POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

TERO PUF Implementation on Xilinx Artix7 FPGA

PROJECT REPORT FOR EMBEDDED SYSTEMS COURSE

Aspesi Andrea, 962608
Putortì Alessandro, 953258

Abstract: Physical Unclonable Functions (PUFs) are becoming important in recent years for various purposes such as Device Identification, True Random Number Generators, Cryptographic Key Generators, IP Protection. Diffent ways of realizing PUFs have been proposed in literature, exploiting process variations occurring inside chips. Among them, some can be efficiently implemented in FPGAs: in our project, after analyzing the state of the art, we chose to implement a Transient Effect Ring Oscillator (TERO) PUF. TERO PUF offers high resistance to surrounding logic influence and temperature changes, providing at the same time high uniqueness and reliability. As target, we chose Basys3 boards from Digilent, shipped with Xilinx Artix7 XC7-A35T.

1. Introduction

Lorem ipsum **dolor** sit amet, consectetur adipiscing elit. Suspendisse facilisis ac erat vitae luctus. Aliquam in faucibus urna. Nulla ullamcorper tristique odio eu euismod. Nunc porta euismod orci vel ornare. Suspendisse suscipit non orci non blandit. In est massa, blandit sed metus non, commodo euismod leo. Nunc nec purus sed est imperdiet lacinia. Nullam convallis lectus neque, nec gravida **dolor** semper vel.

Donec quam odio, pulvinar sit amet ipsum et, volutpat ullamcorper ex. Quisque porta, justo nec tempor ornare, leo mauris iaculis ex, sit amet pellentesque quam mi eget neque. Phasellus maximus bibendum sem non pharetra. Morbi elementum tempor sem in scelerisque. Curabitur egestas pharetra libero eget bibendum. Aenean sit amet molestie risus. Quisque ac sodales elit. Nulla tincidunt ac augue vitae malesuada. Proin eget sagittis arcu, non molestie nibh. Nullam in nulla sit amet lacus semper molestie eget eget turpis. Nunc vel urna sit amet nisl facilisis pulvinar in fermentum ligula. Morbi sollicitudin laoreet est eget pharetra. Quisque laoreet porta sem, quis fermentum leo mollis at.

In facilisis viverra felis, a dapibus mauris maximus sed. Curabitur ut eros a odio mollis fermentum vel vel eros. Donec id vestibulum erat, sit amet laoreet urna. Suspendisse aliquam, sapien quis suscipit dapibus, ligula nisl lacinia sem, in tempus neque quam et turpis. Nulla facilisi. Donec malesuada odio sit amet est egestas, in sollicitudin lorem vehicula. Quisque nec dictum quam, vitae tincidunt est. Curabitur id elit fringilla, tincidunt augue ac, pellentesque **dolor**. Vivamus leo sapien, eleifend eget diam a, porttitor ullamcorper arcu. Donec dignissim ipsum vel sapien porttitor, tincidunt placerat **dolor** condimentum. Aenean non elementum orci, id molestie nunc. Donec pharetra arcu sem, mollis maximus massa pretium ut. Duis sed congue libero, eu laoreet tortor. Phasellus sed consectetur nisl. Nulla interdum ligula eu placerat porttitor.

2. Design

Lorem ipsum **dolor** sit amet, consectetur adipiscing elit. Suspendisse facilisis ac erat vitae luctus. Aliquam in faucibus urna. Nulla ullamcorper tristique odio eu euismod. Nunc porta euismod orci vel ornare. Suspendisse suscipit non orci non blandit. In est massa, blandit sed metus non, commodo euismod leo. Nunc nec purus sed est imperdiet lacinia. Nullam convallis lectus neque, nec gravida **dolor** semper vel.

Donec quam odio, pulvinar sit amet ipsum et, volutpat ullamcorper ex. Quisque porta, justo nec tempor ornare, leo mauris iaculis ex, sit amet pellentesque quam mi eget neque. Phasellus maximus bibendum sem non pharetra. Morbi elementum tempor sem in scelerisque. Curabitur egestas pharetra libero eget bibendum. Aenean sit amet molestie risus. Quisque ac sodales elit. Nulla tincidunt ac augue vitae malesuada. Proin eget sagittis arcu, non molestie nibh. Nullam in nulla sit amet lacus semper molestie eget eget turpis. Nunc vel urna sit amet nisl facilisis pulvinar in fermentum ligula. Morbi sollicitudin laoreet est eget pharetra. Quisque laoreet porta sem, quis fermentum leo mollis at.

In facilisis viverra felis, a dapibus mauris maximus sed. Curabitur ut eros a odio mollis fermentum vel vel eros. Donec id vestibulum erat, sit amet laoreet urna. Suspendisse aliquam, sapien quis suscipit dapibus, ligula nisl lacinia sem, in tempus neque quam et turpis. Nulla facilisi. Donec malesuada odio sit amet est egestas, in sollicitudin lorem vehicula. Quisque nec dictum quam, vitae tincidunt est. Curabitur id elit fringilla, tincidunt augue ac, pellentesque **dolor**. Vivamus leo sapien, eleifend eget diam a, porttitor ullamcorper arcu. Donec dignissim ipsum vel sapien porttitor, tincidunt placerat **dolor** condimentum. Aenean non elementum orci, id molestie nunc. Donec pharetra arcu sem, mollis maximus massa pretium ut. Duis sed congue libero, eu laoreet tortor. Phasellus sed consectetur nisl. Nulla interdum ligula eu placerat porttitor.

3. ID Generation

Lorem ipsum **dolor** sit amet, consectetur adipiscing elit. Suspendisse facilisis ac erat vitae luctus. Aliquam in faucibus urna. Nulla ullamcorper tristique odio eu euismod. Nunc porta euismod orci vel ornare. Suspendisse suscipit non orci non blandit. In est massa, blandit sed metus non, commodo euismod leo. Nunc nec purus sed est imperdiet lacinia. Nullam convallis lectus neque, nec gravida **dolor** semper vel.

Donec quam odio, pulvinar sit amet ipsum et, volutpat ullamcorper ex. Quisque porta, justo nec tempor ornare, leo mauris iaculis ex, sit amet pellentesque quam mi eget neque. Phasellus maximus bibendum sem non pharetra. Morbi elementum tempor sem in scelerisque. Curabitur egestas pharetra libero eget bibendum. Aenean sit amet molestie risus. Quisque ac sodales elit. Nulla tincidunt ac augue vitae malesuada. Proin eget sagittis arcu, non molestie nibh. Nullam in nulla sit amet lacus semper molestie eget eget turpis. Nunc vel urna sit amet nisl facilisis pulvinar in fermentum ligula. Morbi sollicitudin laoreet est eget pharetra. Quisque laoreet porta sem, quis fermentum leo mollis at.

In facilisis viverra felis, a dapibus mauris maximus sed. Curabitur ut eros a odio mollis fermentum vel vel eros. Donec id vestibulum erat, sit amet laoreet urna. Suspendisse aliquam, sapien quis suscipit dapibus, ligula nisl lacinia sem, in tempus neque quam et turpis. Nulla facilisi. Donec malesuada odio sit amet est egestas, in sollicitudin lorem vehicula. Quisque nec dictum quam, vitae tincidunt est. Curabitur id elit fringilla, tincidunt augue ac, pellentesque **dolor**. Vivamus leo sapien, eleifend eget diam a, porttitor ullamcorper arcu. Donec dignissim ipsum vel sapien porttitor, tincidunt placerat **dolor** condimentum. Aenean non elementum orci, id molestie nunc. Donec pharetra arcu sem, mollis maximus massa pretium ut. Duis sed congue libero, eu laoreet tortor. Phasellus sed consectetur nisl. Nulla interdum ligula eu placerat porttitor.

4. Results

Lorem ipsum **dolor** sit amet, consectetur adipiscing elit. Suspendisse facilisis ac erat vitae luctus. Aliquam in faucibus urna. Nulla ullamcorper tristique odio eu euismod. Nunc porta euismod orci vel ornare. Suspendisse suscipit non orci non blandit. In est massa, blandit sed metus non, commodo euismod leo. Nunc nec purus sed est imperdiet lacinia. Nullam convallis lectus neque, nec gravida **dolor** semper vel.

Donec quam odio, pulvinar sit amet ipsum et, volutpat ullamcorper ex. Quisque porta, justo nec tempor ornare, leo mauris iaculis ex, sit amet pellentesque quam mi eget neque. Phasellus maximus bibendum sem non pharetra. Morbi elementum tempor sem in scelerisque. Curabitur egestas pharetra libero eget bibendum. Aenean sit amet molestie risus. Quisque ac sodales elit. Nulla tincidunt ac augue vitae malesuada. Proin eget sagittis arcu, non molestie nibh. Nullam in nulla sit amet lacus semper molestie eget eget turpis. Nunc vel urna sit amet nisl facilisis pulvinar in fermentum ligula. Morbi sollicitudin laoreet est eget pharetra. Quisque laoreet porta sem, quis fermentum leo mollis at.

In facilisis viverra felis, a dapibus mauris maximus sed. Curabitur ut eros a odio mollis fermentum vel vel eros. Donec id vestibulum erat, sit amet laoreet urna. Suspendisse aliquam, sapien quis suscipit dapibus, ligula nisl lacinia sem, in tempus neque quam et turpis. Nulla facilisi. Donec malesuada odio sit amet est egestas, in sollicitudin lorem vehicula. Quisque nec dictum quam, vitae tincidunt est. Curabitur id elit fringilla, tincidunt augue ac, pellentesque **dolor**. Vivamus leo sapien, eleifend eget diam a, porttitor ullamcorper arcu. Donec dignissim ipsum vel sapien porttitor, tincidunt placerat **dolor** condimentum. Aenean non elementum orci, id molestie nunc. Donec pharetra arcu sem, mollis maximus massa pretium ut. Duis sed congue libero, eu laoreet tortor. Phasellus sed consectetur nisl. Nulla interdum ligula eu placerat porttitor.

5. Introduction

This document is intended to be both an example of the Polimi LaTeX template for Master Theses in article format, as well as a short introduction to its use. It is not intended to be a general introduction to LaTeX itself, and the reader is assumed to be familiar with the basics of creating and compiling LaTeX documents (see [5, 7]). The cover page of the thesis in article format must contain all the relevant information: title of the thesis, name of the Study Programme, name(s) of the author(s), student ID number, name of the supervisor, name(s) of the co-supervisor(s) (if any), academic year.

Be sure to select a title that is meaningful. It should contain important keywords to be identified by indexer. Keep the title as concise as possible and comprehensible even to people who are not experts in your field. The title has to be chosen at the end of your work so that it accurately captures the main subject of the manuscript. It is convenient to break the article format of your thesis (in article format) into sections and subsections. If necessary, subsubsections, paragraphs and subparagraphs can be used. A new section is created by the command

`\section{Title of the section}`

The numbering can be turned off by using `\section*{}`. A new subsection is created by the command

`\subsection{Title of the subsection}`

and, similarly, the numbering can be turned off by adding an asterisk as follows

`\subsection*{}`

It is recommended to give a label to each section by using the command

`\label{sec:section_name}%`

where the argument is just a text string that you'll use to reference that part as follows: *Section 5 contains* INTRODUCTION . . . .

6. Equations

This section gives some examples of writing mathematical equations in your thesis.
Maxwell's equations read:

$$
\begin{cases}
\nabla \cdot \boldsymbol{D} = \rho, & \text{(1a)} \\[2mm]
\nabla \times \boldsymbol{E} + \dfrac{\partial \boldsymbol{B}}{\partial t} = \boldsymbol{0}, & \text{(1b)} \\[2mm]
\nabla \cdot \boldsymbol{B} = 0, & \text{(1c)} \\[2mm]
\nabla \times \boldsymbol{H} - \dfrac{\partial \boldsymbol{D}}{\partial t} = \boldsymbol{J}. & \text{(1d)}
\end{cases}
$$

Equation (1) is automatically labeled by `cleveref`, as well as Equation (1a) and Equation (1c). Thanks to the `cleveref` package, there is no need to use `\eqref`. Equations have to be numbered only if they are referenced in the text.
Equations (2), (3), (4), and (5) show again Maxwell's equations without brace:

$$\nabla \cdot \boldsymbol{D} = \rho, \tag{2}$$

$$\nabla \times \boldsymbol{E} + \frac{\partial \boldsymbol{B}}{\partial t} = \boldsymbol{0}, \tag{3}$$

$$\nabla \cdot \boldsymbol{B} = 0, \tag{4}$$

$$\nabla \times \boldsymbol{H} - \frac{\partial \boldsymbol{D}}{\partial t} = \boldsymbol{J}. \tag{5}$$

Equation (6) is the same as before, but with just one label:

$$
\begin{cases}
\nabla \cdot \boldsymbol{D} = \rho, \\[2mm]
\nabla \times \boldsymbol{E} + \dfrac{\partial \boldsymbol{B}}{\partial t} = \boldsymbol{0}, \\[2mm]
\nabla \cdot \boldsymbol{B} = 0, \\[2mm]
\nabla \times \boldsymbol{H} - \dfrac{\partial \boldsymbol{D}}{\partial t} = \boldsymbol{J}.
\end{cases}
\tag{6}
$$

7. Figures, Tables and Algorithms

Figures, Tables and Algorithms have to contain a Caption that describes their content, and have to be properly referred in the text.

7.1. Figures

For including pictures in your text you can use `TikZ` for high-quality hand-made figures [2], or just include them with the command

`\includegraphics[options]{filename.xxx}`

Here xxx is the correct format, e.g. `.png`, `.jpg`, `.eps`, ...

Figure 1: Caption of the Figure.

Thanks to the `\subfloat` command, a single figure, such as Figure 1, can contain multiple sub-figures with their own caption and label, e.g. Figure 2a and Figure 2b.

(a) One PoliMi logo.   (b) Another one PoliMi logo.

Figure 2: Caption of the Figure.

7.2. Tables

Within the environments `table` and `tabular` you can create very fancy tables as the one shown in Table 1.

Example of Table (optional)

	column1	column2	column3
row1	1	2	3
row2	α	β	γ
row3	alpha	beta	gamma

Table 1: Caption of the Table.

You can also consider to highlight selected columns or rows in order to make tables more readable. Moreover, with the use of `table*` and the option `bp` it is possible to align them at the bottom of the page. One example is presented in Table 2.

7.3. Algorithms

Pseudo-algorithms can be written in LaTeX with the `algorithm` and `algorithmic` packages. An example is shown in Algorithm 1.

Algorithm 1 Name of the Algorithm

1: Initial instructions
2: **for** $for - condition$ **do**
3:     Some instructions
4:     **if** $if - condition$ **then**
5:         Some other instructions
6:     **end if**
7: **end for**
8: **while** $while - condition$ **do**
9:     Some further instructions
10: **end while**
11: Final instructions
---

8.   Some further useful suggestions

Theorems have to be formatted as follows:

Theorem 8.1. *Write here your theorem.*

Proof. If useful you can report here the proof.

Propositions have to be formatted as follows:

Proposition 8.1. *Write here your proposition.*

How to insert itemized lists:
- first item;
- second item.

How to write numbered lists:
1. first item;
2. second item.

9.   Use of copyrighted material

Each student is responsible for obtaining copyright permissions, if necessary, to include published material in the thesis. This applies typically to third-party material published by someone else.

	column1	column2	column3	column4	column5	column6
row1	1	2	3	4	5	6
row2	a	b	c	d	e	f
row3	α	β	γ	δ	ϕ	ω
row4	alpha	beta	gamma	delta	phi	omega

Table 2: Highlighting the columns

10. Plagiarism

You have to be sure to respect the rules on Copyright and avoid an involuntary plagiarism. It is allowed to take other persons' ideas only if the author and his original work are clearly mentioned. As stated in the Code of Ethics and Conduct, Politecnico di Milano *promotes the integrity of research, condemns manipulation and the infringement of intellectual property*, and gives opportunity to all those who carry out research activities to have an adequate training on ethical conduct and integrity while doing research. To be sure to respect the copyright rules, read the guides on Copyright legislation and citation styles available at:

`https://www.biblio.polimi.it/en/tools/courses-and-tutorials`

You can also attend the courses which are periodically organized on "Bibliographic citations and bibliography management".

11. Conclusions

A final section containing the main conclusions of your research/study and possible future developments of your work have to be inserted in the section "Conclusions".

12. Bibliography and citations

Your thesis must contain a suitable Bibliography which lists all the sources consulted on developing the work. The list of references is placed at the end of the manuscript after the chapter containing the conclusions. It is suggested to use the BibTeX package and save the bibliographic references in the file `bibliography.bib`. This is indeed a database containing all the information about the references. To cite in your manuscript, use the `\cite{}` command as follows:
Here is how you cite bibliography entries: [3], or multiple ones at once: [4, 6].
The bibliography and list of references are generated automatically by running BibTeX [1].

References

[1] CTAN. BiBTeX documentation.

[2] CTAN. pgf – create PostScript and PDF graphics in TEX.

[3] Donald E. Knuth. Computer programming as an art. *Commun. ACM*, pages 667–673, 1974.

[4] Donald E. Knuth. Two notes on notation. *Amer. Math. Monthly*, 99:403–422, 1992.

[5] Stefan Kottwitz. *LaTeX Cookbook*. Packt Publishing Ltd, 2015.

[6] Leslie Lamport. *LaTeX: A Document Preparation System*. Pearson Education India, 1994.

[7] Tobias Oetiker, Hubert Partl, Irene Hyna, and Elisabeth Schlegl. The not so short introduction to latex2ε. *Electronic document available at http://www. tex. ac. uk/tex-archive/info/lshort*, 1995.

A. Appendix A

If you need to include an appendix to support the research in your thesis, you can place it at the end of the manuscript. An appendix contains supplementary material (figures, tables, data, codes, mathematical proofs, surveys, ...) which supplement the main results contained in the previous sections.

B. Appendix B

It may be necessary to include another appendix to better organize the presentation of supplementary material.

Abstract in lingua italiana

Qui va l'Abstract in lingua italiana della tesi seguito dalla lista di parole chiave.

Parole chiave: qui, le parole chiave, della tesi, in italiano

Acknowledgements