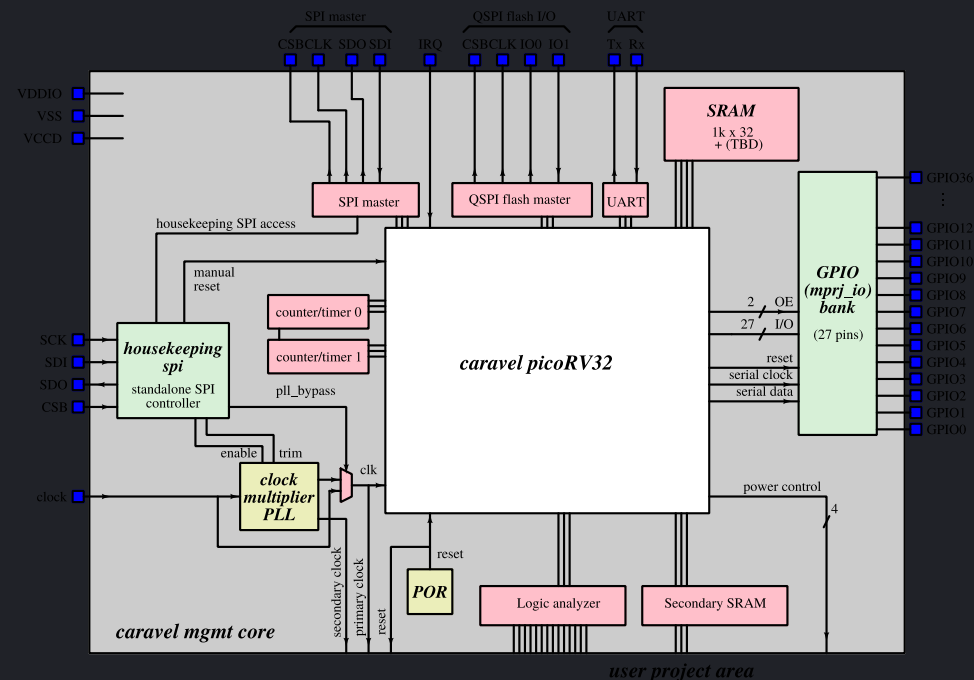


# ASIC Design With SKY130

ZEN team: Cole Blackman, Justin Zhang, Ceylan Morgul  
*ECE HPLP Lab UVA 2021*



# Table of Contents

**1. Caravel**

**2. Openlane (hardening process)**

**3. Caravel I/O**

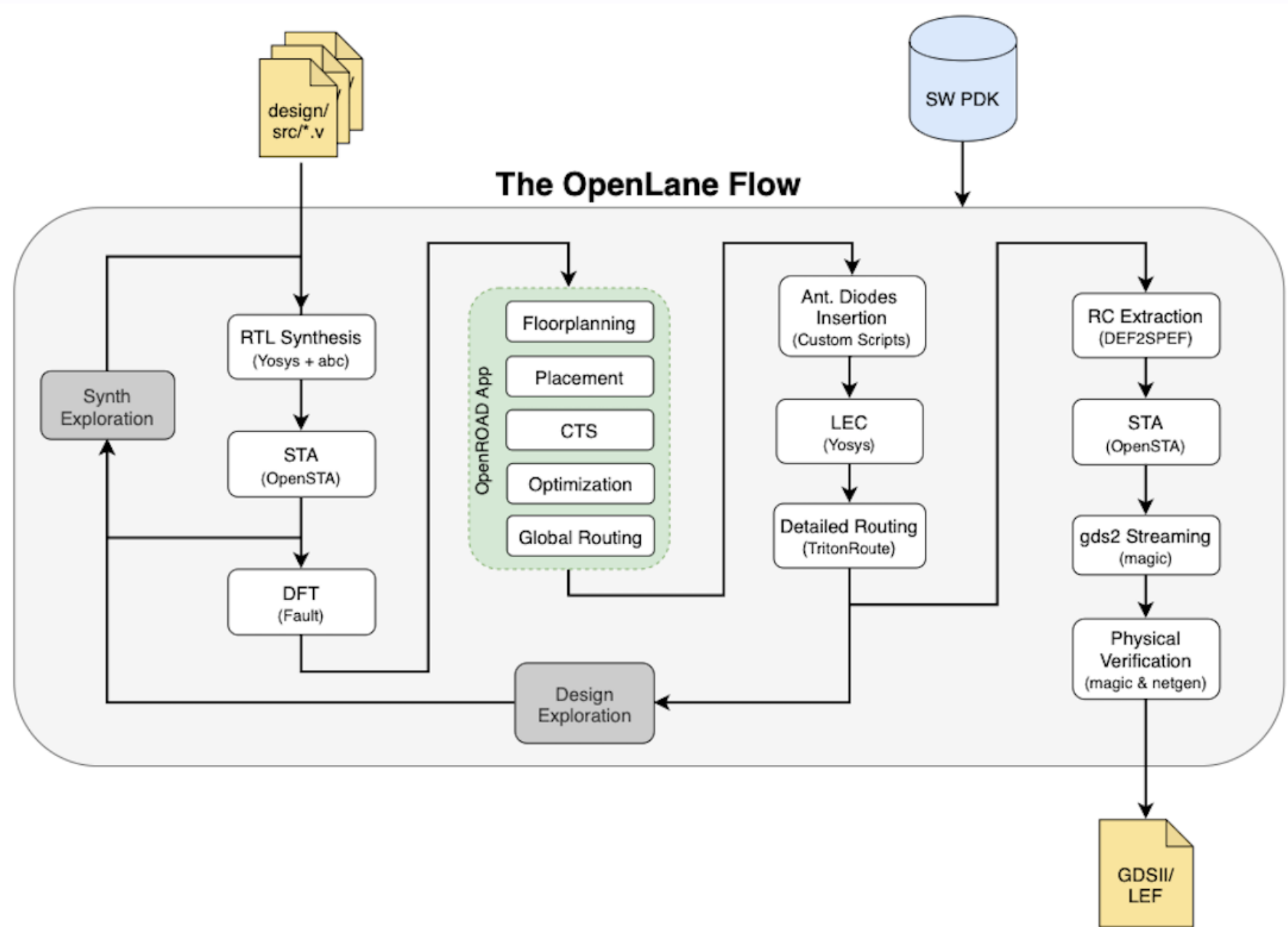
**4. Future work (SHA256)**

# Background: Skywater PDK and Sky130 process node

- Open source toolset
- Google and Skywater
- Design fabrication processes and ICs
- Work in progress (not recommended for commercial use yet)
- <https://skywater-pdk.readthedocs.io/en/latest/>

# Background: OpenLane Flow

- Complete process for building GDSII database files (IC layouts)
- "Converts" designer's verilog files to GDSII instructions



# Background: Efabless Open MPW Shuttle Program

- Fabricates your Skywater PDK 130nm process design using Openlane for free
- Your design must conform to submission standards (open source, git-compatible repo, etc)
- Design must pass checks

# Caravel

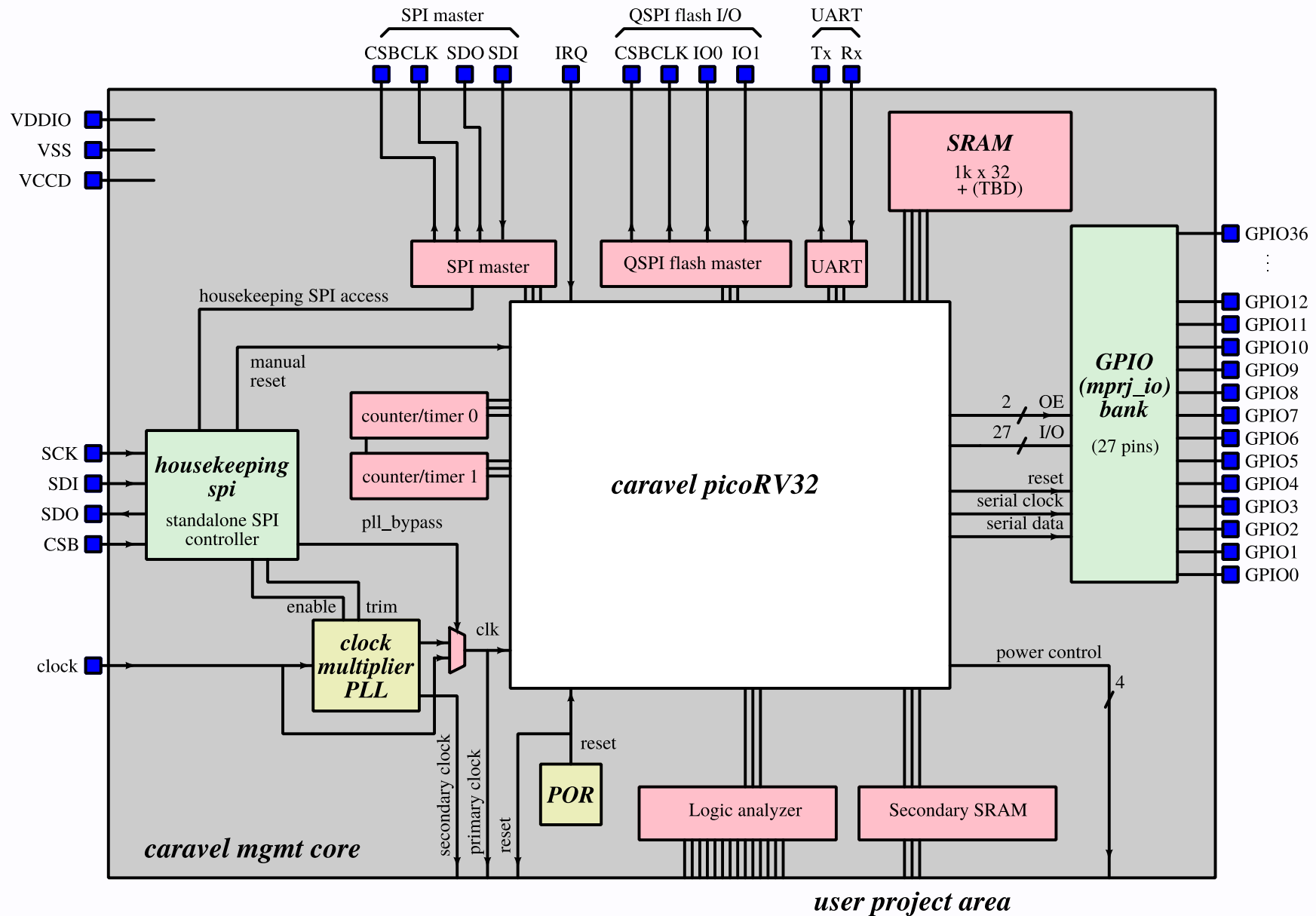
- Test harness for Skywater 130nm OS PDK
- RISC-V RV32IMC IS running on PicoRV32 processor core
- **Provides a test "harness" consisting of tools like SRAM and GP I/O for open user area circuits**

# Components of Caravel

**What does caravel provide the developer?**

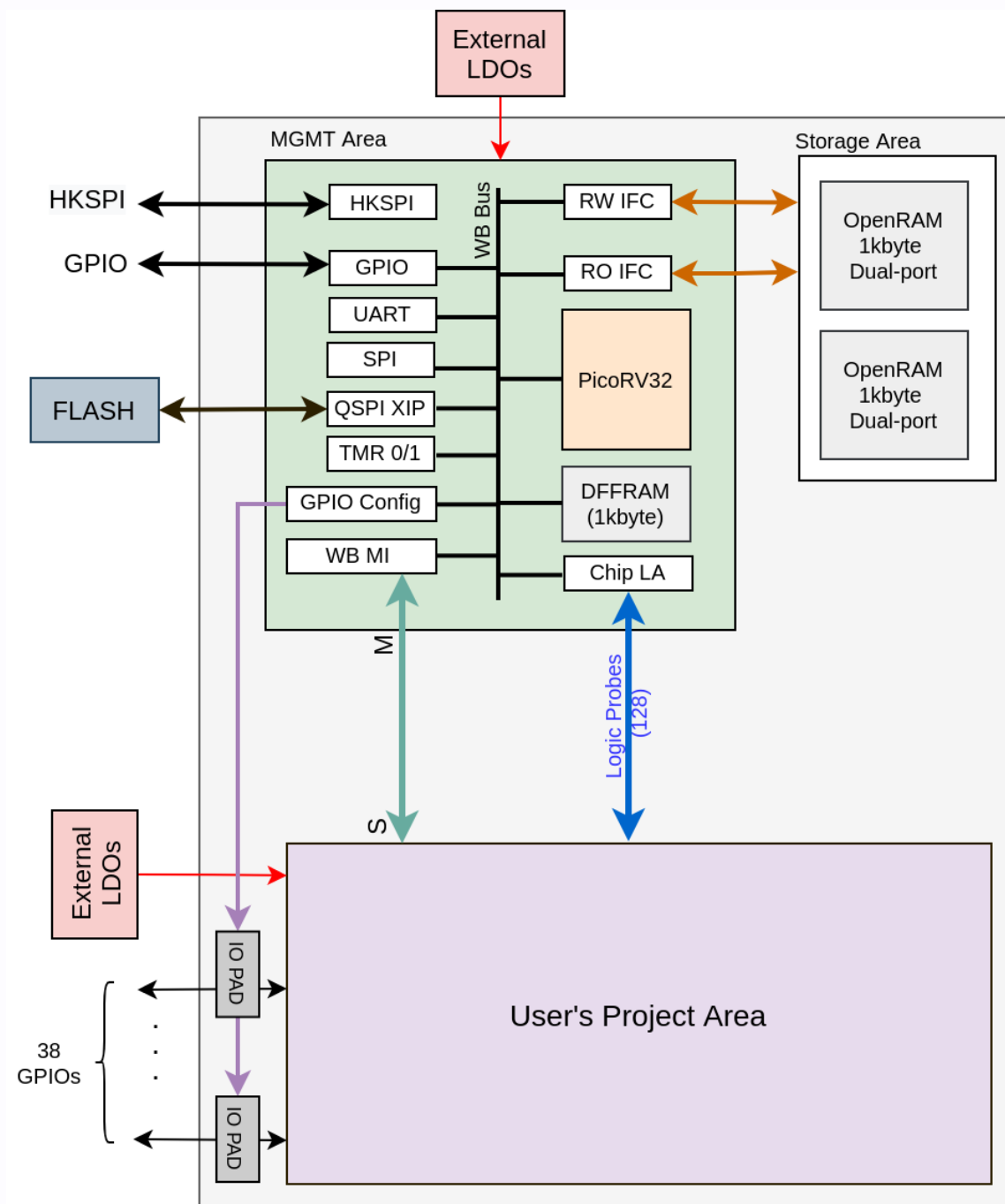
- Wishbone (32-bit)
- 128-bit logic analyzer
- UART
- SPI controller and SPI flash controller
- Large SRAM
- I/O
- And more...





# Comments on Diagrams

- mprj\_io I/O bank interfaces with caravel userspace
- User project area die size has decreased (from Efabless MPW Shuttle 1 to Shuttle 2)



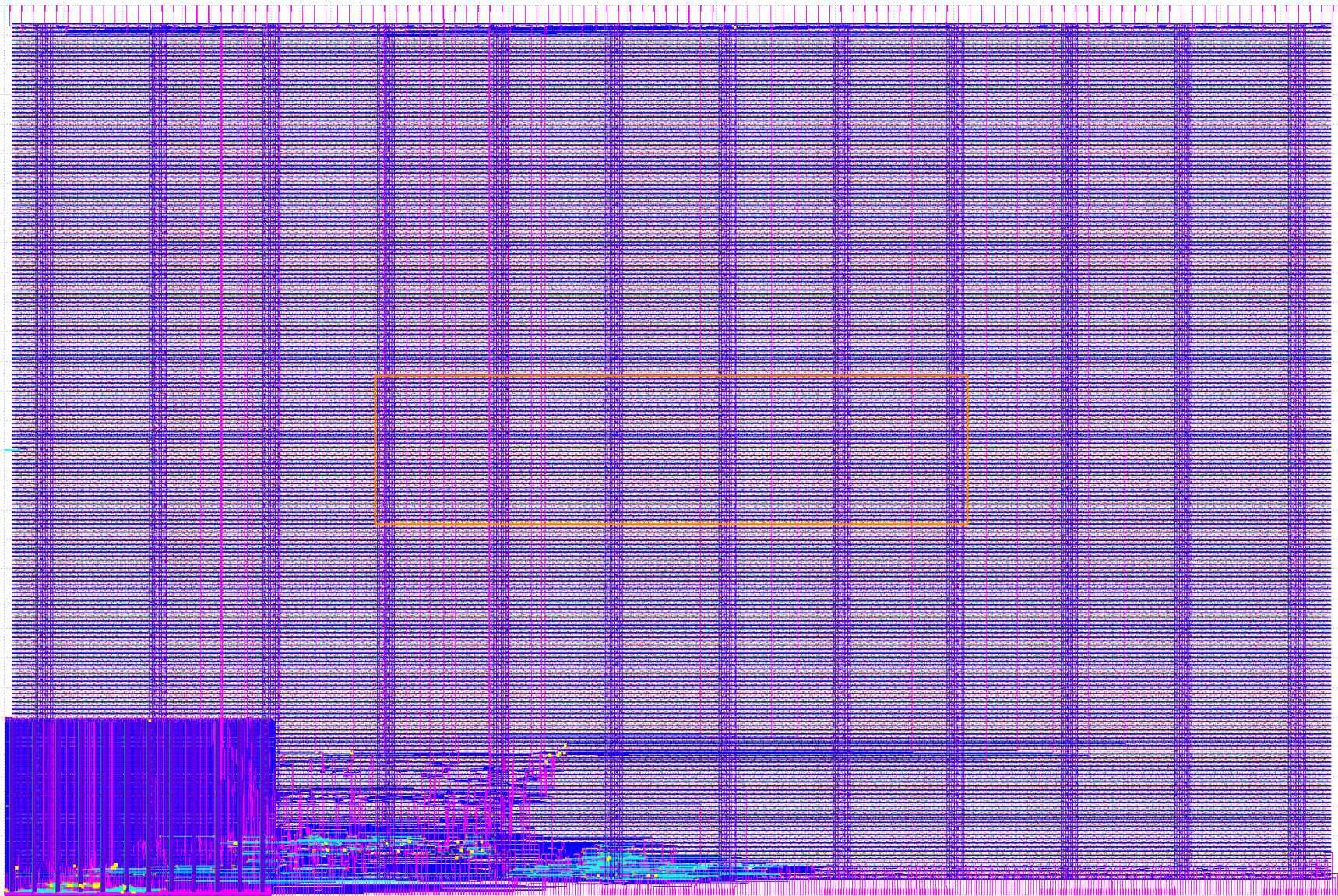
# Openlane Hardening

- Caravel is hardened with Openlane
- Can use Openlane or provide your own GDSII

# Johnson Counter With Caravel

- This example defines circuits for the caravel userspace, but does not require the use of I/O (see verilog code on our repository)





# IO Example: SHA3-256

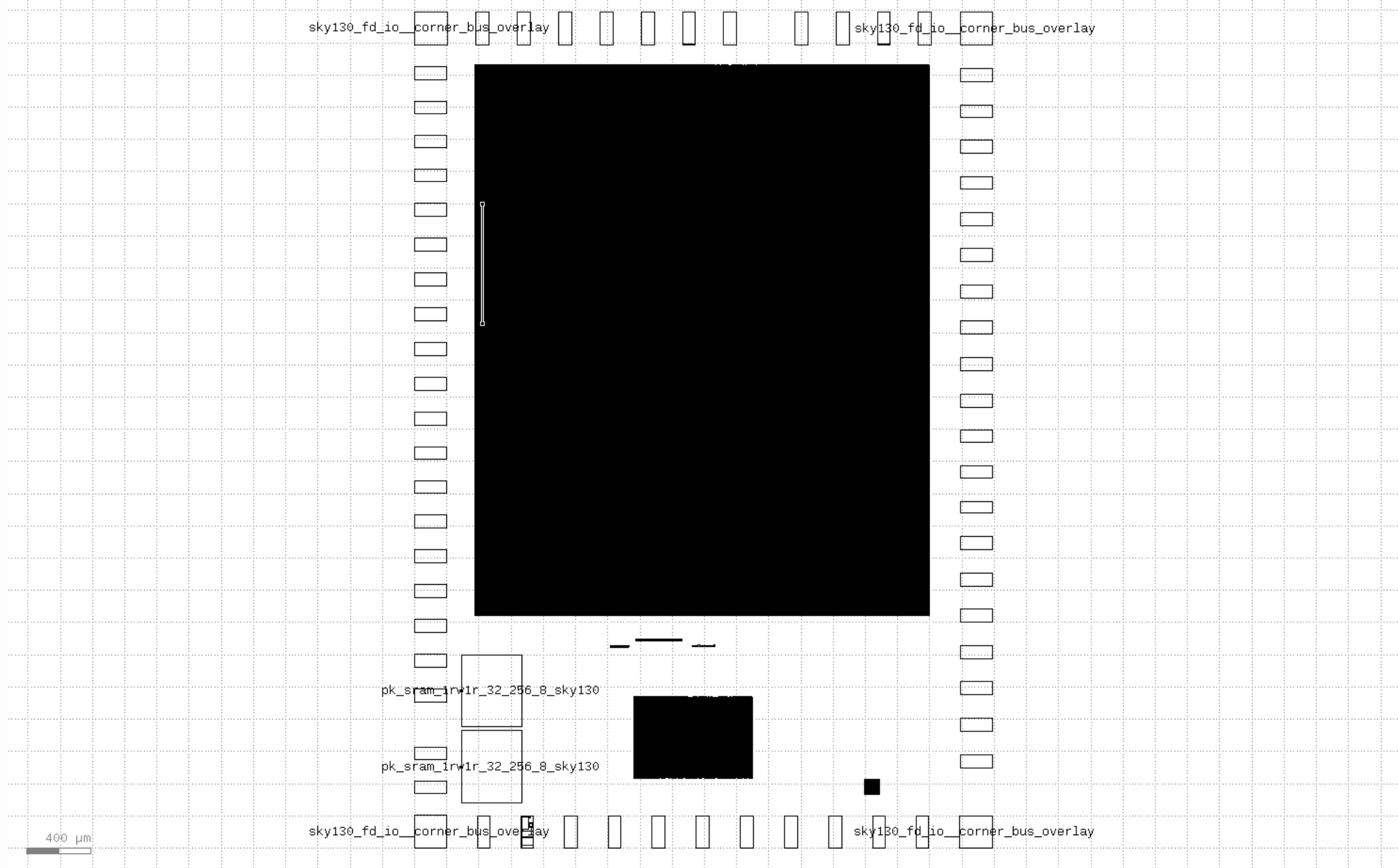
\*Unlike the previous example, this was written by Jean Cyr, not by us. We changed sections of the code to be compatible with the new die size requirements of the MPW Shuttle 2.0 and rewrote small sections for optimization.

# SHA-3 Keccak

- Hashing algorithm (secure hashing algorithm series of functions written by the NSA+NIST)
- Multi-step process based on manipulating the bits of the input data
- Computing SHA-3 hashes is a technique for Proof of Work in some cryptocurrencies
- A modified version of Keccak is used by the Ethereum cryptocurrency in PoW



**SHA3-256 on Caravel (I/O)**





```

sha3_256_miner_regs #
(
    .DATA_WIDTH(DATA_WIDTH),
    .ADDR_WIDTH(ADDR_WIDTH)
)
s3r
(
    .clk(wb_clk_i),          // clock
    .reset(wb_rst_i),        // reset
    .addr(wbs_adr_i),         // address
    .ack(wbs_ack_o),          // acknowledge
    .read(active_cyc),        // AND of two wishbone things
    .write(write_cyc),        //
    .rdata(wbs_dat_o),        // data out
    .wdata(wbs_dat_i),        // data in
    .sel(wbs_sel_i),          // select

    .header_o(header),        // header
    ...
);

```

# Our Work

- Compiled documentation
- Wrote ECE Wiki pages
- Adapted SHA-3 for MPW Shuttle 2.0 and wrote SHA-3 documentation
- Wrote and hardened Johnson counter within Openlane/Caravel harness (doesn't use I/O)
- Wrote Verilog tutorial
- Adapted SHA-3 algorithm

# Possible improvements for SHA-3

- Adapt to smaller die area
- Change number of stages in pipeline
- Offload padding etc. from ASIC
- Variable message size

# Our Future Work

- Implementation of SHA-2 (256) hashing algorithm in a custom user area ASIC ontop of the Caravel Harness (Bitcoin/Crypto mining applications)
- Entrance into IEEE SSCS design contest

# Our Future Work: SHA2-256

- Similar to SHA3-256 in nature (SHA)
- Still widely used today (coexists with SHA-3)
- Used in Bitcoin (ASIC)



# SSCS "PICO" Open-Source Design Contest

- First year members only, pre-college and undergraduates
- Encouraged to use an SSCS circuit
- Can reuse open-source circuits
- chipIgnite: still uses caravel and openlane

Efabless - Project Form

efabless.com/projects/create?project\_group=sscs-21

☆ J

efabless

Projects ▾ Tools ▾ Marketplace ▾ Community ▾ Company ▾

Hi, Jeff J

## PROJECT

Basics

Details

Images

Project Title \*

my\_project

Visibility \*

Private ▾

Summary (In a few words describe the project) \*

This is a short sentence about my project.

Organization URL

GIT URL ?

Project files (\*.tar.gz format expected) ?

Choose file to upload

Choose File

Version

Shuttle Tags

chipignite

SSCS-21

Tags

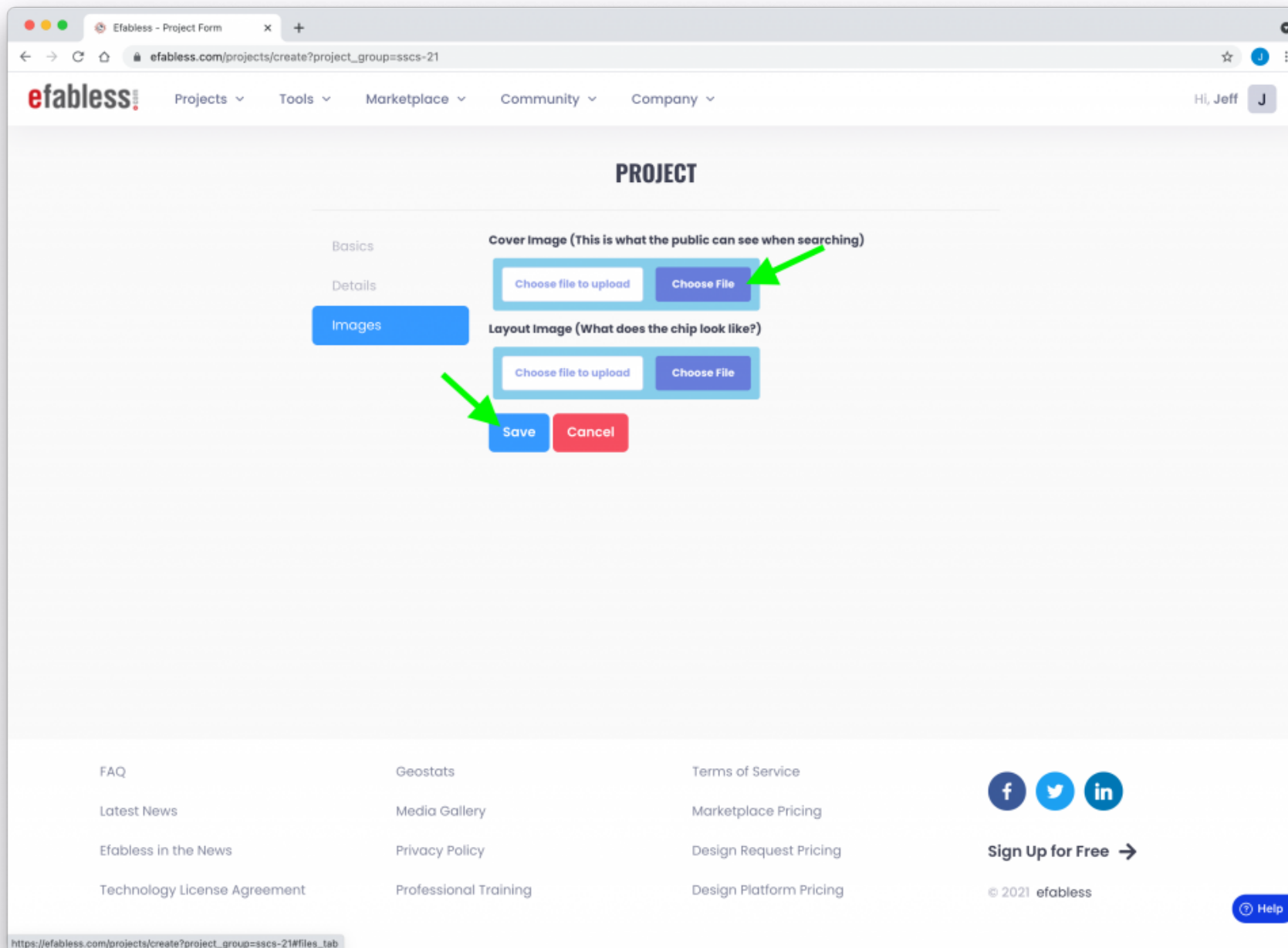
× RISCv

× ADC

Save

Cancel

Help



Efabless - Project Form

efabless.com/projects/create?project\_group=sscs-21

☆ 1

efabless

ProjectsToolsMarketplaceCommunityCompany

Hi, Jeff J

PROJECT

Basics

Details

Images

Category

A/D Converter

Process

sky130A

Description (Tell everyone about your project and why you decided to make it)

File Edit View Insert Format Tools Table

↶ ↷ Paragraph B I U S A ↕ I ...

Description

<insert text here>

Design Goals

< insert text here>

Block Diagram

< insert image here>

Schematics

< insert image here>

References

Team Members

P 24 WORDS POWERED BY TINY

Save

Cancel

FAQ

Geostats

Terms of Service

Help

# PICO timeline

- July 30: submit proposal
- 15-20 selected round 1 design teams
  - Weekly meetings until October
- Sept. 24: 6 designs selected
- Can still apply for shuttles

# Key Takeaways

- Skywater PDK - maturing and useful
- Caravel test harness - good for small applications and education
- Caravel makes it easy to realize Verilog designs
- These tools provide a good testbench for samples of more complex circuits like hashing algorithms

# More Information /Sources /References

- Caravel documentation: <https://caravel-harness.readthedocs.io/en/latest/>
- Openlane documentation  
<https://openlane.readthedocs.io/en/latest/>
- Jean Cyr <https://github.com/miscellaneousbits/>
- Verilog by Example - Blaine Readler
- Efabless - <https://efabless.com/>