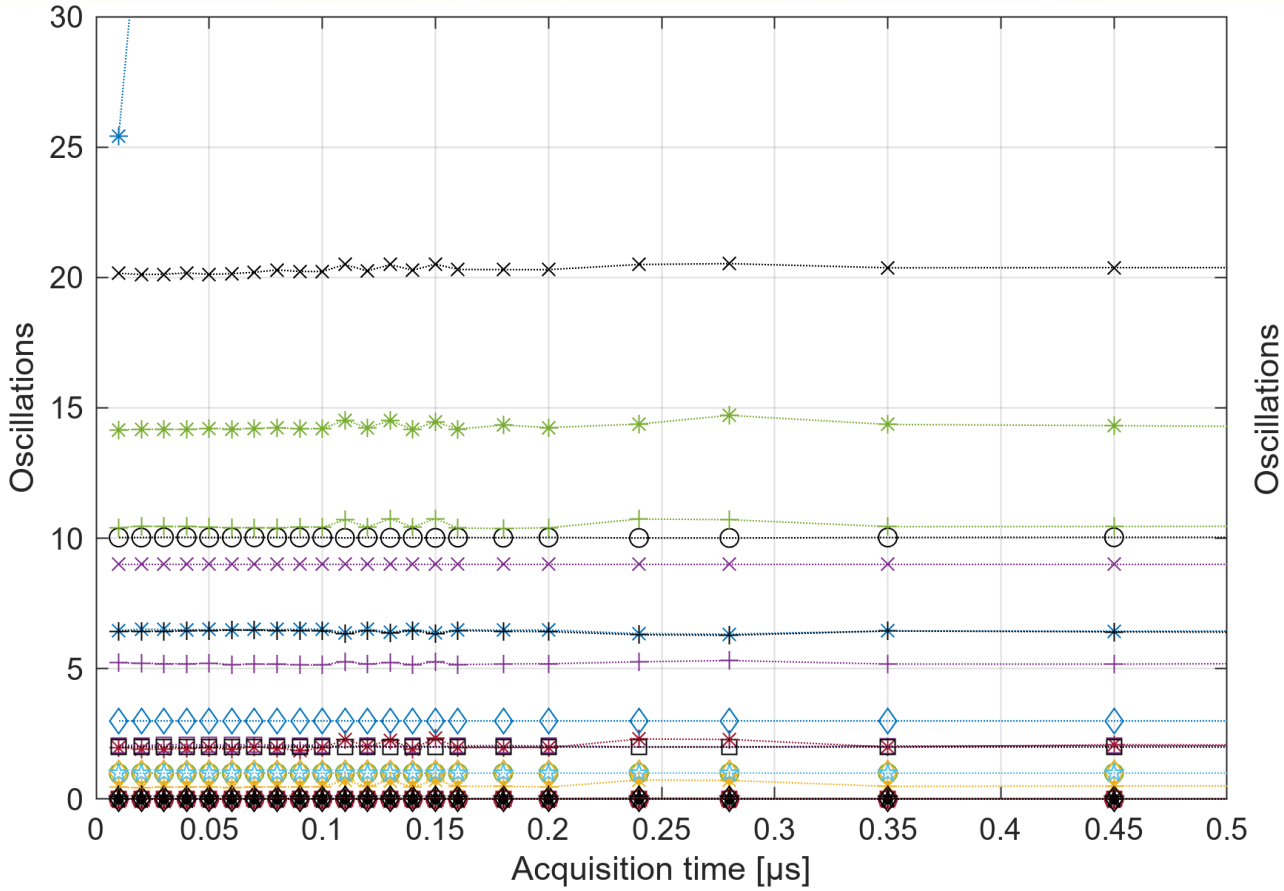
Average **uniformity**

Average **reliability**

Uniqueness

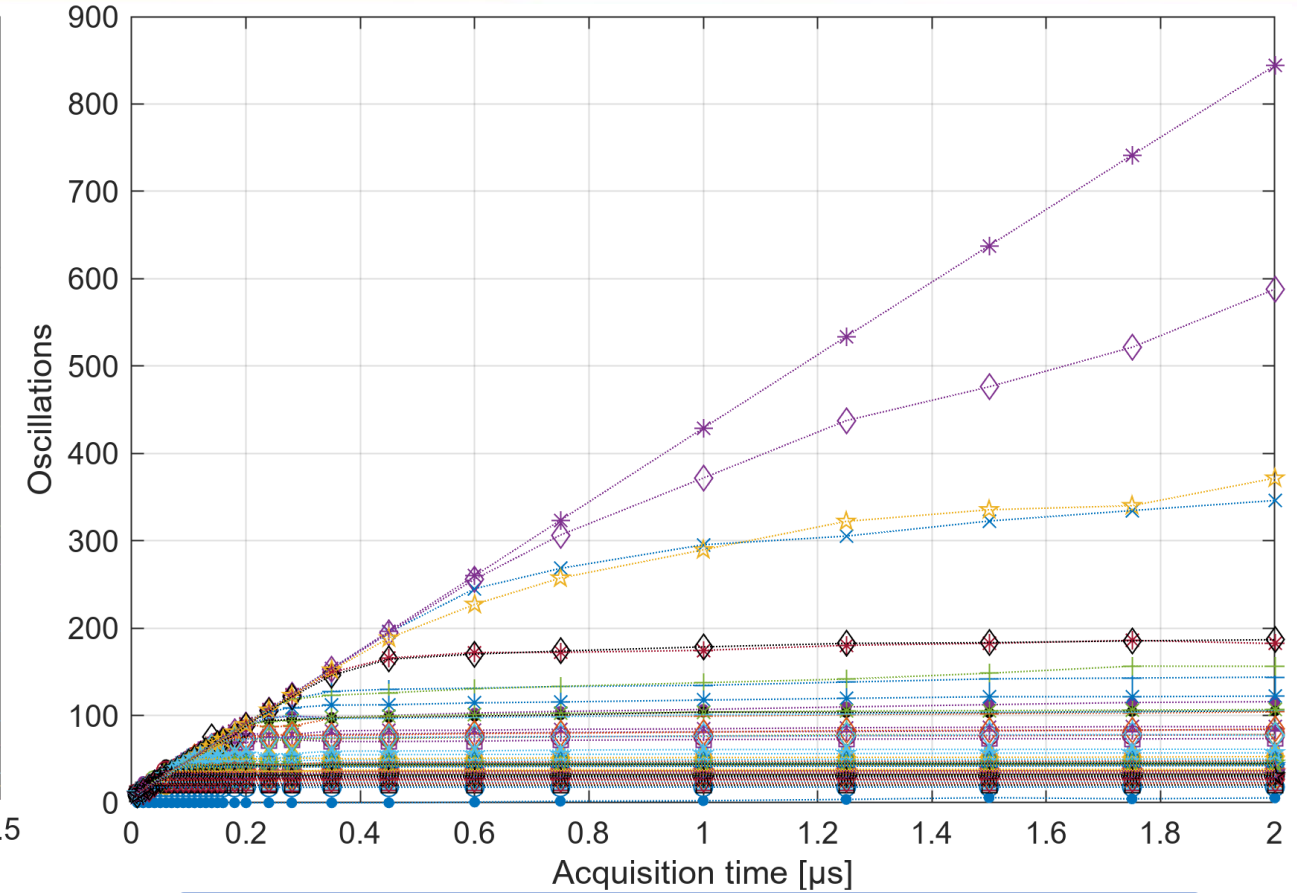
Bit-aliasing

Results • 1 Device • Oscillations (0 → 2 µs)



TERO-4

- Immediate stabilisation
- **47/64** Cells have **0** oscillation



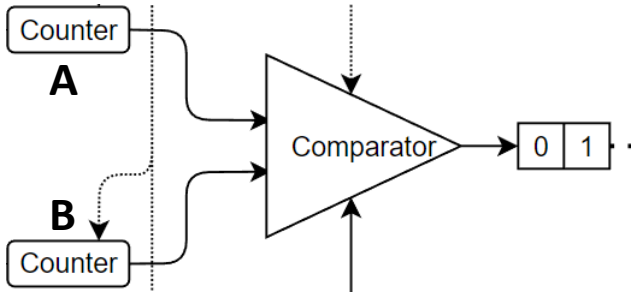
TERO-8

- Most stabilisation before **0.5**µs.
- **1/64** Cells has **0** oscillation

Results • 1 Device • Equalities (0 → 2 µs)

Equalities

- A > B ⟶ 0
- A < B ⟶ 1
- **A = B ⟶ 0**



TERO-4

- **96.9%** of equalities

TERO-8

- < **1%** of equalities

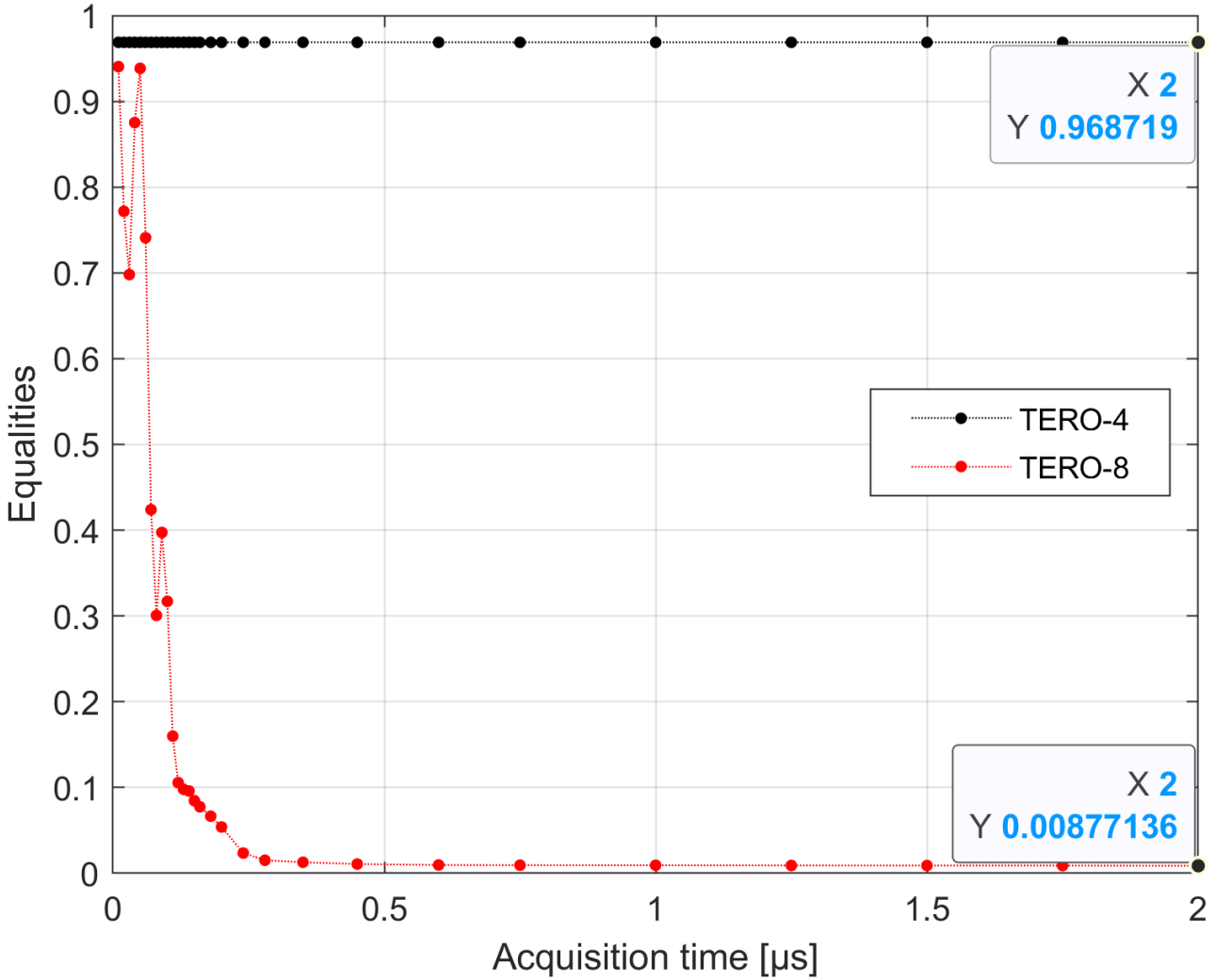


Figure 8: Cells equalities

Results • 1 Device • Uniformity (0 → 2 µs)

Intra-device uniformity

- Ideally equal to **50%**

TERO-4

- Constantly at **3%**

TERO-8

- Raises up to **53%**

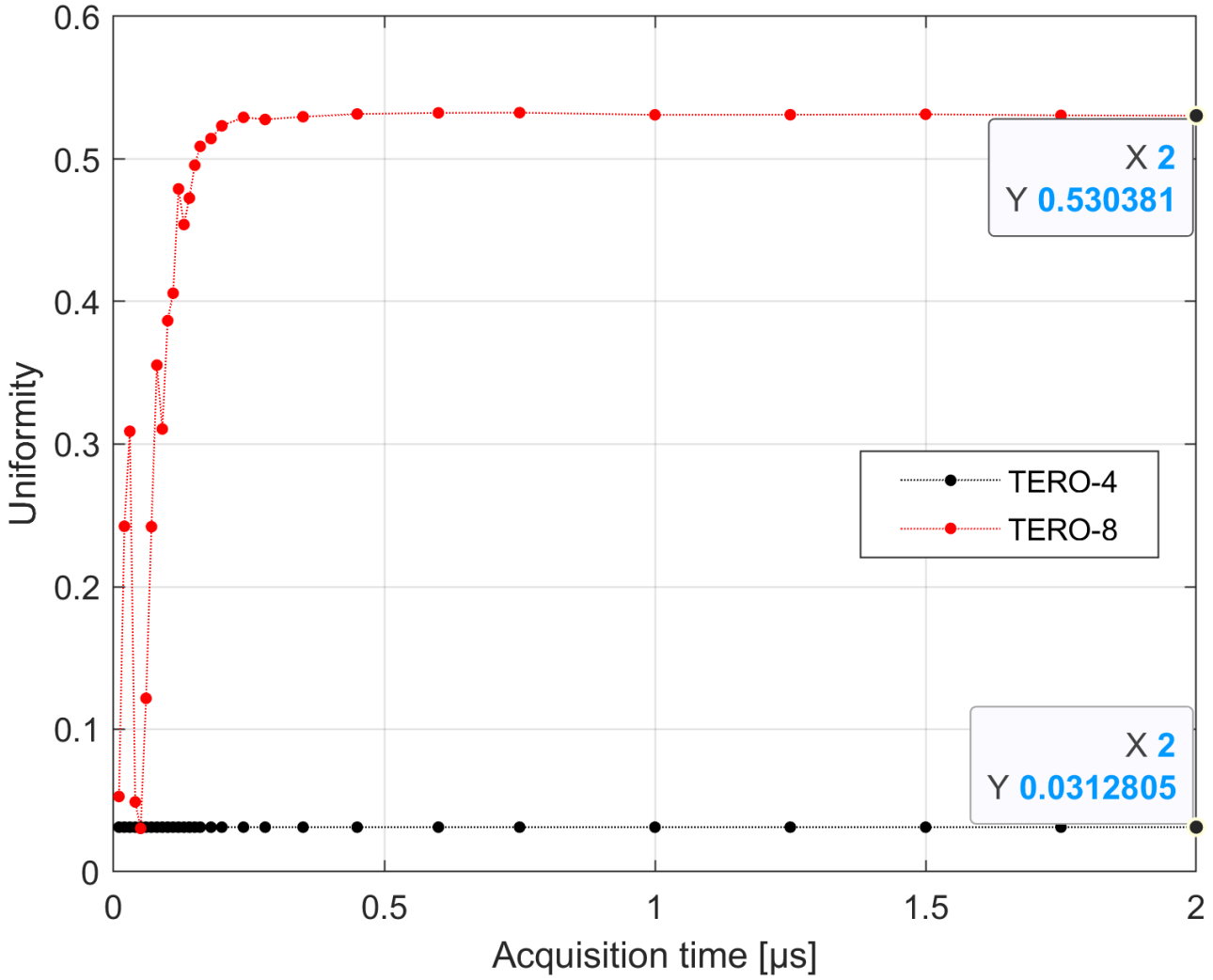


Figure 9: Uniformity

Results • 1 Device • Reliability (0 → 2 µs)

Intra-device reliabiliy

- Ideally equal to **100%**

TERO-4

- Constantly at **100%**

TERO-8

- Raises up to **97.7%**

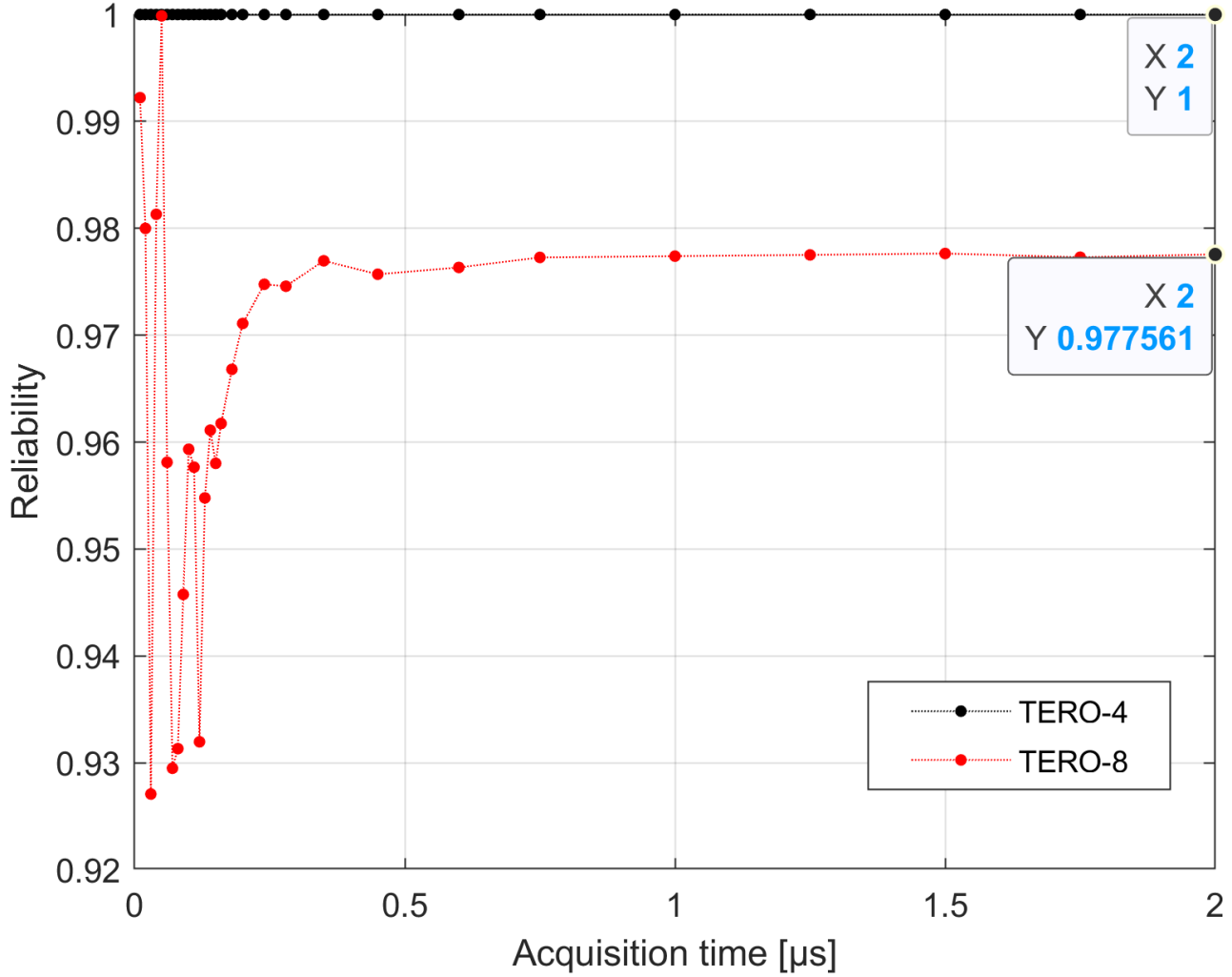


Figure 10: Reliability

Results • Acquisition time

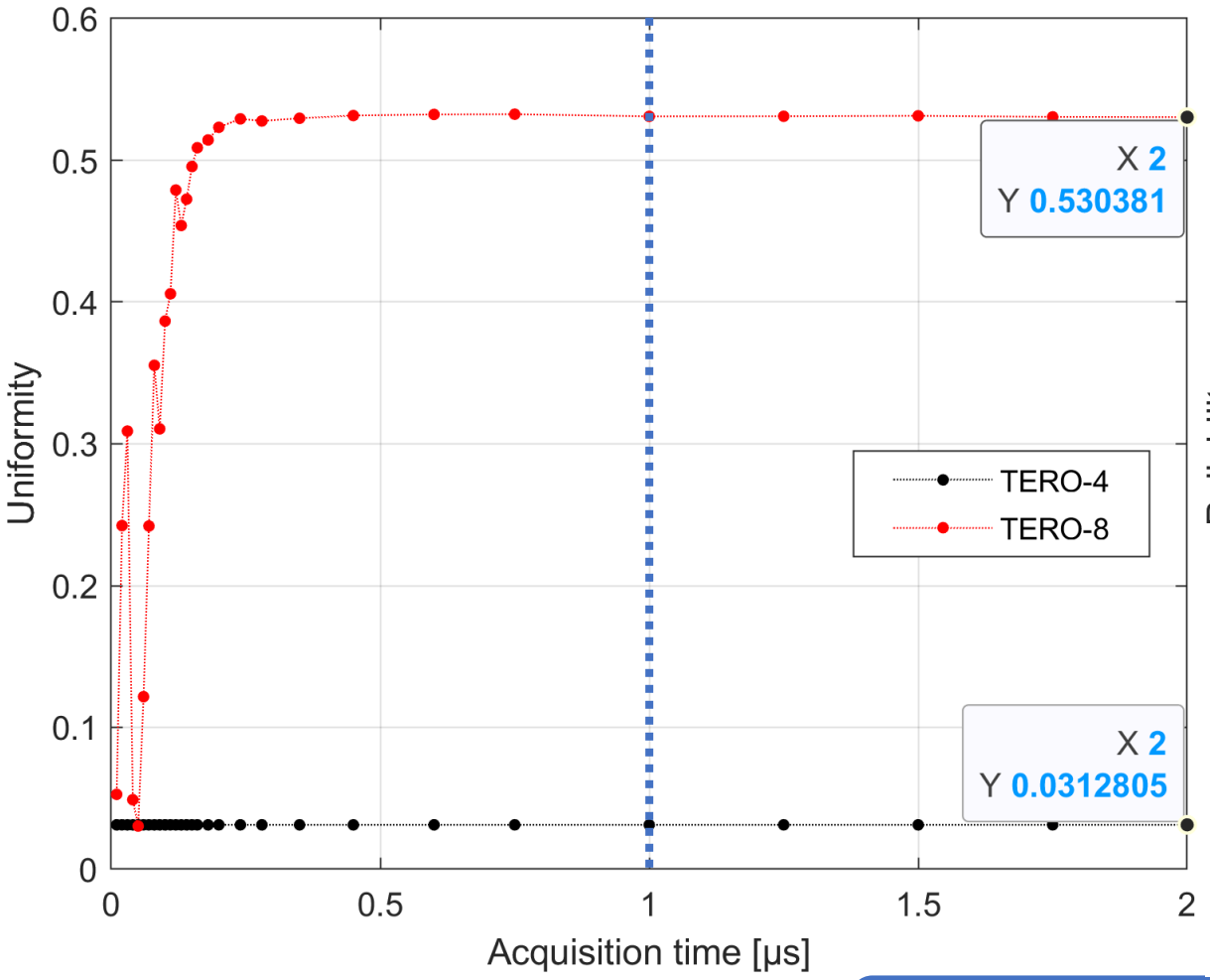


Figure 9: Uniformity

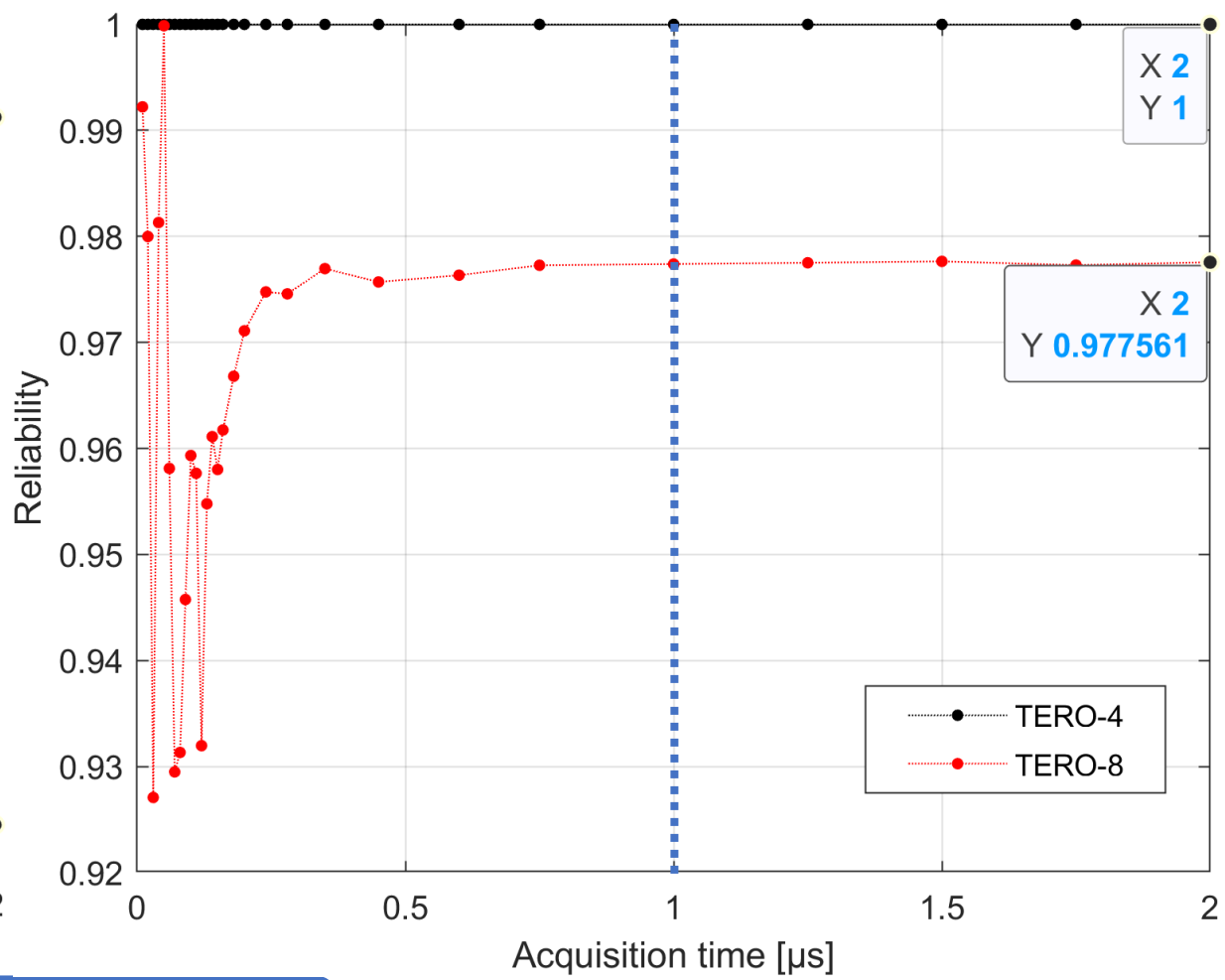


Figure 10: Reliability

Acquisition time = 1 µs

Results • 33 Devices • Uniqueness

	Average Uniformity		Average Reliability		Uniqueness	
IDEAL	*50%*		*100%*		*50%*	
TERO-4 (1st device)	8.1% (3%)	✗	99.8% (100%)	✓	8.2%	✗
TERO-8 (1st device)	53.4% (53%)	✓	97.6% (97.7%)	✓	49.4%	✓

Results • 33 Devices • Bit-aliasing

Bit-aliasing

- Ideally follows a binormal distribution around **50%**

TERO-4

- Highly shifted toward **0**
- Not following a binormal

TERO-8

- Slightly shifted toward **1**
- Binormal centered on **53.5%**

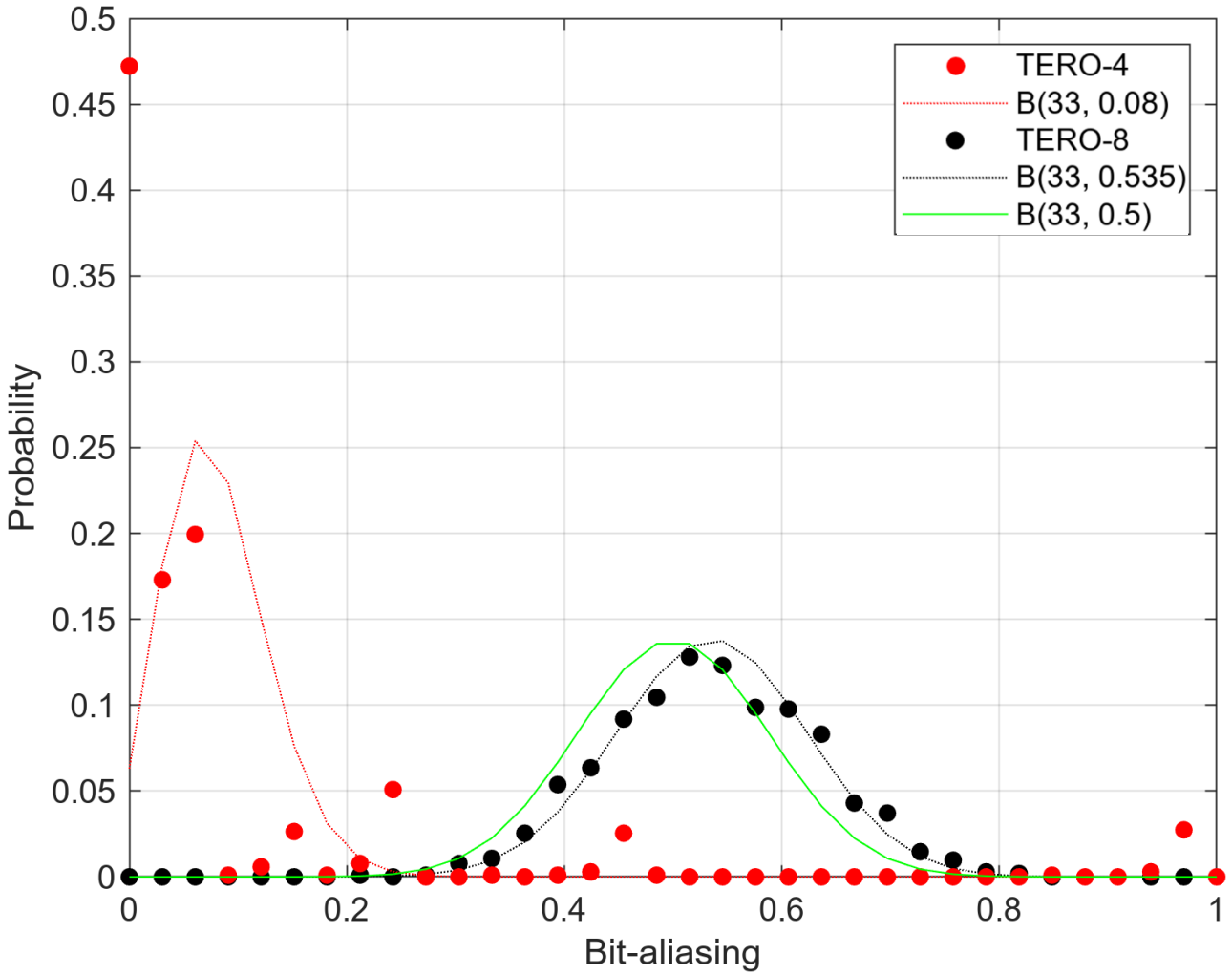


Figure 11: Bit-aliasing

Results • Error correction

PUF
- **Full response**
- 1023 bits

Pre-decoder
- **Reduced response**
- 171 first bits

Decoder
- **ECC response**
- 171 corrected bits

TERO-8	Size	Avr uniformity	Avr reliability	Uniqueness	Bit-aliasing
Full	1023	53.4%	**97.6%**	49.4%	53.5%
Reduced	171	53.4%	**97.7%**	49.9%	54.4%
ECC	171	53.5%	**99.9%**	49.9%	54.4%

Results • Comparison

Method	TERO-8 (This study)		XOR-APUF	BST-APUF	RO-PUF	BST-ROPUF	RWC-SRAM	Flip-Flop PUF	TERO	TERO	TERO		PDL-TERO
	Raw	Ecc											
Reliability	**97.6%**	**99.9%**	99.4%	99.9%	99.2%	99.9%	98.9%	99%	98.3%	99.9%	97.4%	98.2%	98.8%
Uniformity	**53.4%**	**53.5%**	50.7%	*N/A*	51.0%	46.8%	55.4%	49.2%	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Uniqueness	**49.4%**	**49.9%**	48.7%	49.1%	47.9%	48.6%	37.4%	*N/A*	48%	46.7%	48.5%	47.6%	49.3%
Bit-aliasing	**53.5%**	**54.4%**	*N/A*	50.3%	51.0%	*N/A*	46.9%	48.7%	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Device	**Artix-7**		Artix-7	Artix-7	Artix-7	Artix-7	Artix-7	Artix-7	Cyclon-II	Altera DE2	Spartan-6	Spartan-V	Spartan-3

Conclusion

Objectives

- ✓ **1 control logic block** per cell
- ✓ SOTA performances over **33 devices**

} **TERO-8**

- ✓ **Error correction** to improve reliability
- ✓ **Key hashing**
- ✗ **Ciphering**

Futur work

- **Onboard ciphering**
- **Variability** (temperature, voltage, …)
- **Larger** cells

Questions

Questions ?

Appendices • Response generation methods

Direct method

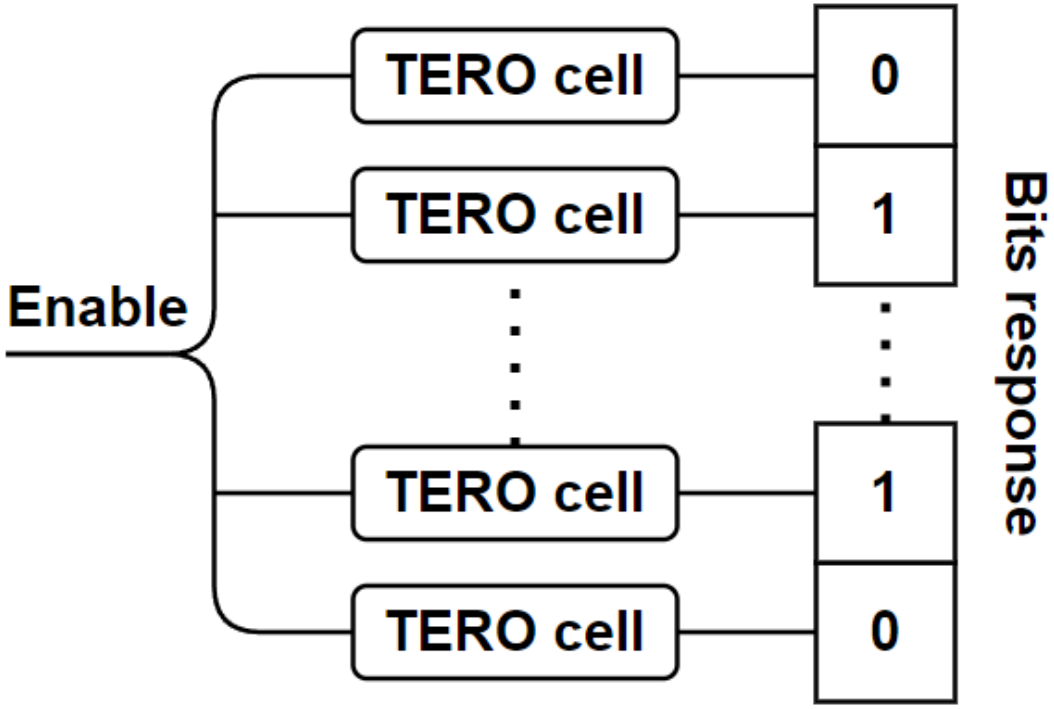


Figure 12: Direct method

Comparison method

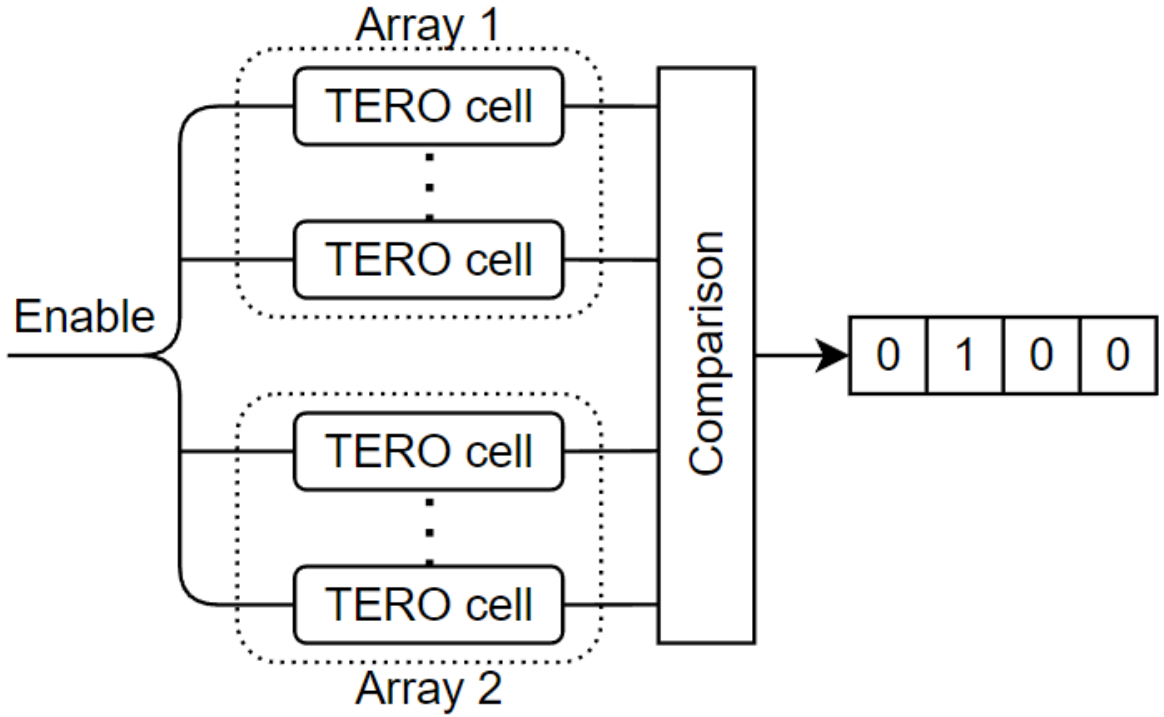


Figure 13: Comparison method

Appendices • Final oscillations

TERO-4

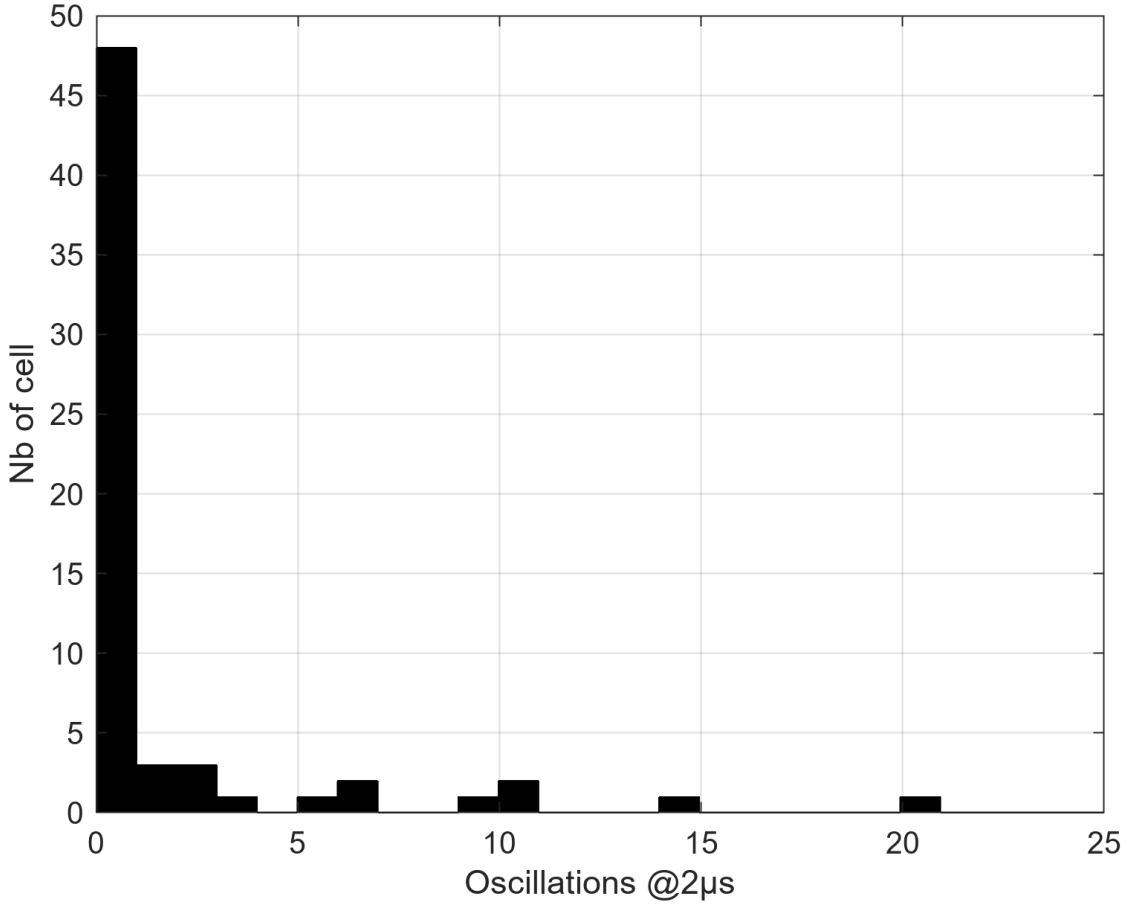


Figure 14: TERO-4 final oscillations

TERO-8

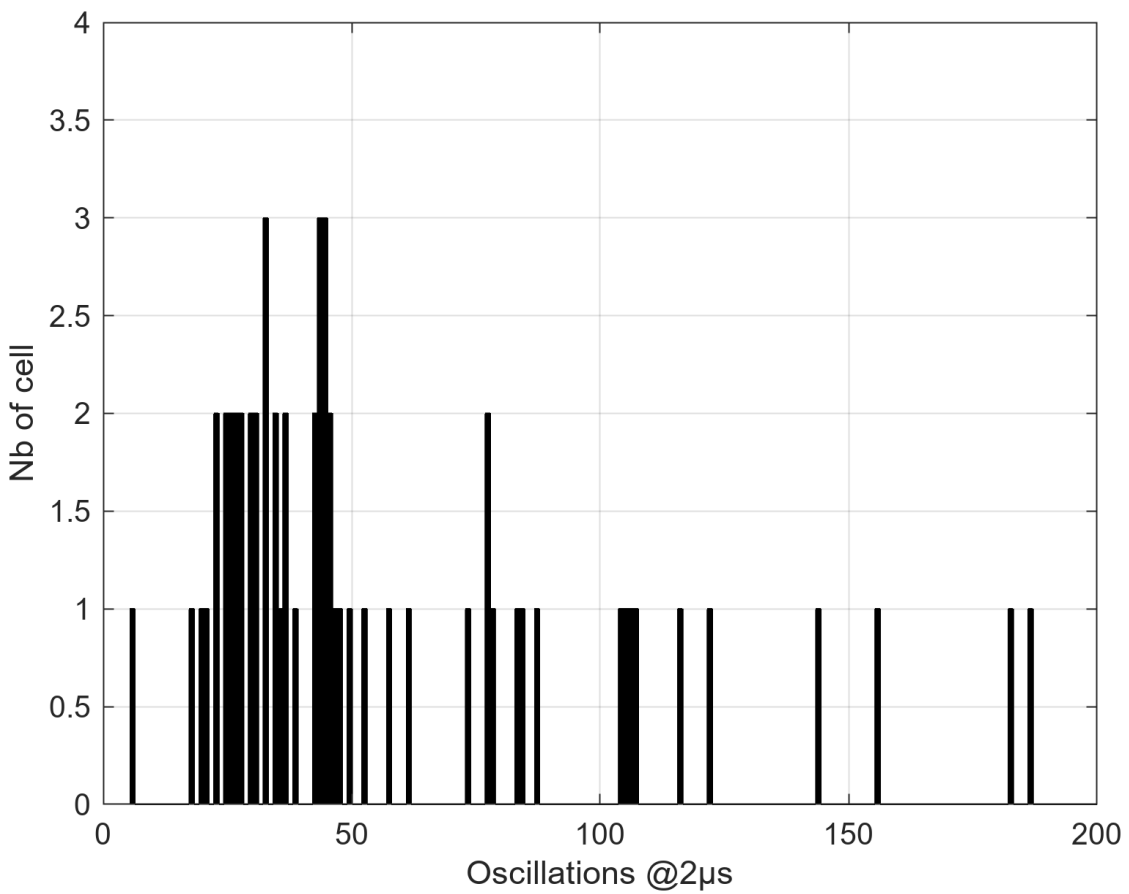


Figure 15: TERO-8 final oscillations

Appendices • Inter-device deviation

Uniformities

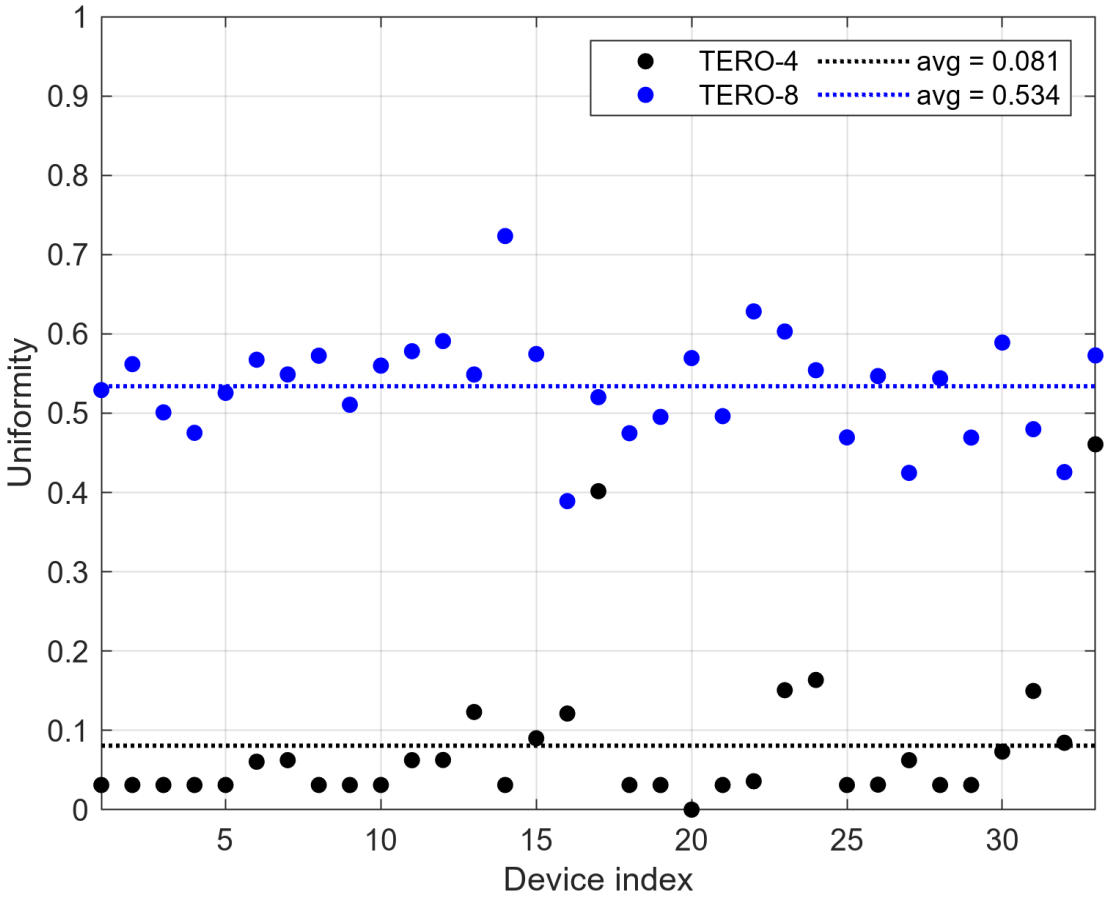


Figure 16: Uniformities

Reliabilities

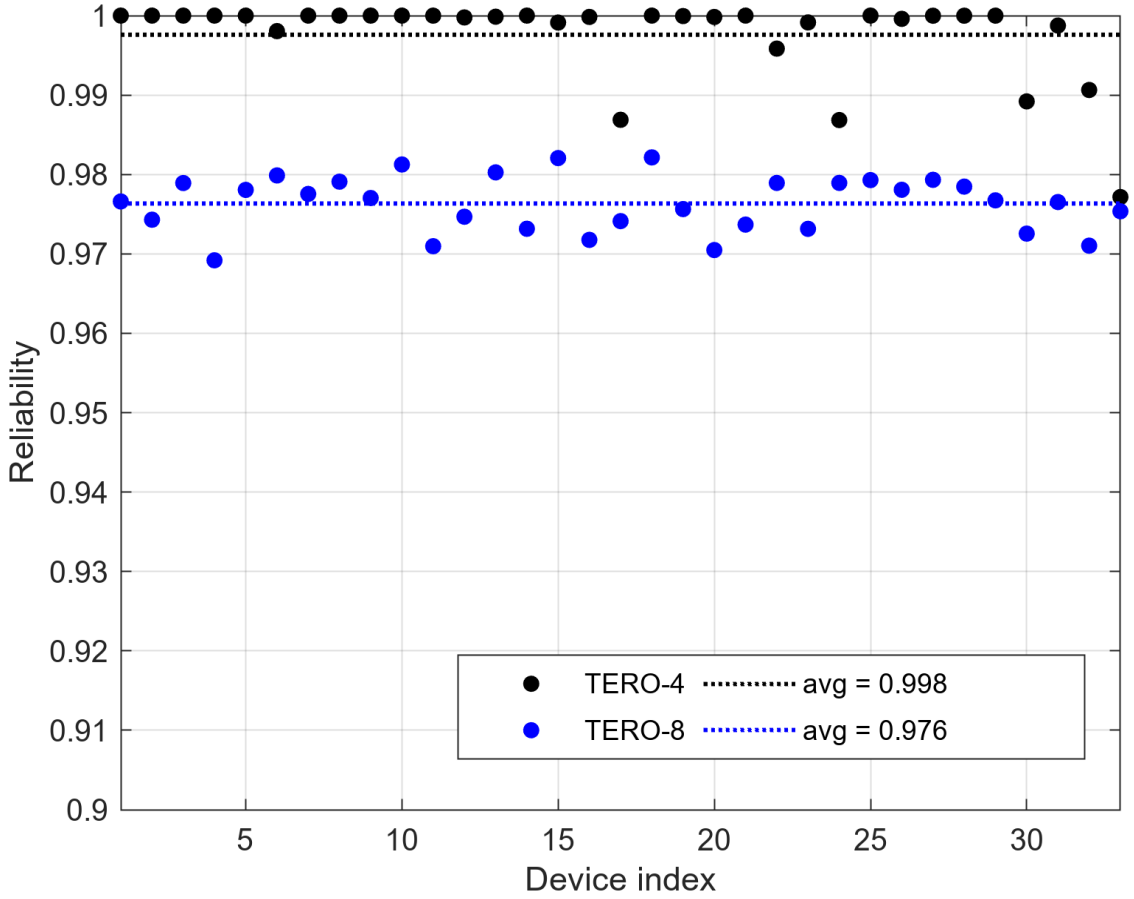


Figure 17: Reliabilities

Appendices • LSFR cell occurency

TERO-8	Size	Uniformity	Reliability	Uniqueness	Bit-aliasing
Full	1023 bits	53.4%	97.6%	49.4%	53.5%
Reduced	171 bits	53.4%	97.6%	49.9%	54.4%

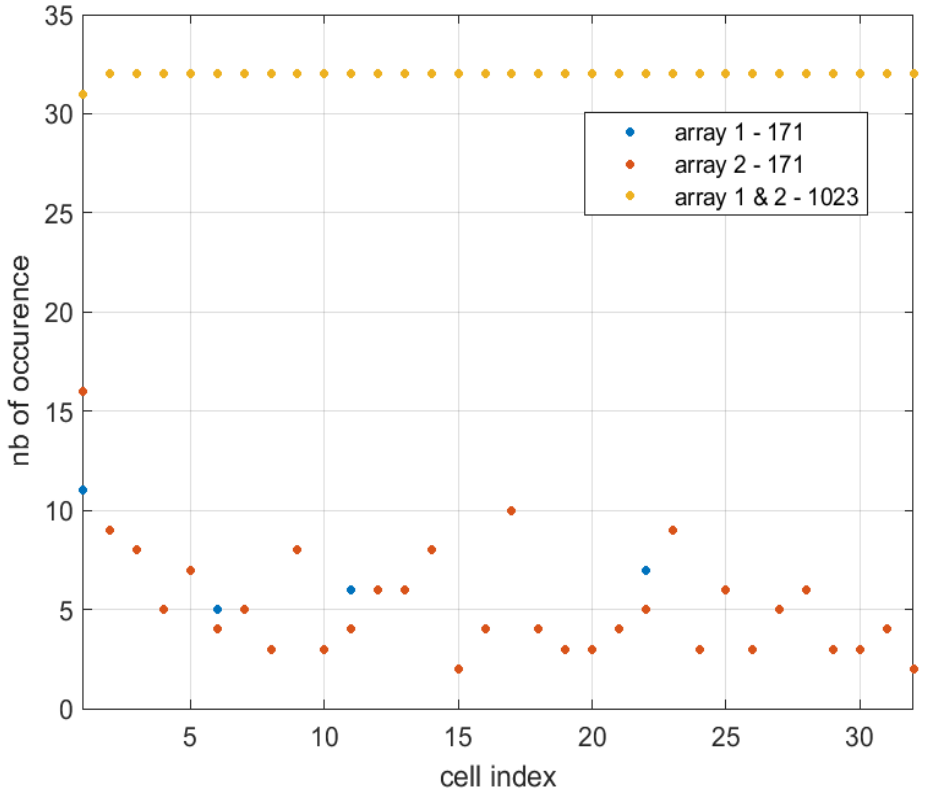


Figure 18: LSFR Cell occurency

Appendices • FPGA usage • Area

	LUTs		FFs	
	TERO-4	**TERO-8**	**TERO-4**	**TERO-8**
TERO block	**428** (11%)	**684** (16%)	**162** (5%)	**162** (5%)
BCH decoder	**797** (20%)	**797** (19%)	**981** (29%)	**981** (29%)
SHA-256	**895** (23%)	**895** (21%)	**950** (28%)	**950** (28%)
Control & UART	**1792** (46%)	**1792** (43%)	**1308** (38%)	**1308** (38%)
Total	**3912**	**4168**	**3401**	**3401**

Figure 19: Area usage

Appendices • FPGA usage • Power

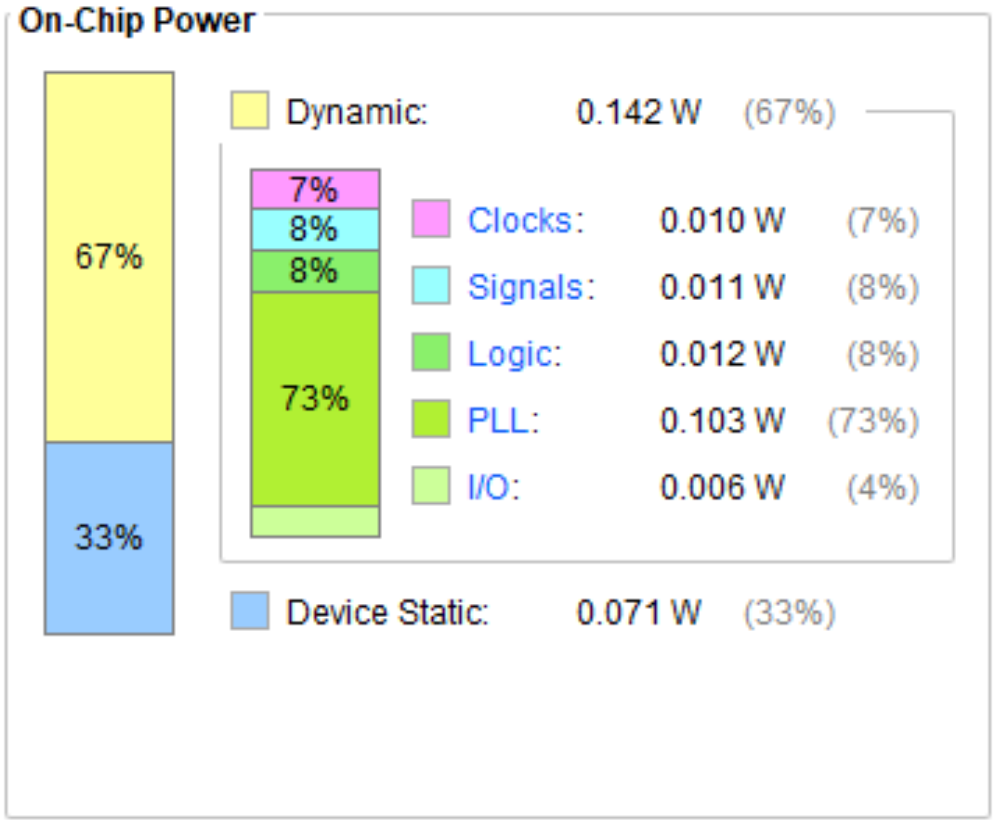


Figure 20: Power usage