AES Hardware Accelerator design using PicoRV32 RISC-V Core

Ufuk Resul YILDIRIM (21788985)

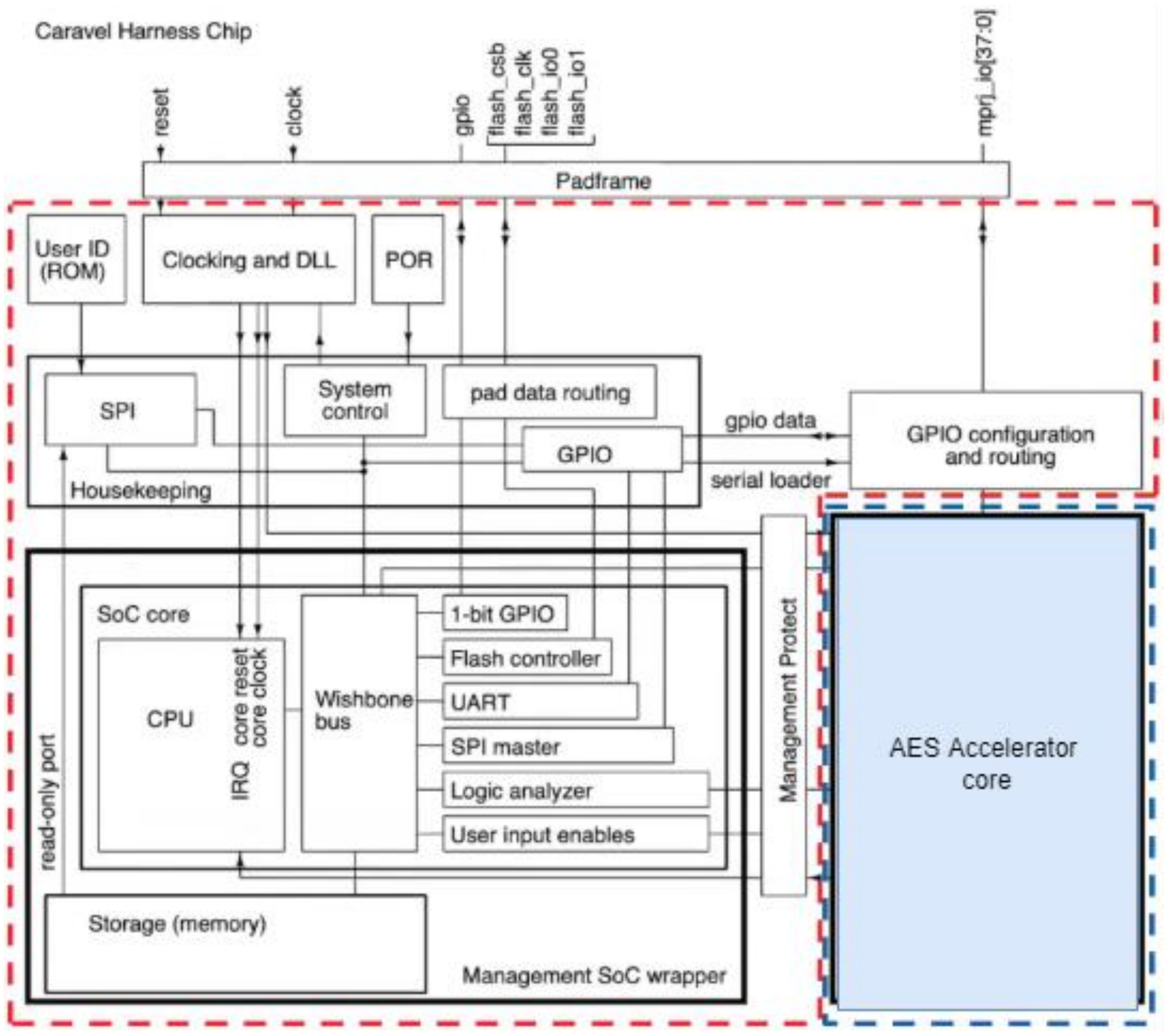
Supervisor
Professor Ali Ziya ALKAR
Electrical and Electronics Engineering, Hacettepe University

Introduction

- ❖ In this project we implemented a Block Cipher algorithm in accelerator fashion on Efabless' Caravel SoC which includes an RISC-V CPU PicoRV32.
- ❖ All tools, compilers, simulators and IPs that are used in this project are **open-source** and completely free.
- ❖ Output of the project (GDS) is the final output of an ASIC design flow and is **ready to tape-out**.
- ❖ We have submitted our project to Efabless's Open MPW-6 Shuttle Program, which is funded by Google, with the name of '**HUEE AES Accelerator**' and hopefully we will obtain chip form of the design which is fabricated using Skywater's 130nm technology.

Specifications

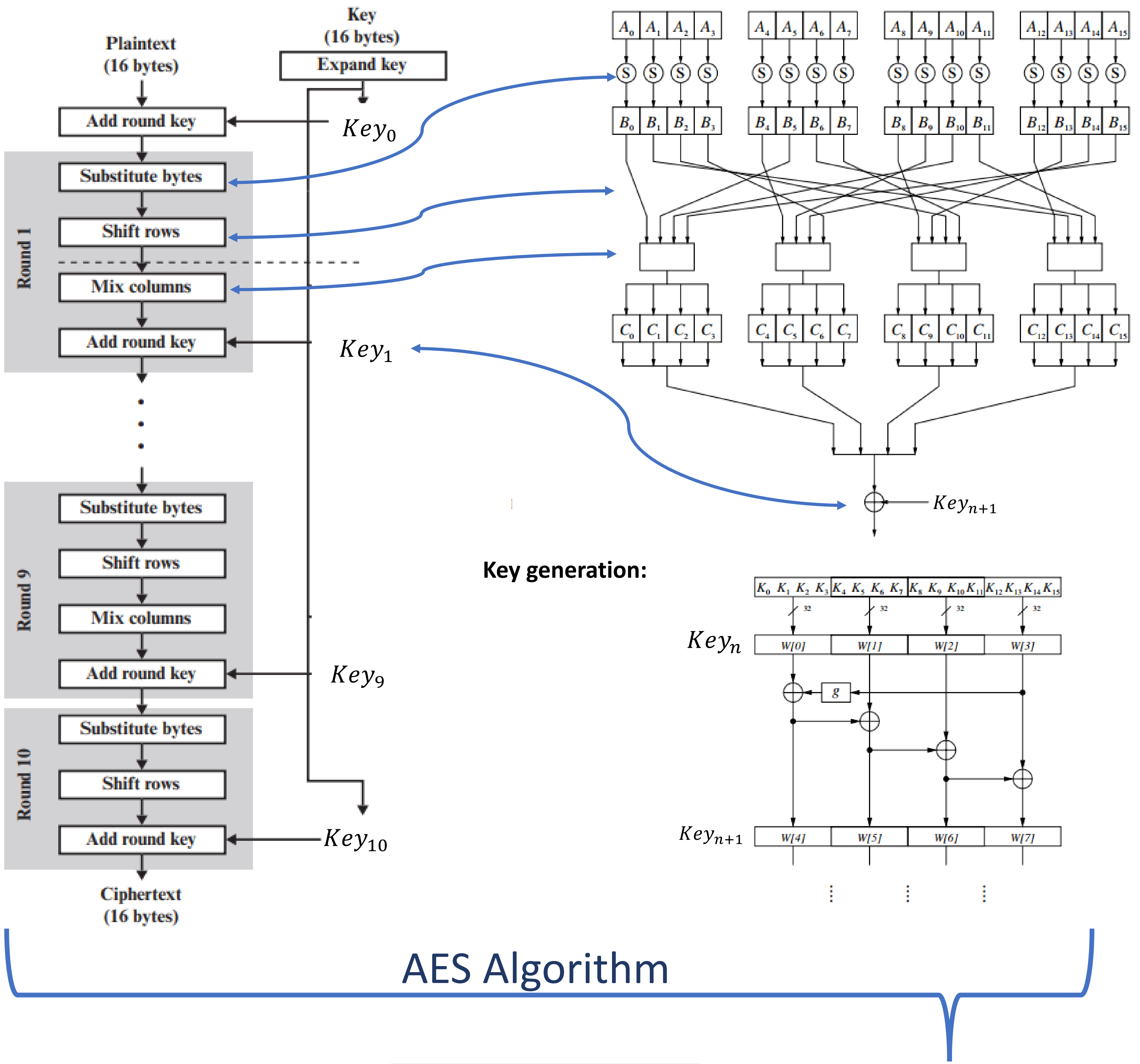
- ❖ It takes 67 clock cycles to encrypt/decrypt.
- ❖ We used Direct Bus Access method for acceleration due to design requirements.
- ❖ In essence we are reaching to a specific address on main memory of the PicoRV32 using Wishbone interface and getting commands, plaintexts and key from CPU and writing back when the encryption/decryption process is completed.

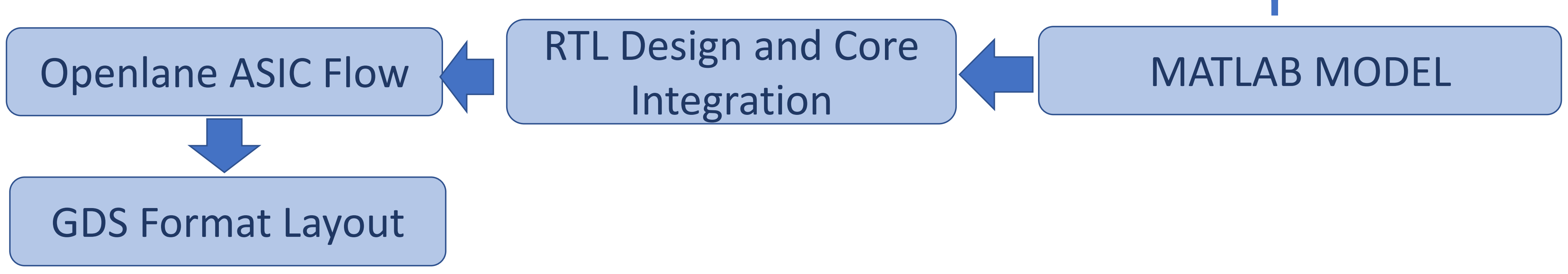


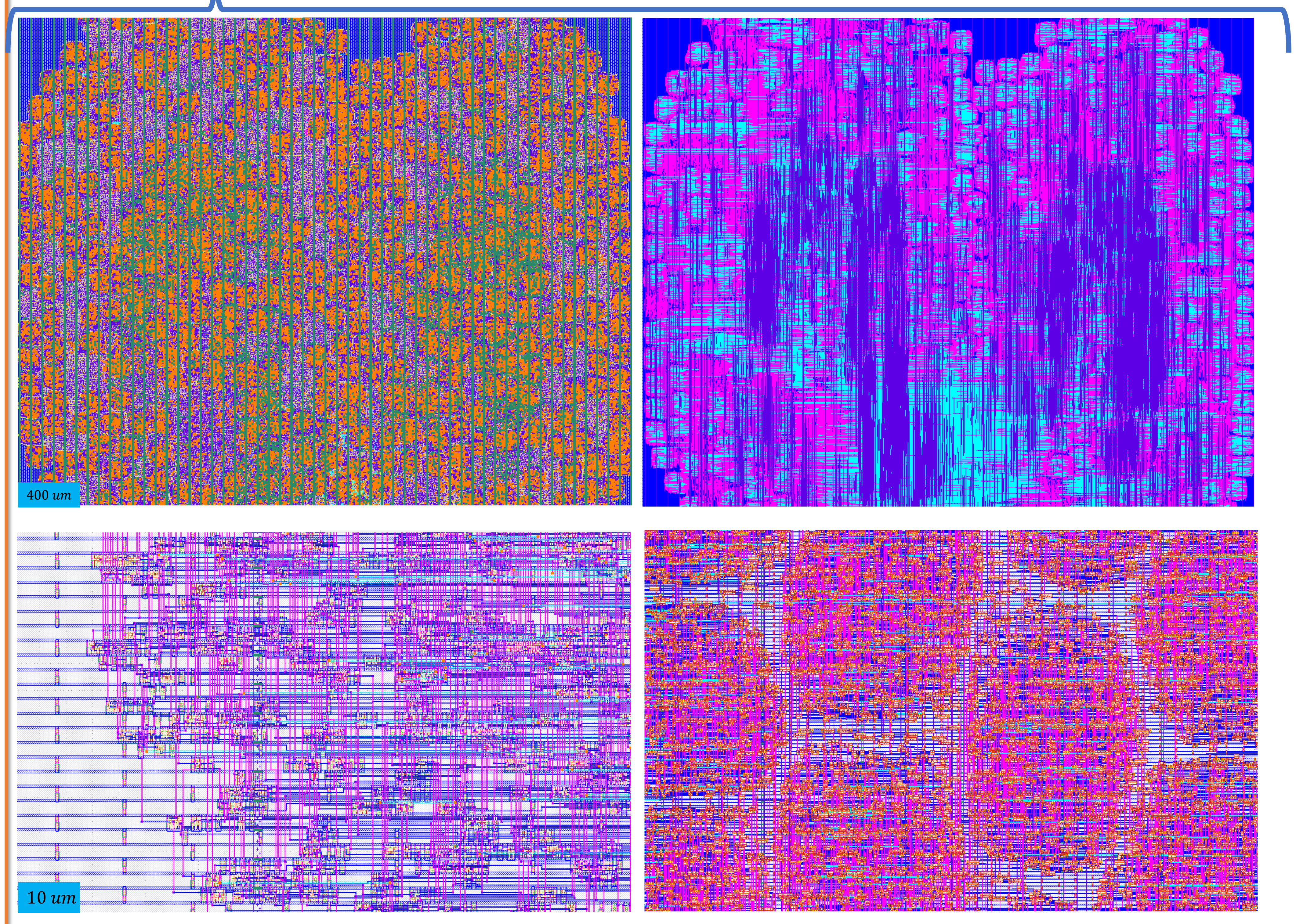
- ❖ The accelerator unit has a non-pipelined architecture in accordance with its design specifications. Hence it ended up with a clock frequency of 25 MHz which is was relatively lower.
- ❖ Final layout specifications can be briefly listed as:
  - ❖ Total number of cells : 308054
  - ❖ 7.696 D Flip-flops, 1.408 NAND, 366.324 OR, 12.000 AND, 17.867 XOR, 4.440 XNOR gates, 596 MUXs , 3.198.158 Vias
  - ❖ DIE area : 17.57 mm^2
  - ❖ Core Utilization : 111.888 $cells/mm^2$

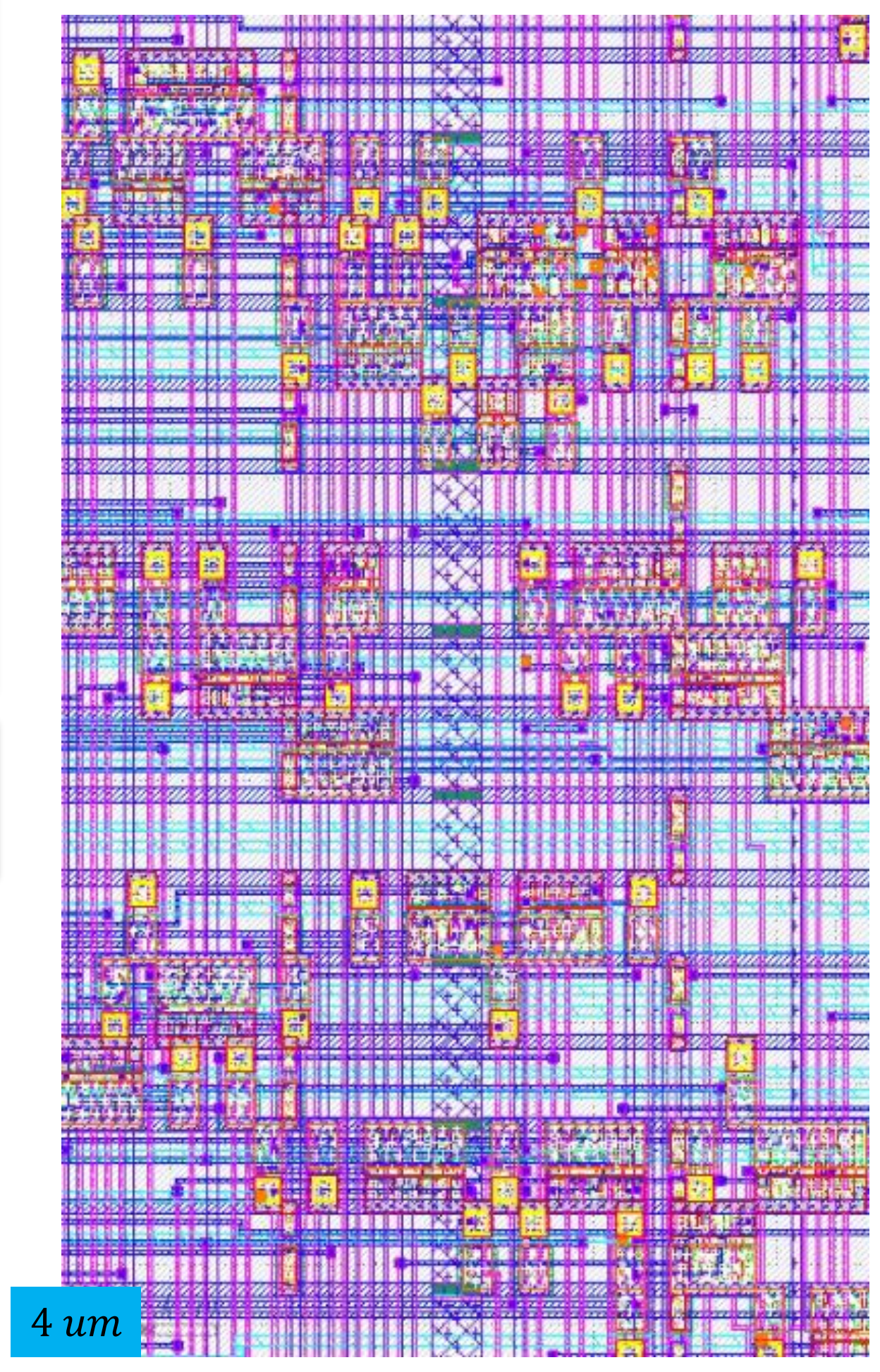
Acknowledgements

❖This project was completed within the context of ELE401-401 Graduation Project courses in Hacettepe University, Faculty of Engineering, Department of Electrical and Electronics Engineering. We thank Prof. Ali Ziya ALKAR for his invaluable contributions to our project.

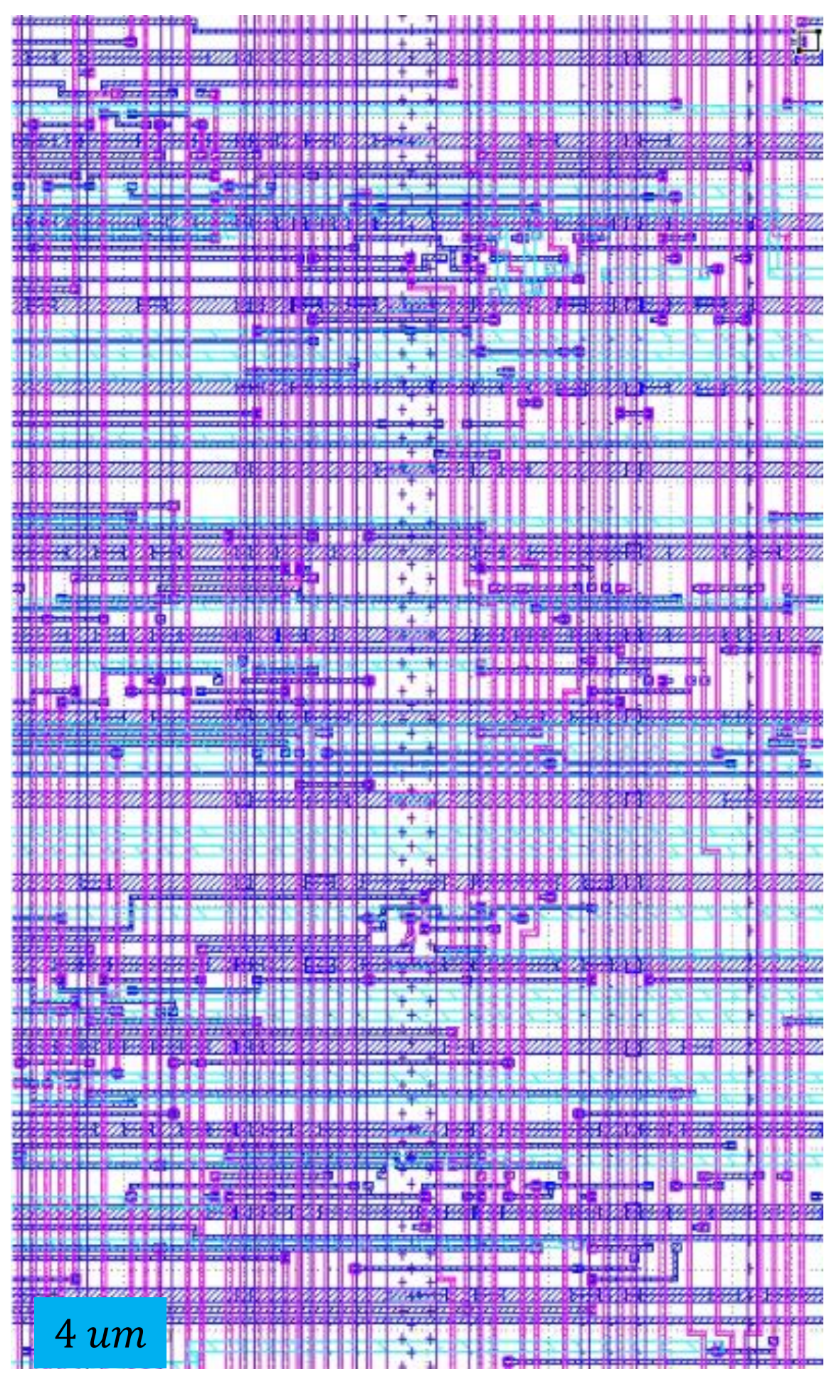




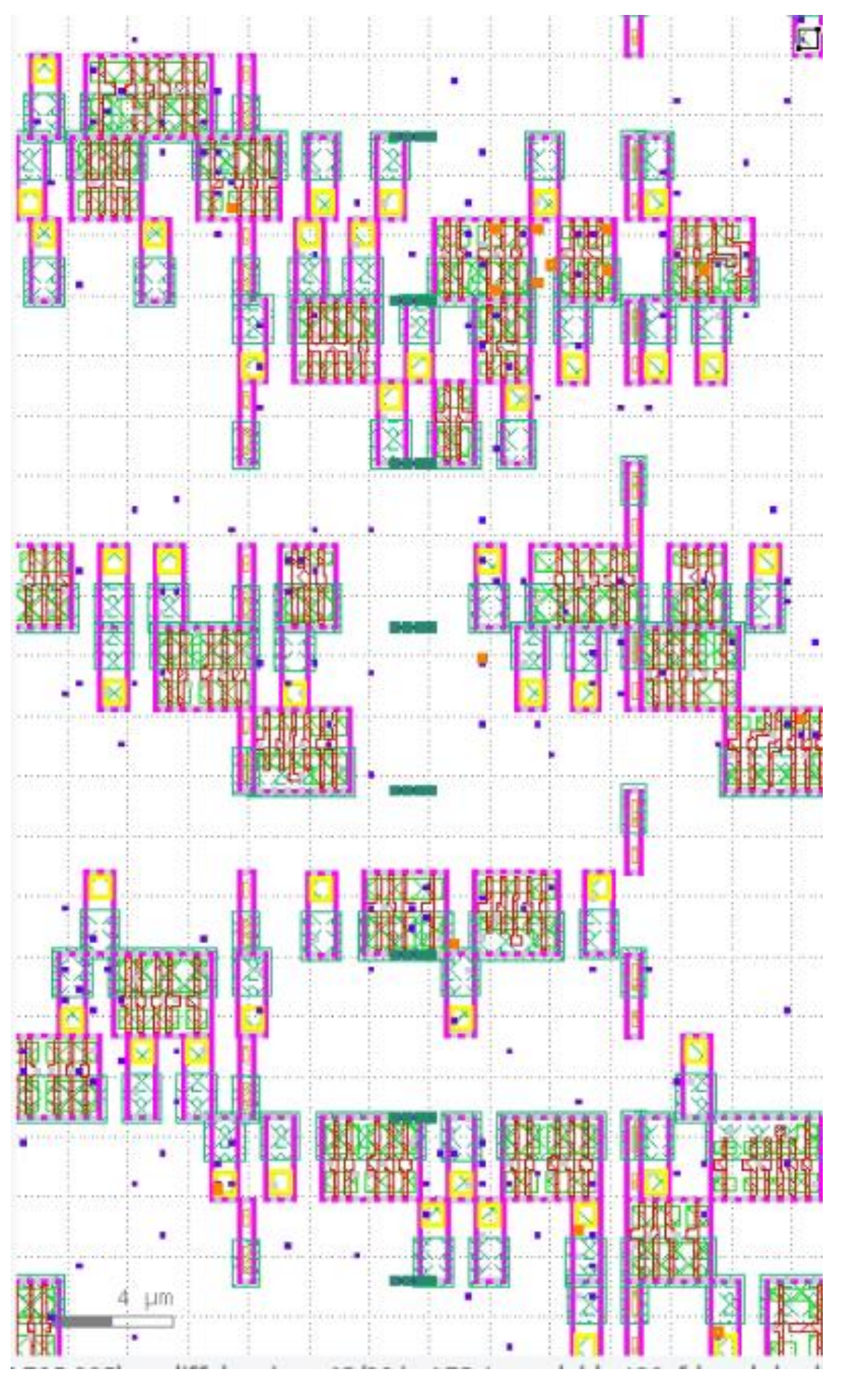




(Without decouplinc capacitors)



(Only with metal layers)



(Only Vias, n-p wells, silicons, polys)