Programming Management Unit: Open-Source Core for Secure FPGA Bitstream Configuration

Allen Boston

R. Gauchi, Pierre-Emmanuel Gaillardon

Department of Electrical and Computer Engineering – University of Utah

Open-Source Computer Architecture Research 2023

06/18/2023

Motivation

- FPGAs are essential to modern high-performance systems

Wired and wireless communications

Audio and video broadcasting

Data center

[Author's Own]

Motivation

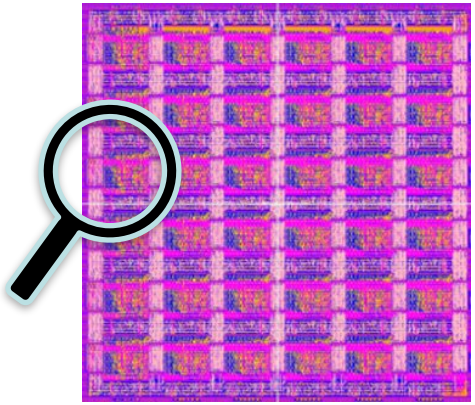
- FPGAs are essential to modern high-performance systems

Wired and wireless communications

Audio and video broadcasting

Data center

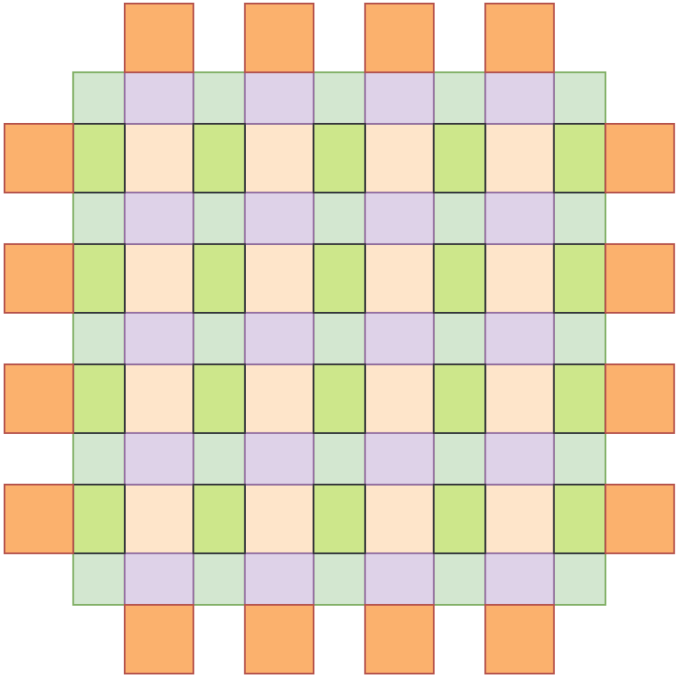
- Prime target for adversaries



[Author's Own]

Motivation

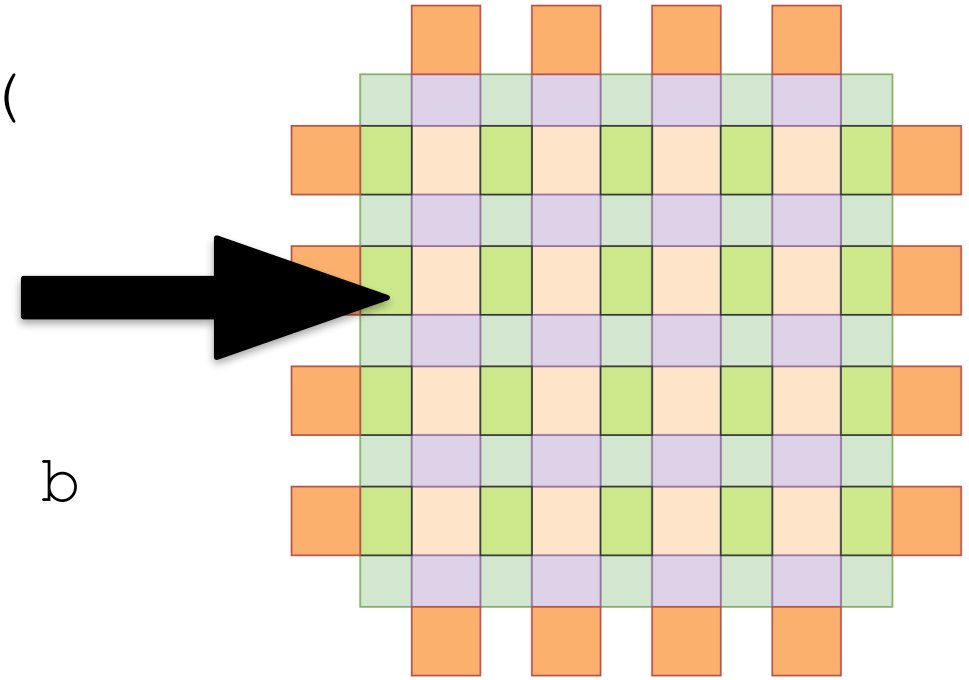
- Configurable architectures are generic in nature



Motivation

- Configurable architectures are generic in nature
- FPGAs are programmed with user IP

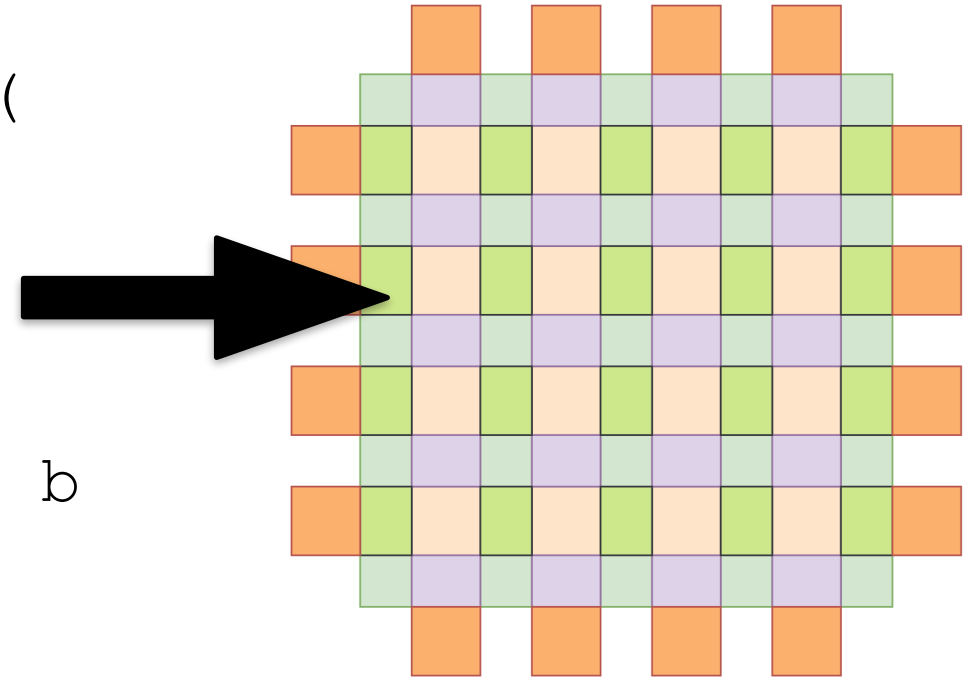
```
module adder_16bit(
  input [15:0] a,
  input [15:0] b,
  output [15:0] sum
  );
    assign sum = a + b
  endmodule
```



Motivation

- Configurable architectures are generic in nature
- FPGAs are programmed with user IP

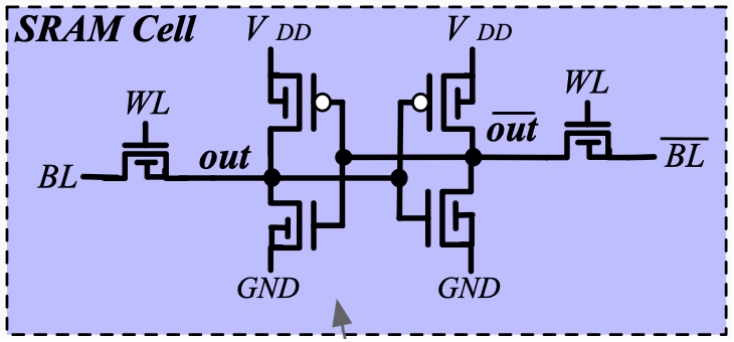
```
module adder_16bit(
  input [15:0] a,
  input [15:0] b,
  output [15:0] sum
  );
    assign sum = a + b
  endmodule
```



Essential to essential to safeguard the configuration data

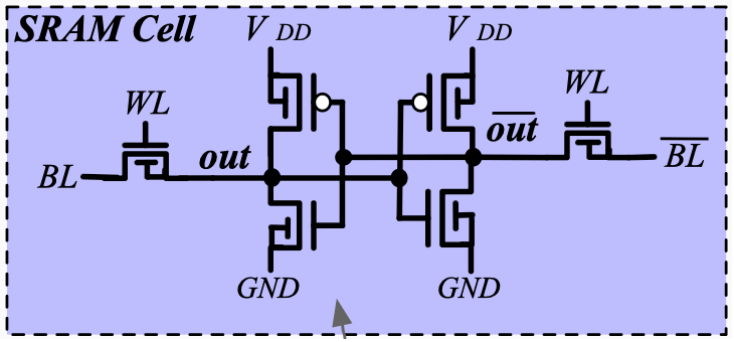
FPGA Configuration Protocol

- State-of-the-art FPGAs leverage SRAM-based configuration
  - High speed, low power, scalable



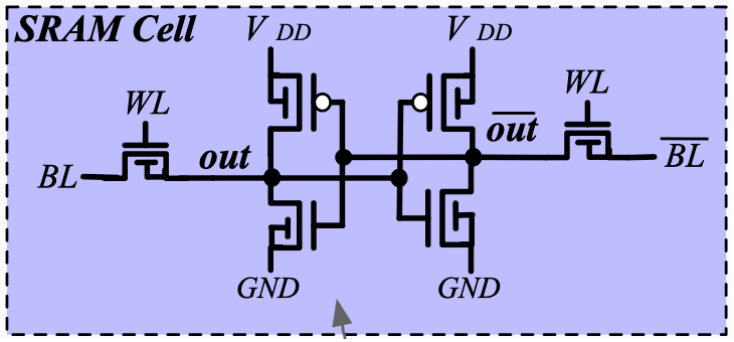
FPGA Configuration Protocol

- State-of-the-art FPGAs leverage SRAM-based configuration
  - High speed, low power, scalable
- Flash is a non-volatile alternative



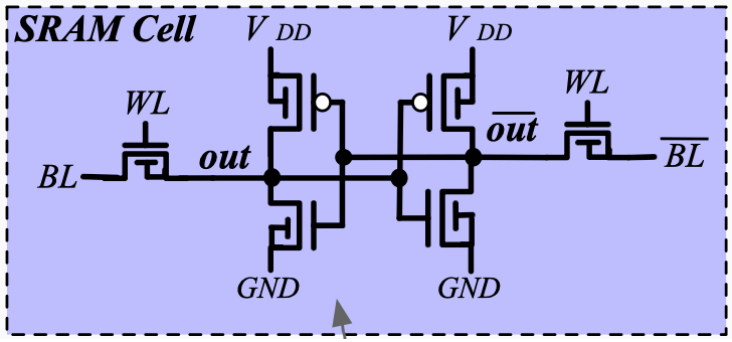
FPGA Configuration Protocol

- State-of-the-art FPGAs leverage SRAM-based configuration
  - High speed, low power, scalable
- Flash is a non-volatile alternative
- Parallel and serial data acquisition

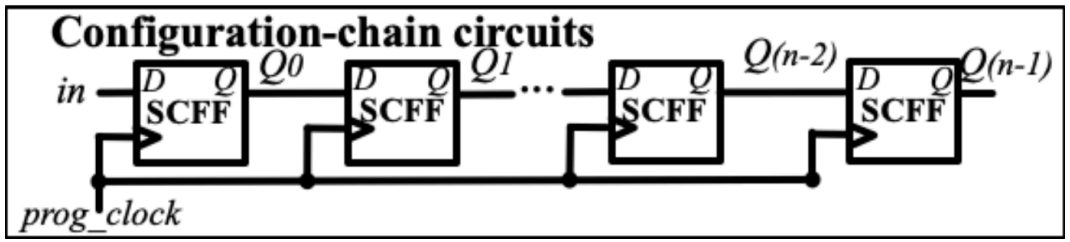


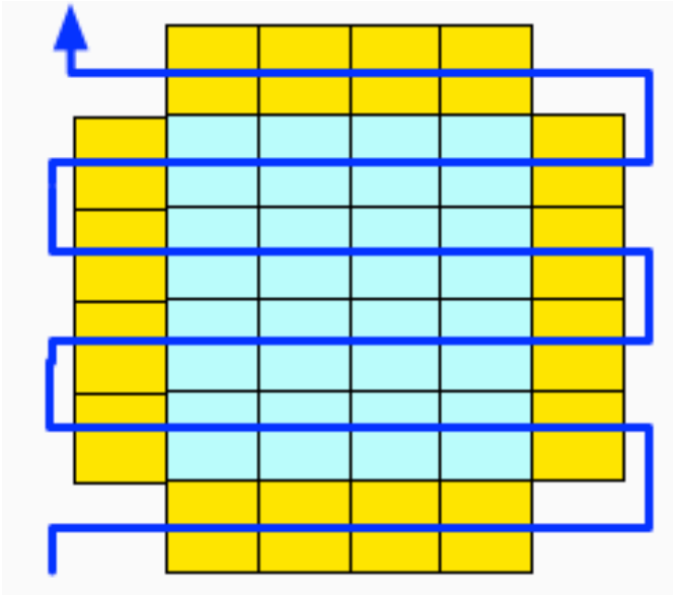
FPGA Configuration Protocol

- State-of-the-art FPGAs leverage SRAM-based configuration
  - High speed, low power, scalable
- Flash is a non-volatile alternative
- Parallel and serial data acquisition
- PMU targets a OpenFPGA serial configuration-chain protocol



OPEN FPGA



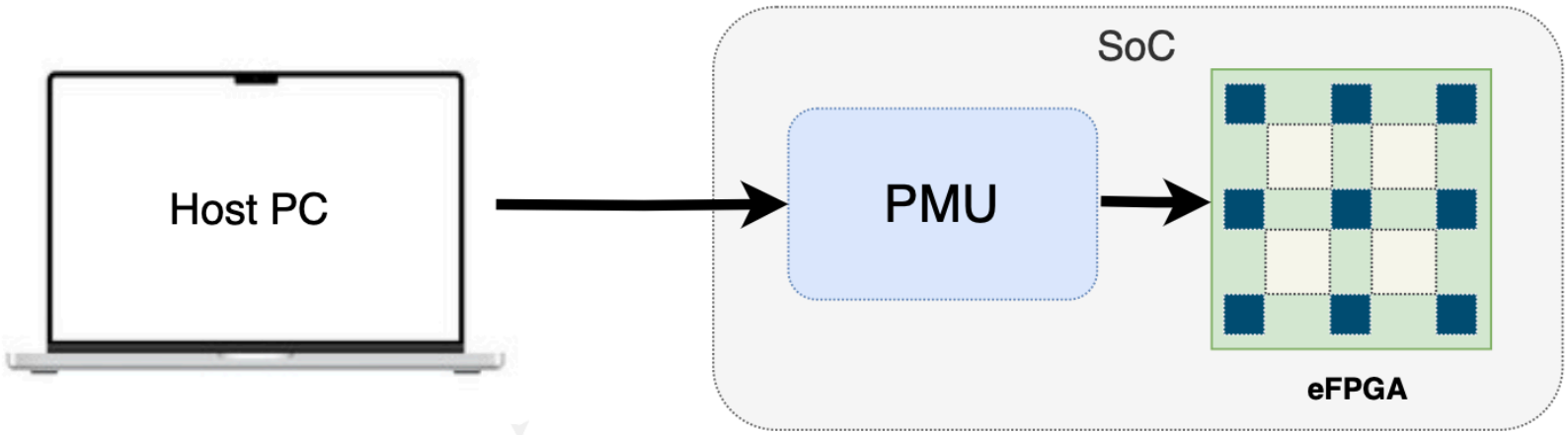


Programming Management Unit

- **Problem:**
  - FPGA bitstream configuration is complex
  - Impossible to customize security IP in commercial FPGAs.
  - Open-source landscape lacks security aware FPGA configuration circuitry

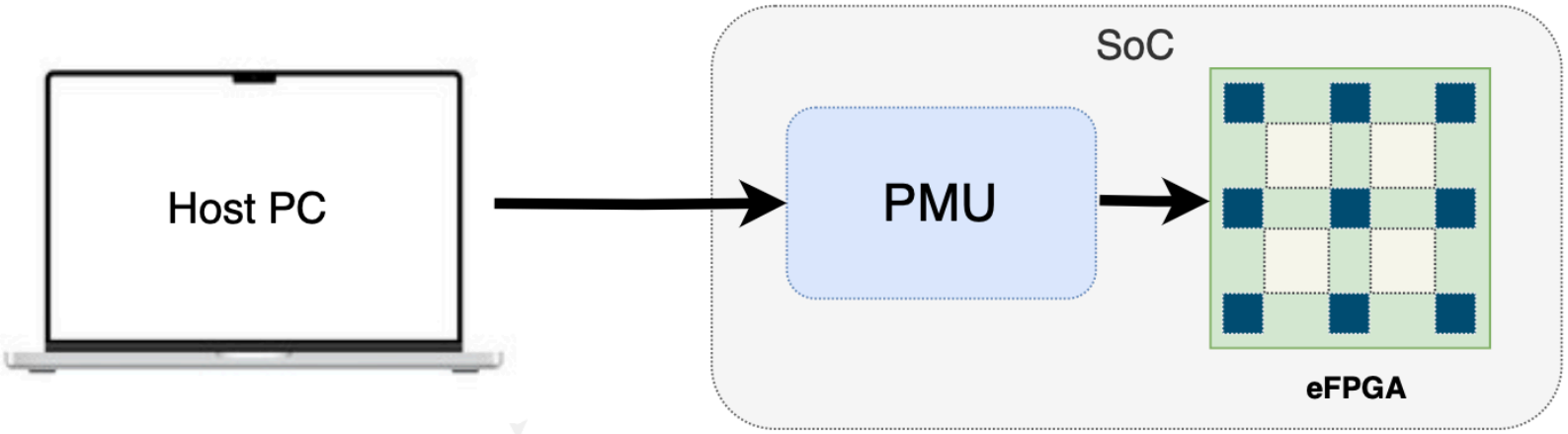
Programming Management Unit

- **Problem:**
  - FPGA bitstream configuration is complex
  - Impossible to customize security IP in commercial FPGAs.
  - Open-source landscape lacks security aware FPGA configuration circuitry
- **Proposal:**
  - First open-source IP core specifically dedicated to FPGA configuration
  - Customizable framework dedicated to secure data movement from EDA bitstream generation to FPGA core configuration circuitry.



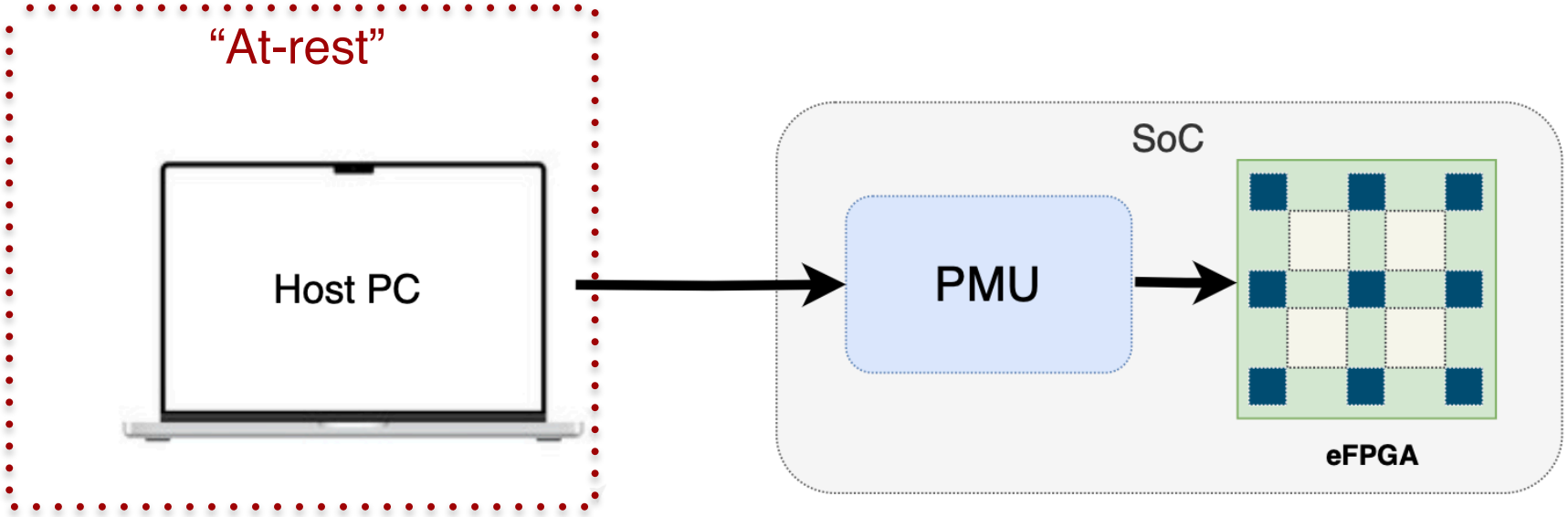
PMU Threat Model

- PMU bitstream security measures constrained to “at-rest” and “loading” stages of configuration procedure



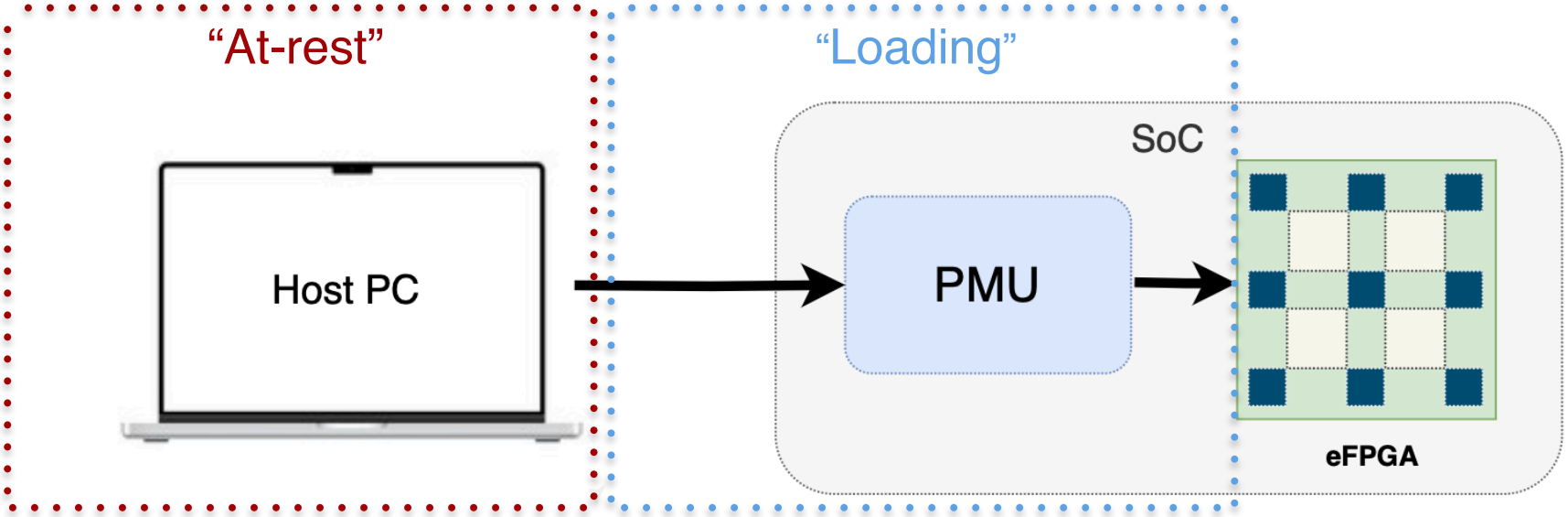
PMU Threat Model

- PMU bitstream security measures constrained to “at-rest” and “loading” stages of configuration procedure



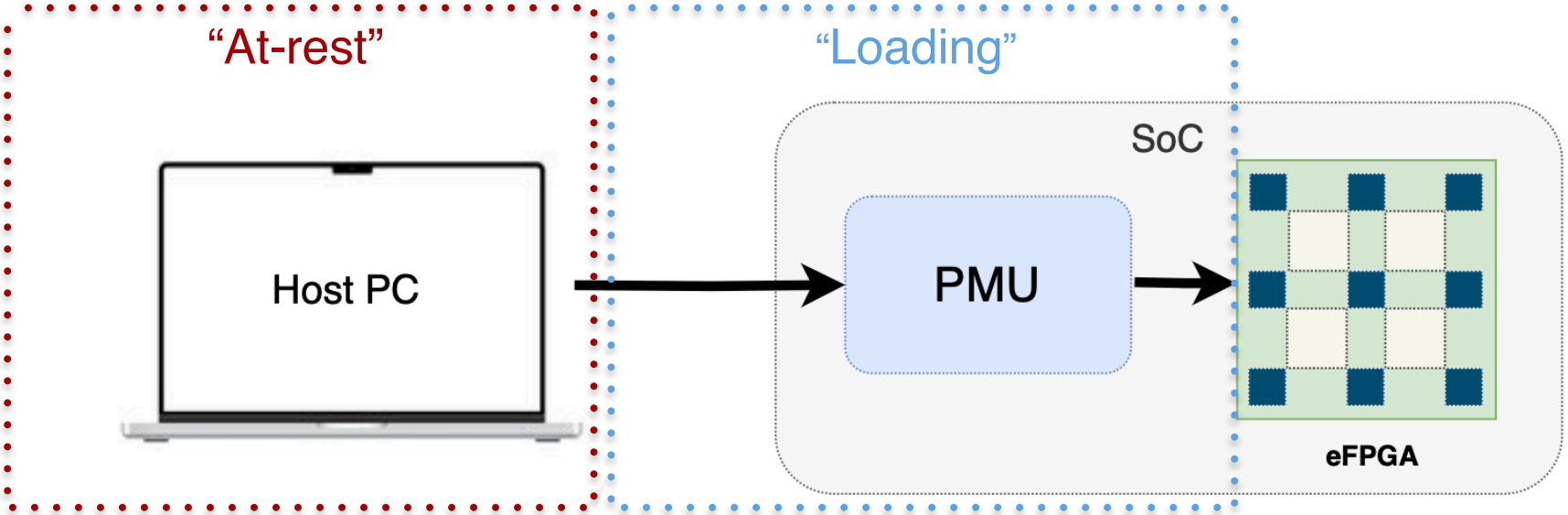
PMU Threat Model

- PMU bitstream security measures constrained to “at-rest” and “loading” stages of configuration procedure



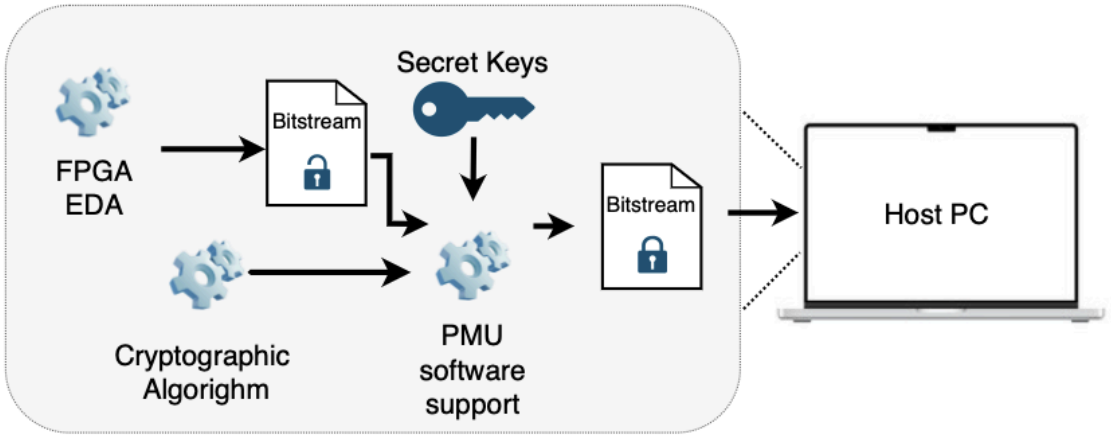
PMU Threat Model

- PMU bitstream security measures constrained to “at-rest” and “loading” stages of configuration procedure

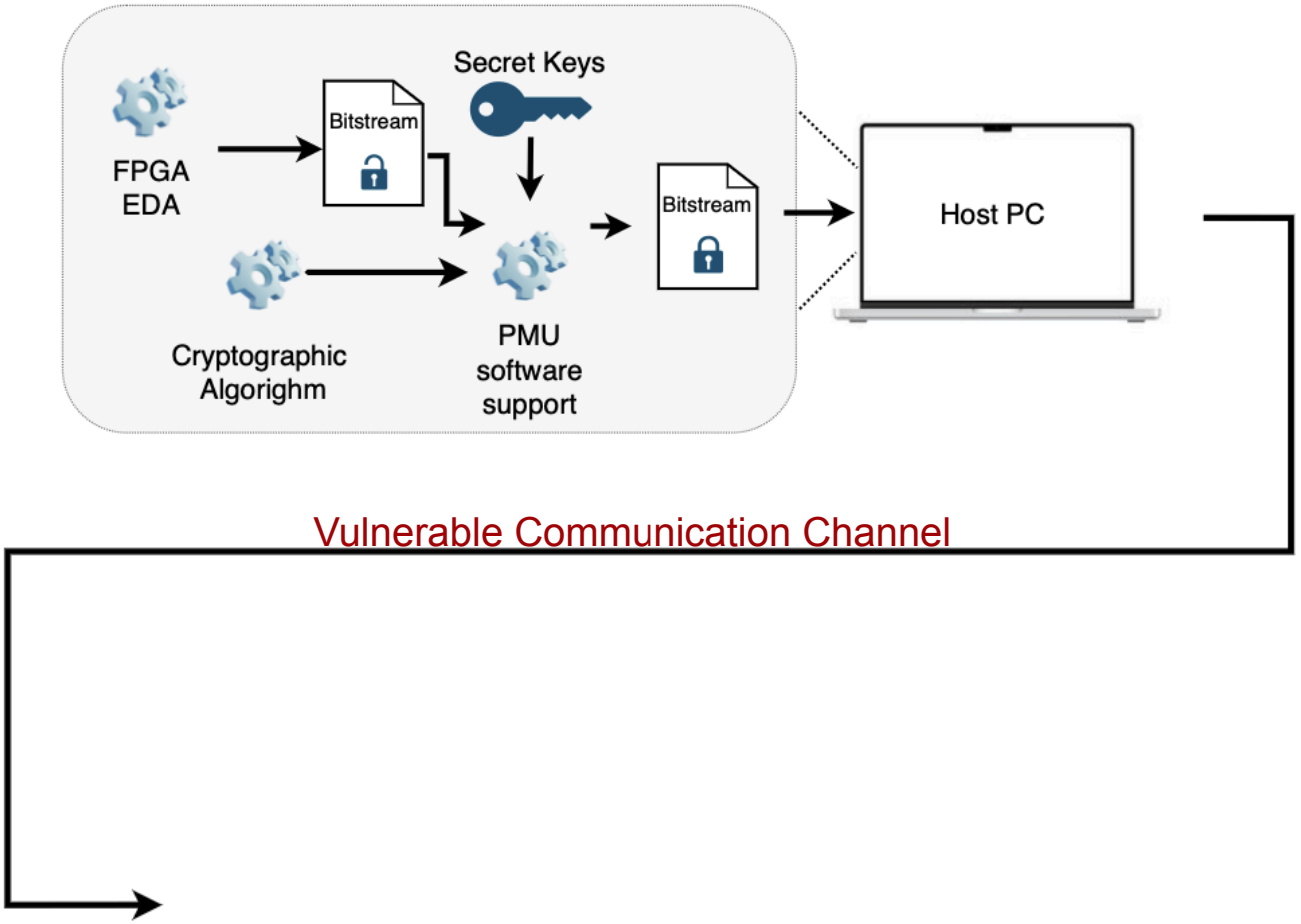


- Key storage falls outside the scope of work for this project.

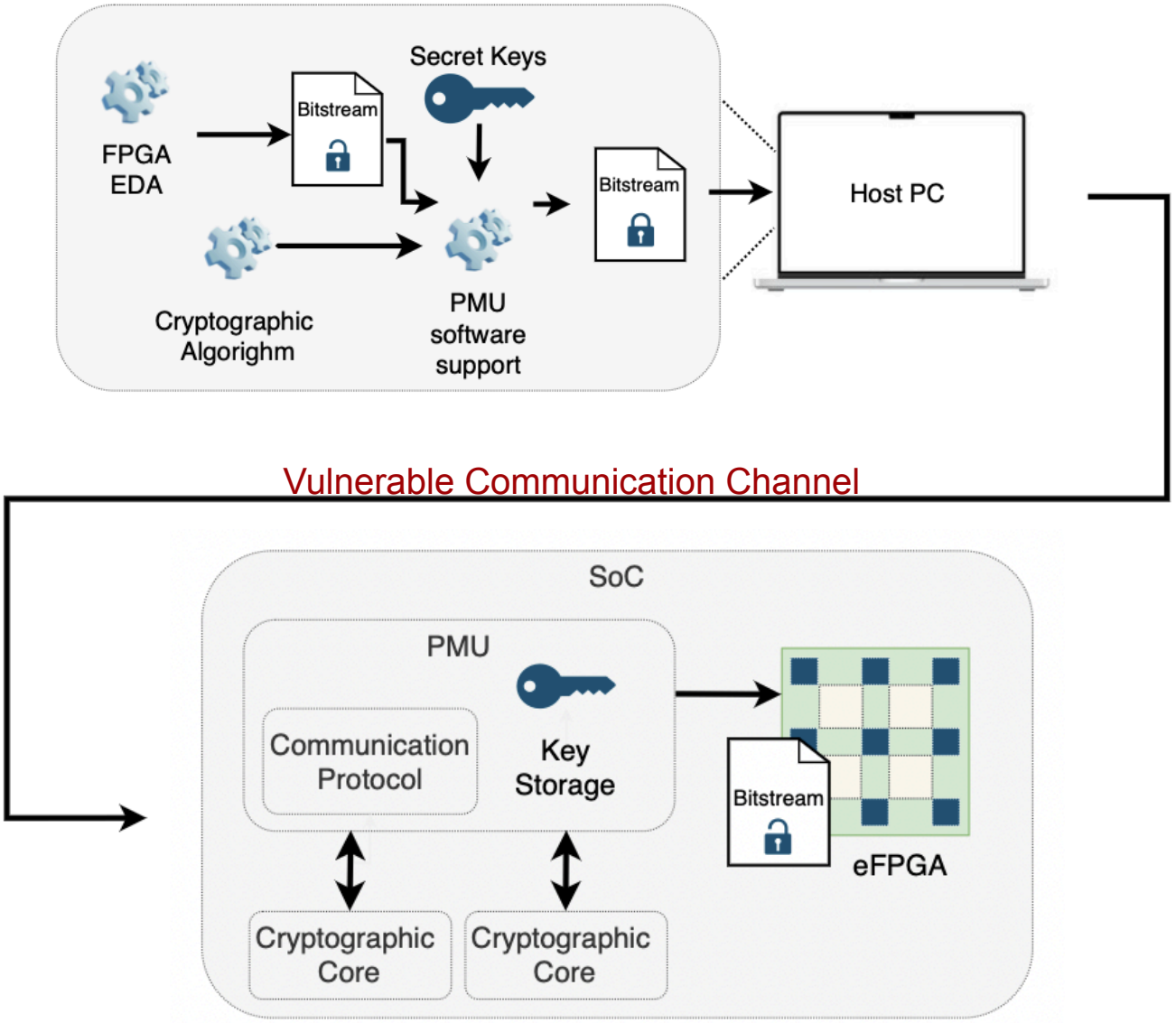
Proposed System Architecture



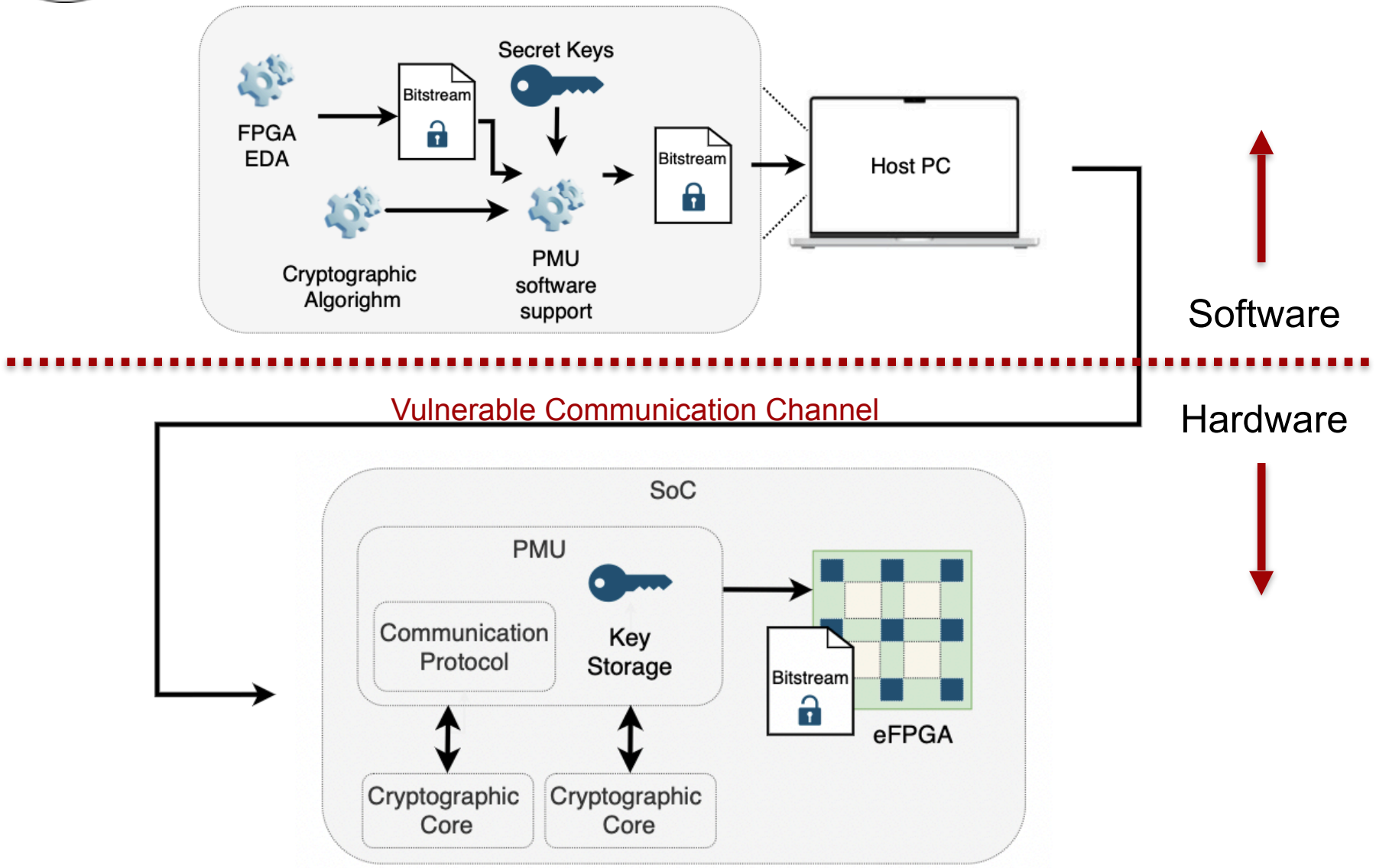
Proposed System Architecture



Proposed System Architecture



Proposed System Architecture



PMU Integration Showcase

- Leverage the open-source ecosystem by utilizing pre-existing IPs

PMU Integration Showcase

- Leverage the open-source ecosystem by utilizing pre-existing IPs
- 10x10 OpenFPGA fabric
  - OpenFPGA Github: https://github.com/lnis-uofu/OpenFPGA

PMU Integration Showcase

- Leverage the open-source ecosystem by utilizing pre-existing IPs
- 10x10 OpenFPGA fabric
  - OpenFPGA Github: https://github.com/lnis-uofu/OpenFPGA
- Joint-Action Test Group
  - JTAG Github: https://github.com/freecores/jtag

PMU Integration Showcase

- Leverage the open-source ecosystem by utilizing pre-existing IPs
- 10x10 OpenFPGA fabric
  - OpenFPGA Github: **https://github.com/lnis-uofu/OpenFPGA**
- Joint-Action Test Group
  - JTAG Github: **https://github.com/freecores/jtag**
- Advanced Encryption Standard
  - AES Github: **https://github.com/secworks/aes**

PMU Integration Showcase

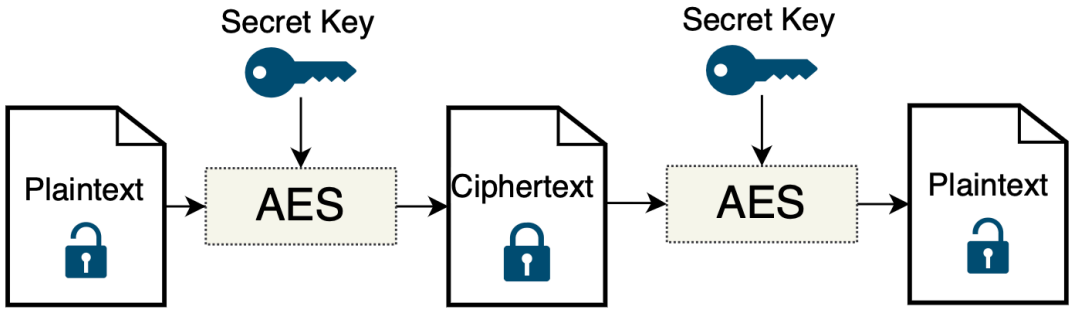
- Leverage the open-source ecosystem by utilizing pre-existing IPs
- 10x10 OpenFPGA fabric
  - OpenFPGA Github: https://github.com/lnis-uofu/OpenFPGA
- Joint-Action Test Group
  - JTAG Github: https://github.com/freecores/jtag
- Advanced Encryption Standard
  - AES Github: https://github.com/secworks/aes
- Secure Hash Algorithm
  - SHA Github: https://github.com/secworks/sha256

Security Measures

- Bitstream confidentiality

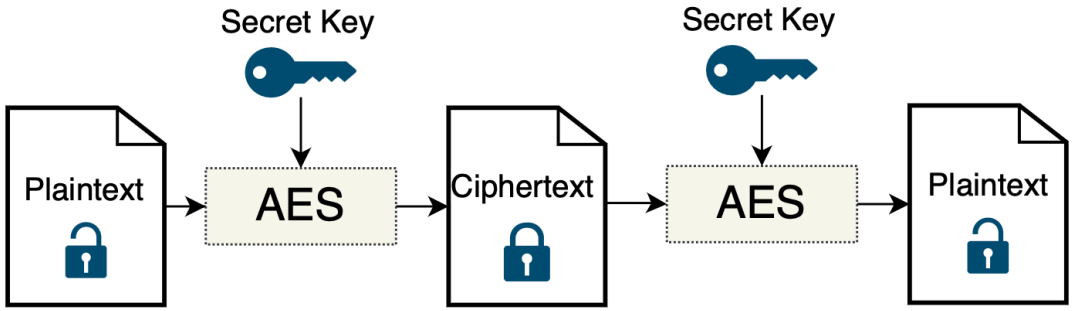
Security Measures

- Bitstream confidentiality
  - Advanced Encryption Standard (AES)



Security Measures

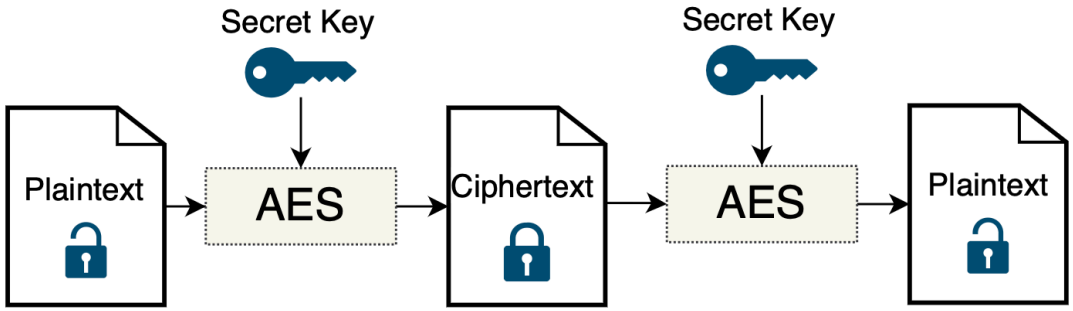
- Bitstream confidentiality
  - Advanced Encryption Standard (AES)



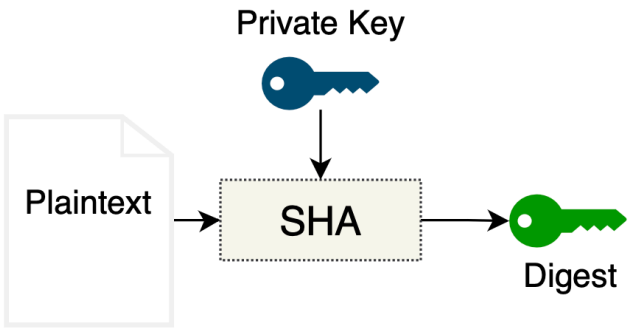
- Authentication and Data Integrity

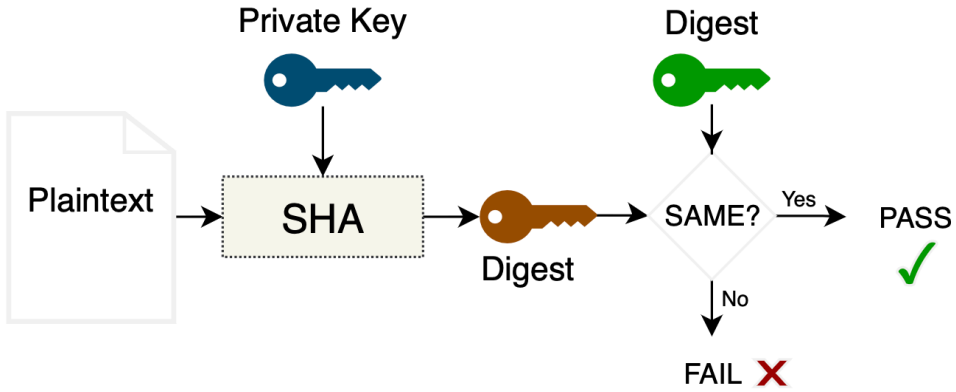
Security Measures

- Bitstream confidentiality
  - Advanced Encryption Standard (AES)

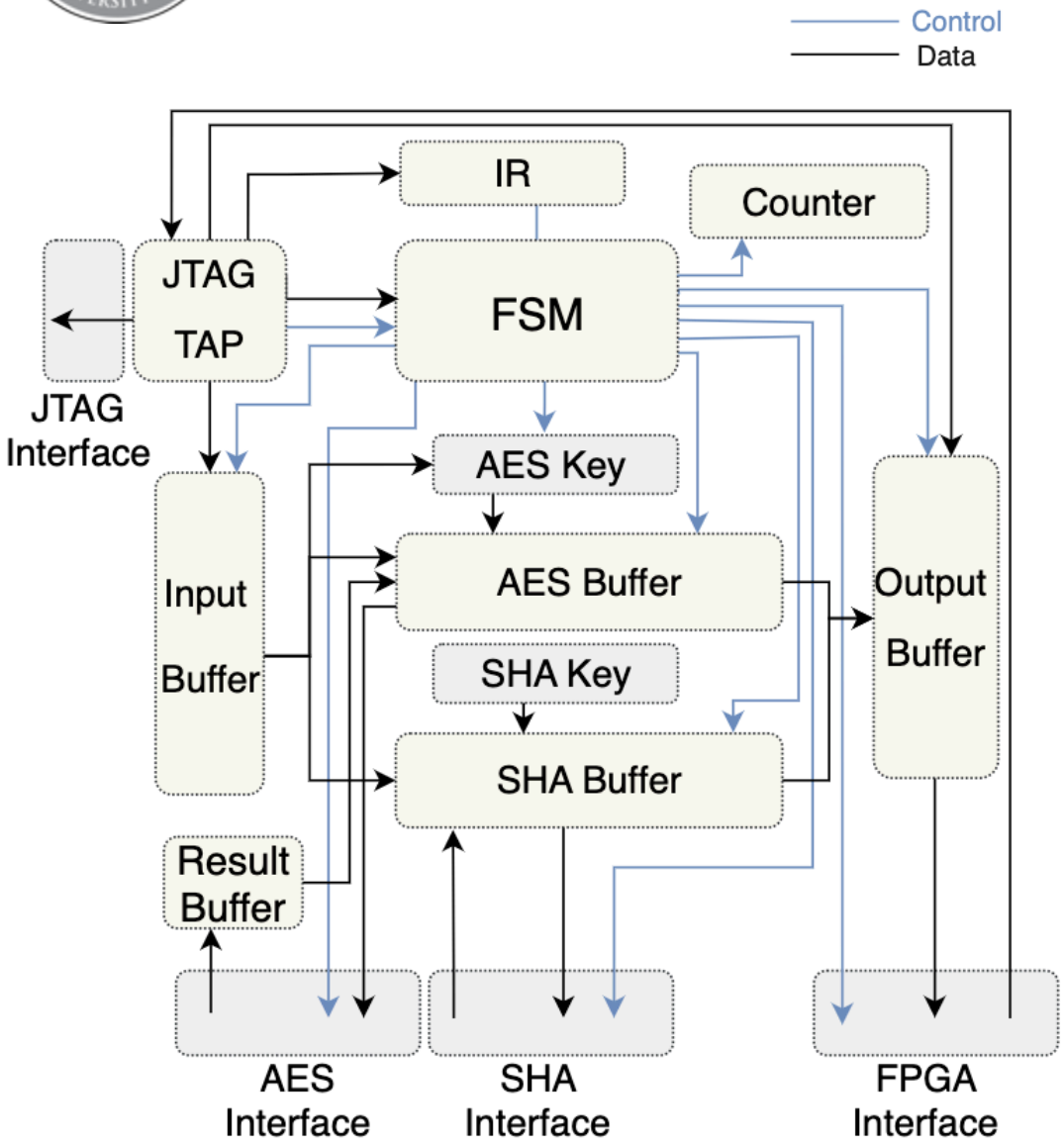


- Authentication and Data Integrity
  - Secure Hash Algorithm (SHA)

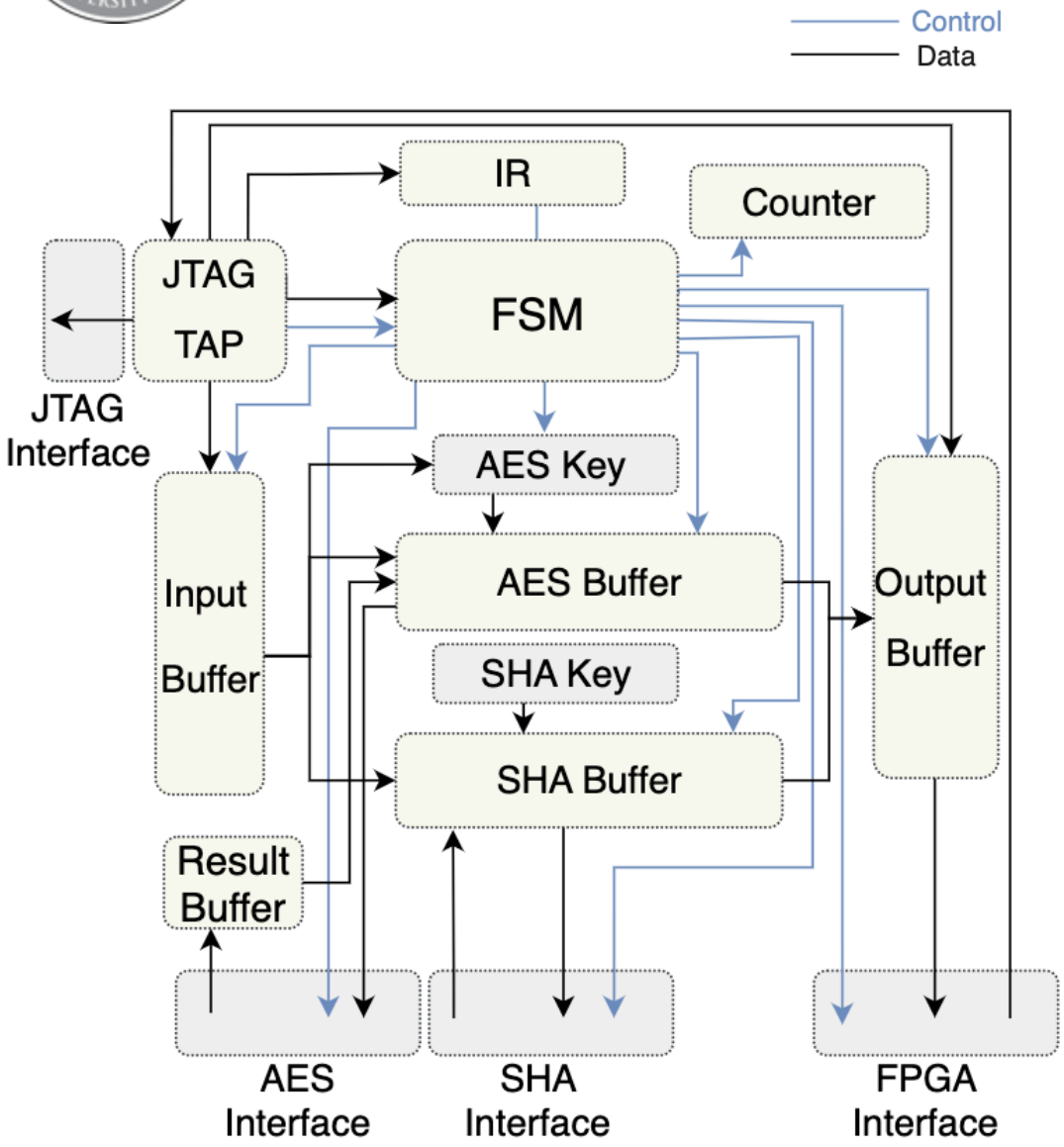




PMU Core Block Diagram

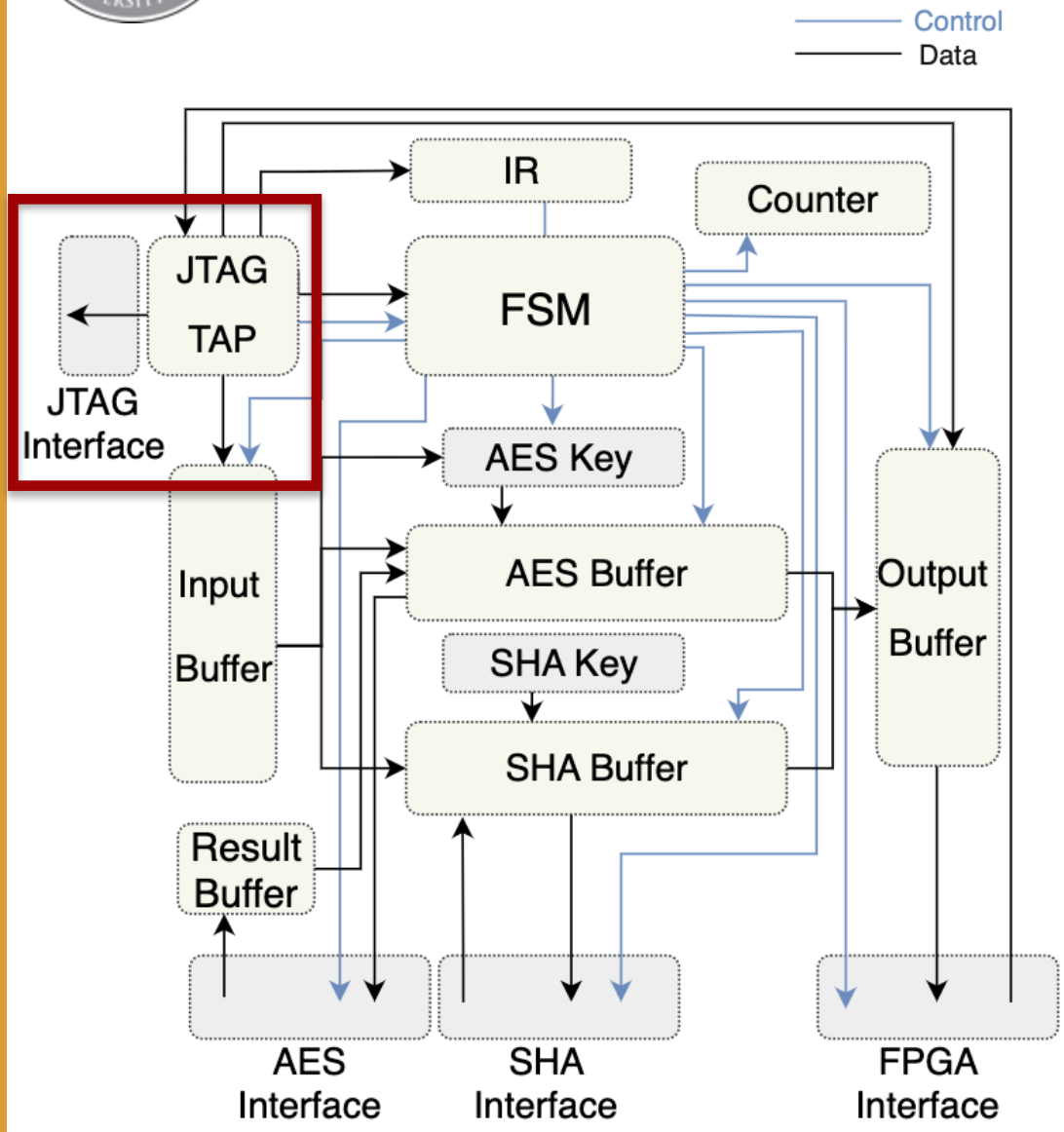


PMU Core Block Diagram



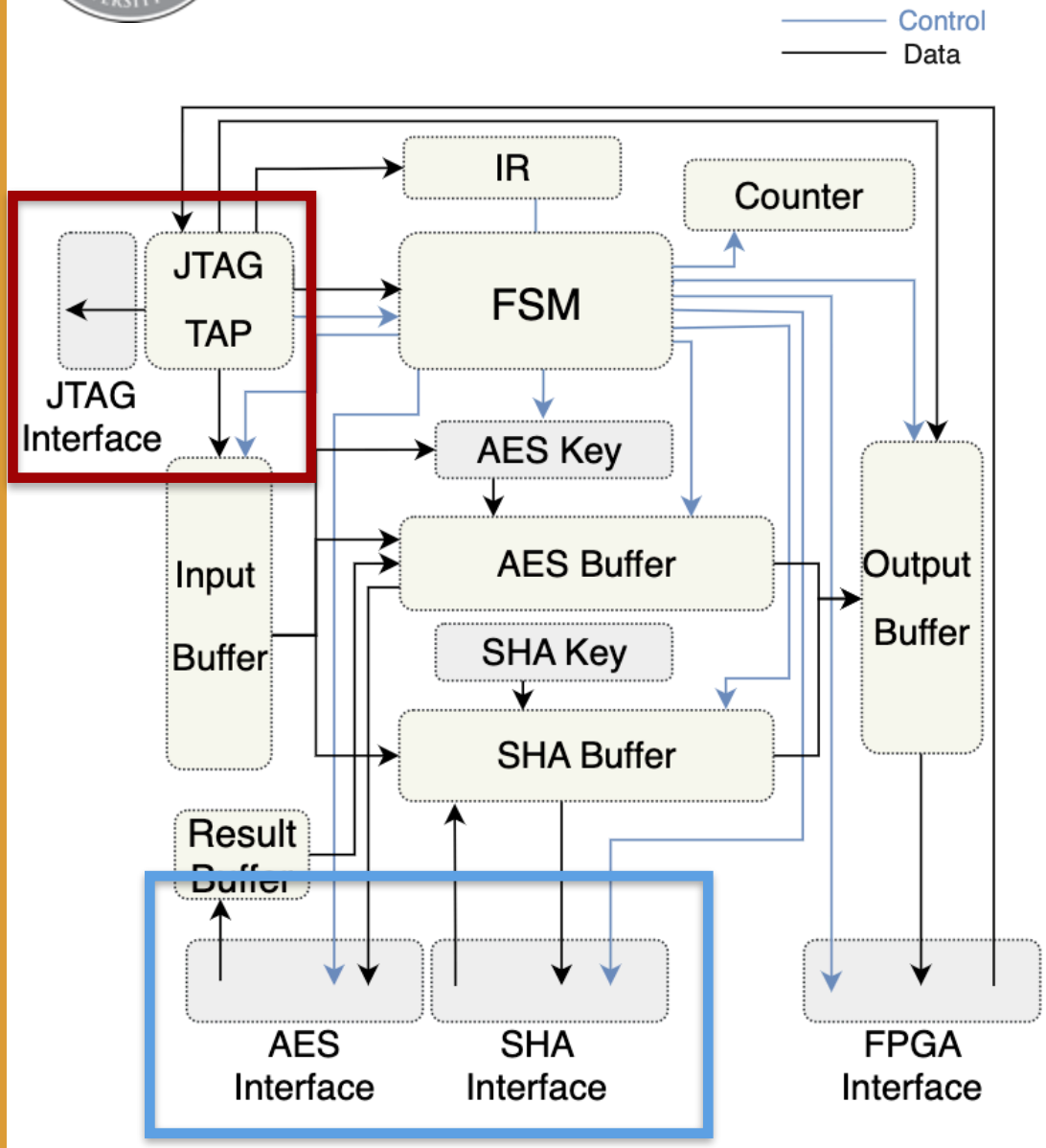
- Designed to be readily adaptable

PMU Core Block Diagram



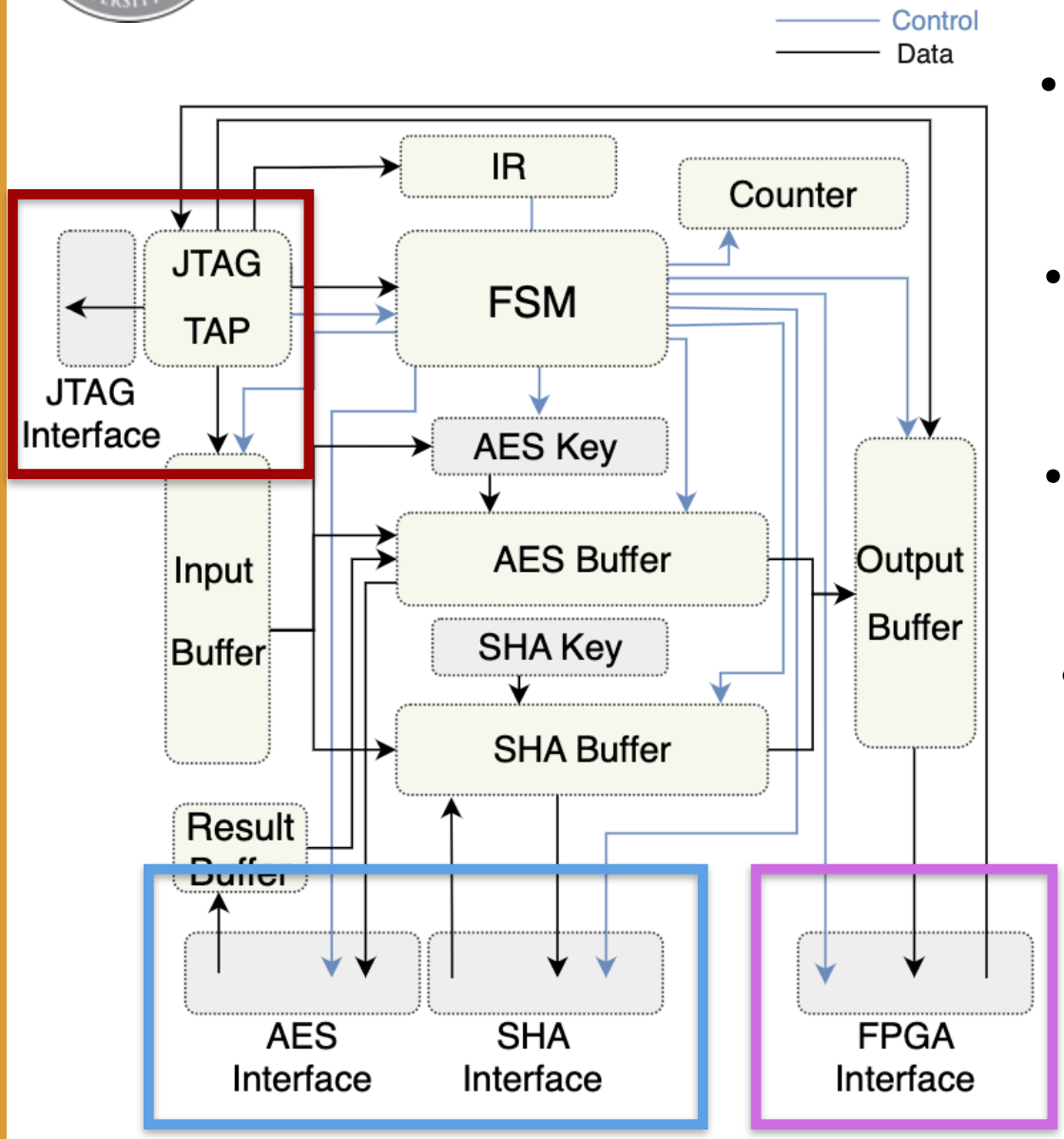
- Designed to be readily adaptable
- Communication Protocol
  - SPI, I2C, USB

PMU Core Block Diagram



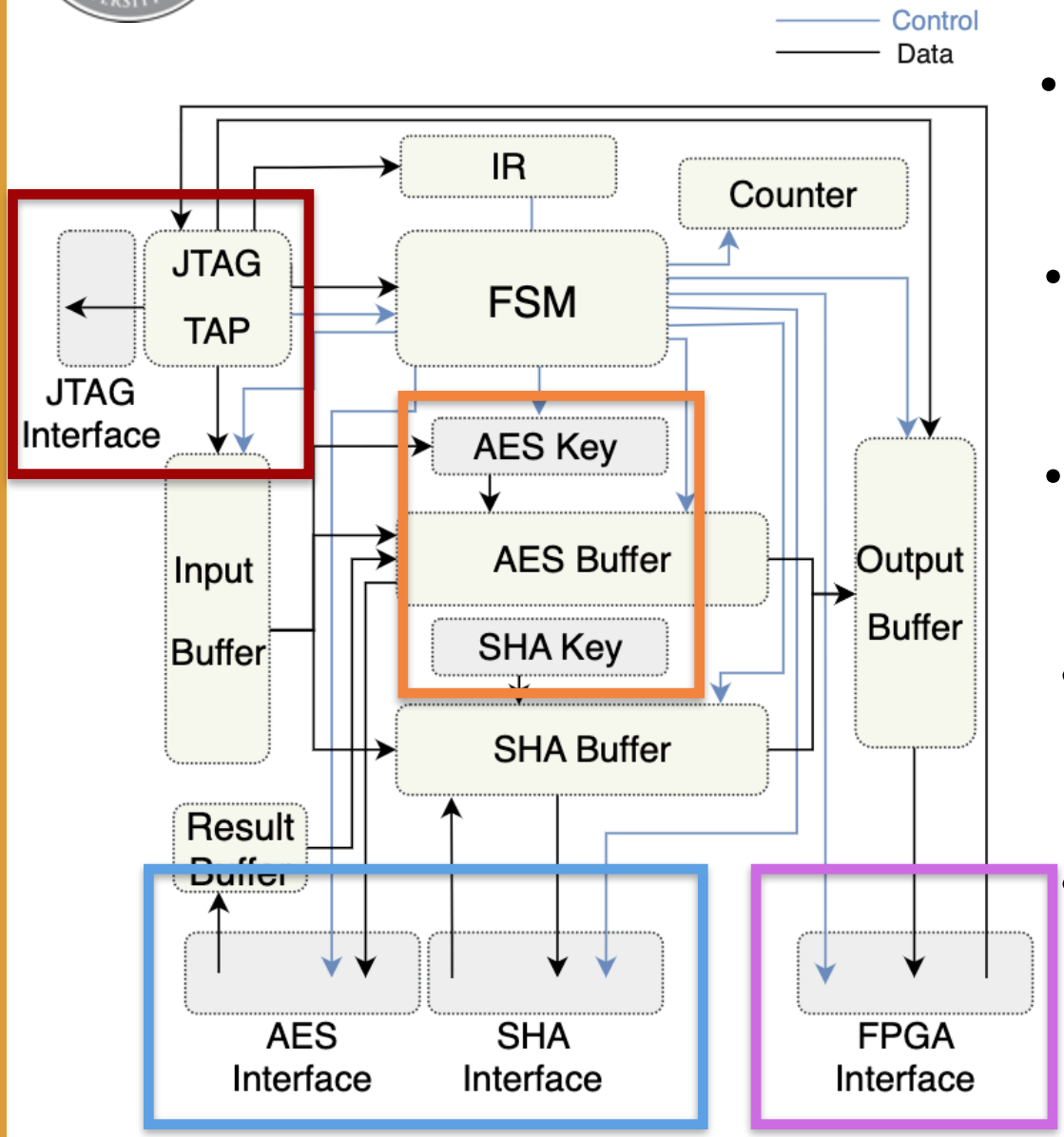
- Designed to be readily adaptable
- Communication Protocol
  - SPI, I2C, USB
- Cryptography
  - RSA, ECC, HMAC, DES

PMU Core Block Diagram



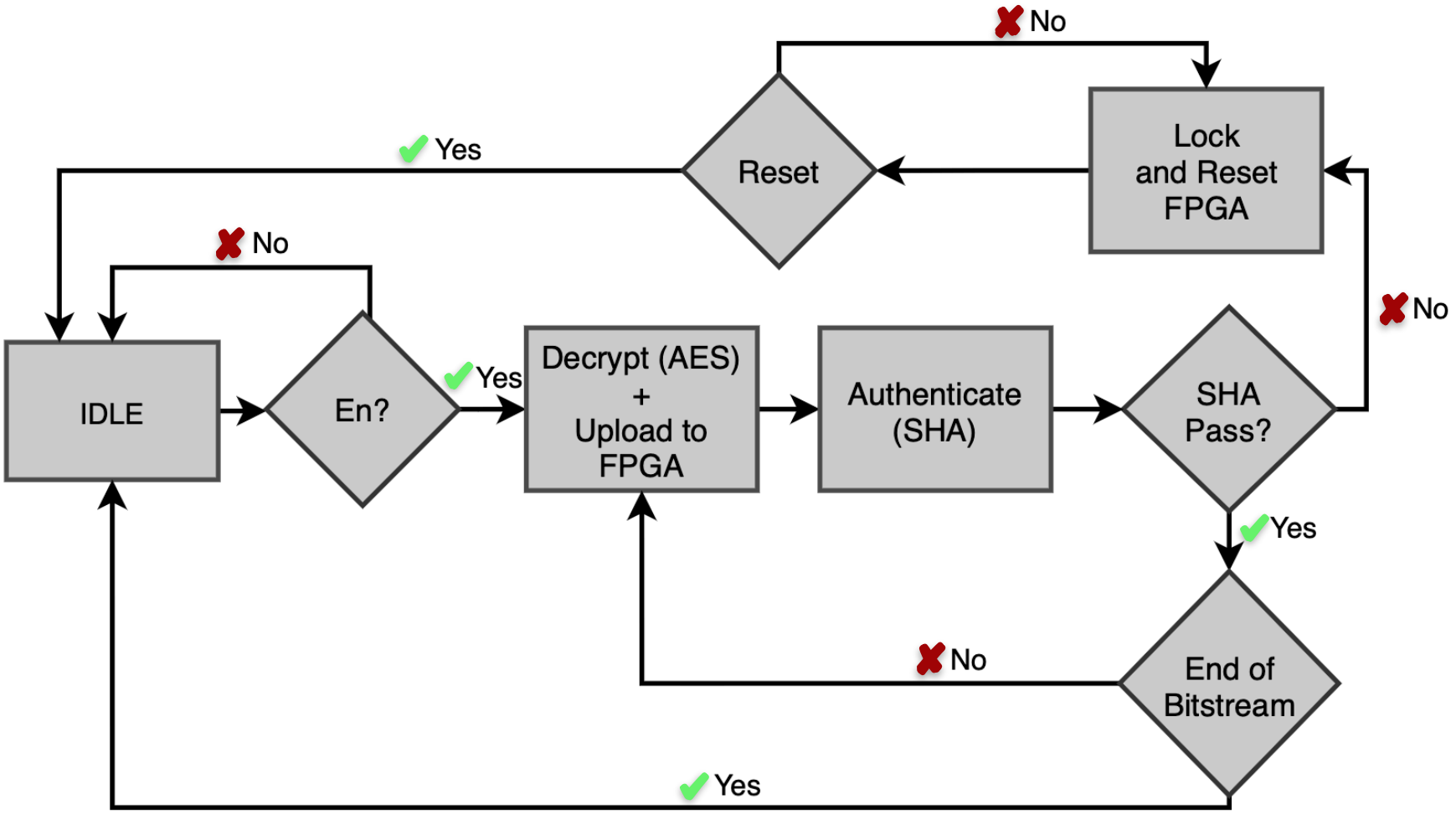
- Designed to be readily adaptable
- Communication Protocol
  - SPI, I2C, USB
- Cryptography
  - RSA, ECC, HMAC, DES
- Configuration Protocol
  - SRAM, Flash, Active Serial

PMU Core Block Diagram

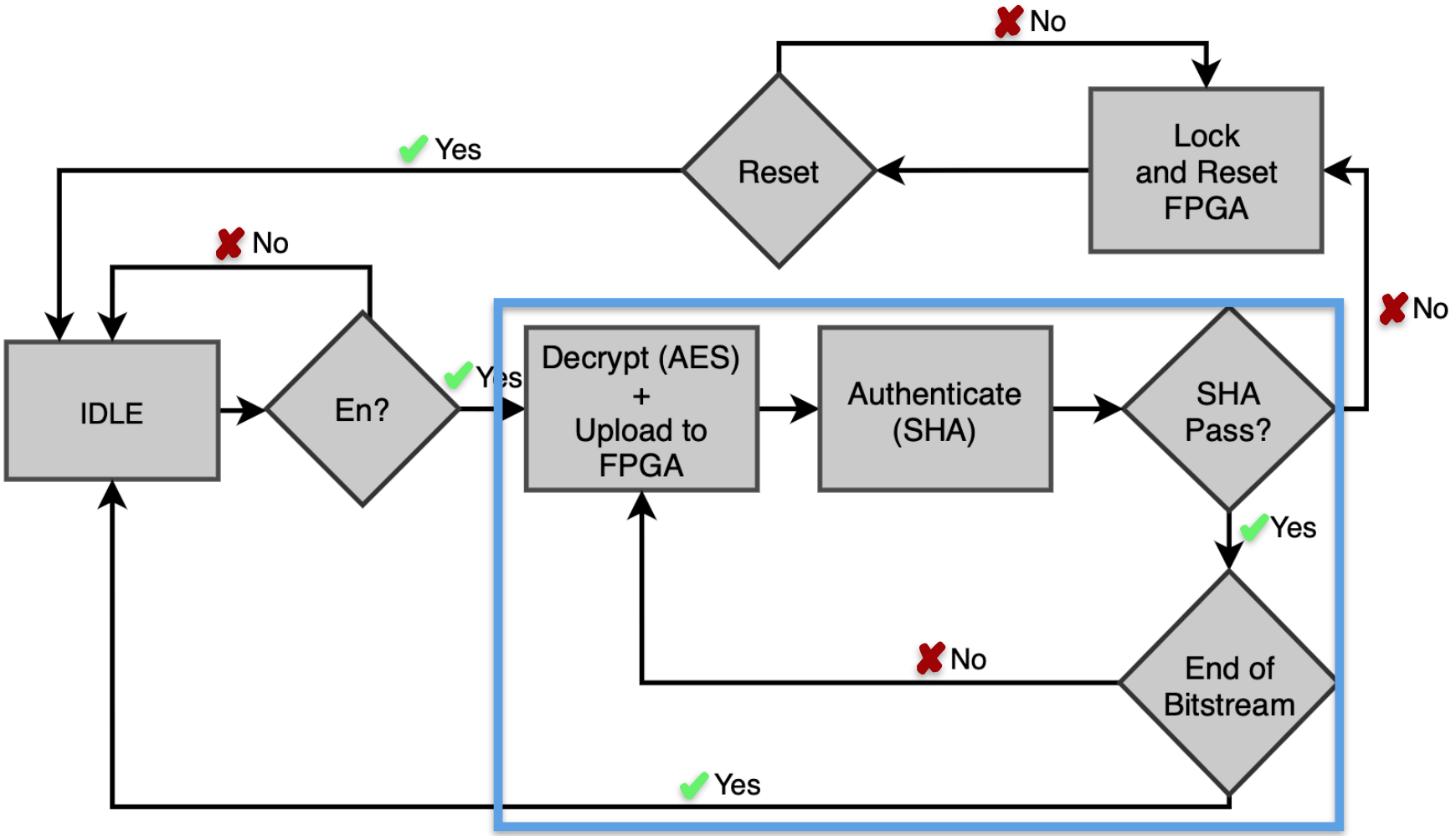


- Designed to be readily adaptable
- Communication Protocol
  - SPI, I2C, USB
- Cryptography
  - RSA, ECC, HMAC, DES
- Configuration Protocol
  - SRAM, Flash, Active Serial
- Key Storage
  - OTP Memory, PUF, Secure Element

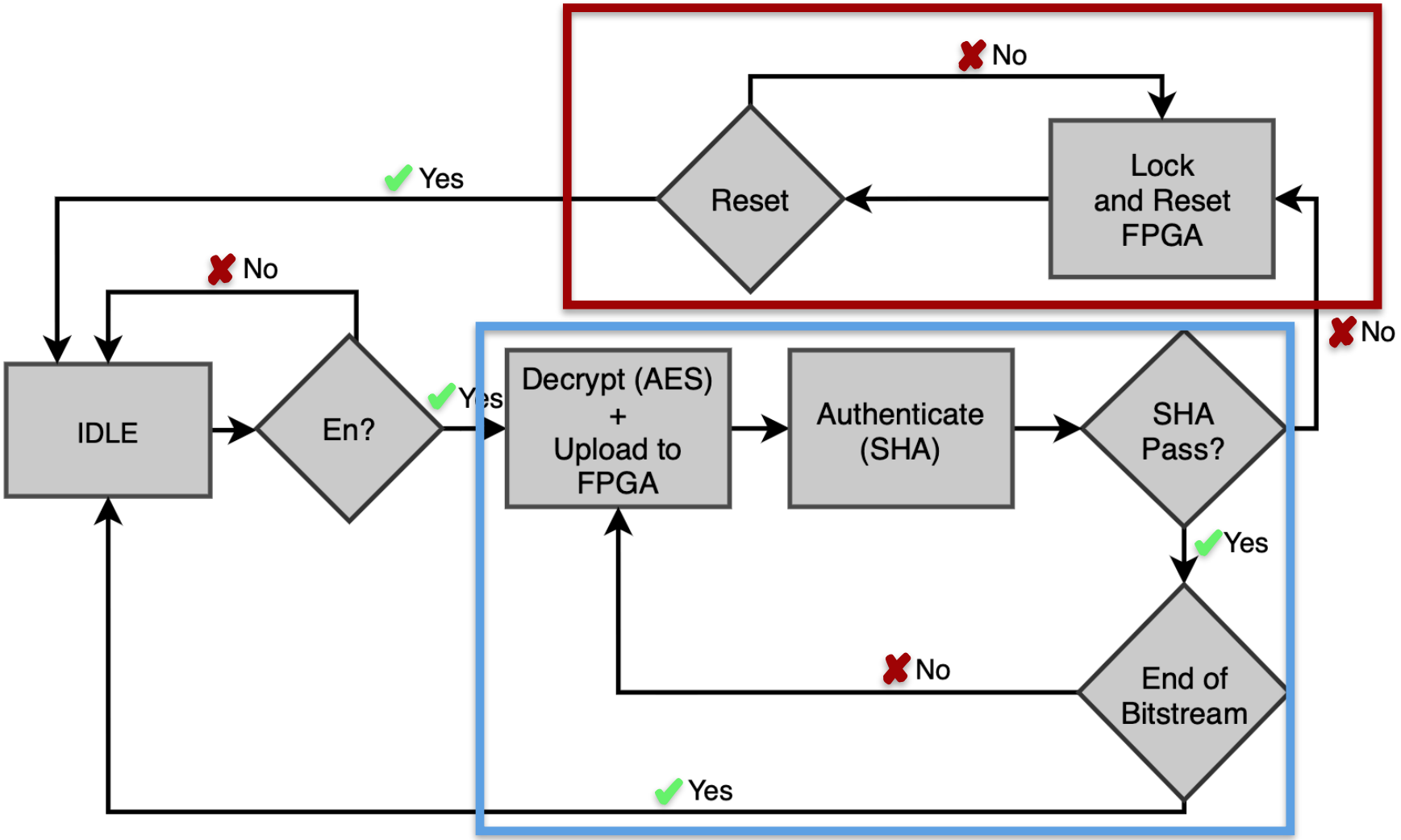
PMU Core Operation



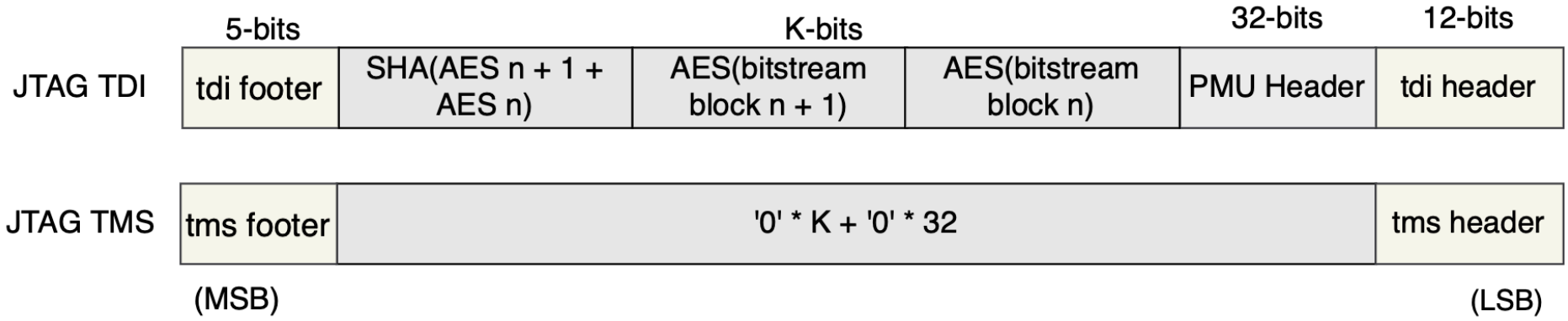
PMU Core Operation



PMU Core Operation



Encoding Scheme



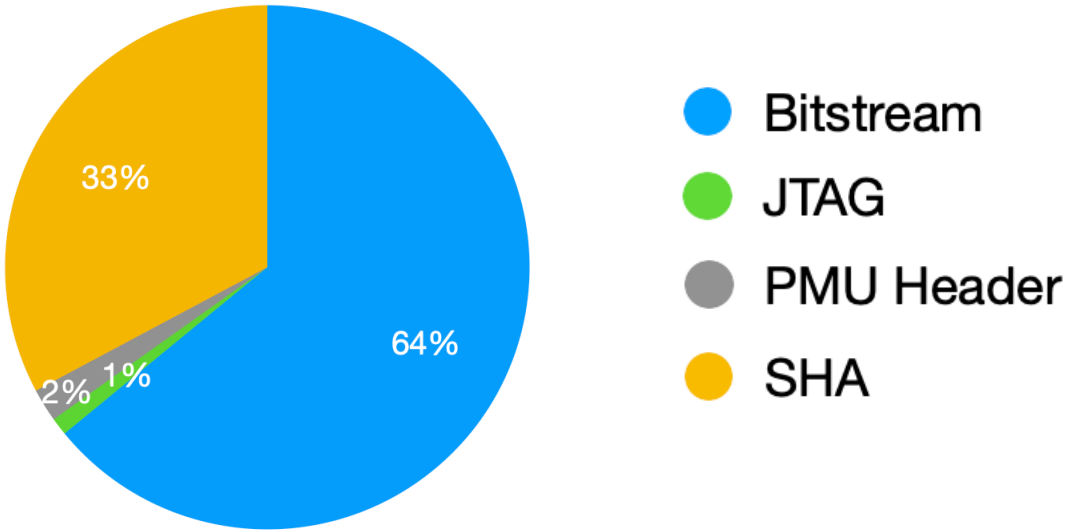
Encoding Scheme

	5-bits	K-bits		32-bits	12-bits
JTAG TDI	tdi footer	SHA(AES n + 1 + AES n)	AES(bitstream block n + 1)	AES(bitstream block n)	PMU Header	tdi header

JTAG TMS	tms footer	'0' * K + '0' * 32	tms header

(MSB) (LSB)

- Consider 1000-bit bitstream
  - SHA evaluation every 500-bits



Encoding Scheme

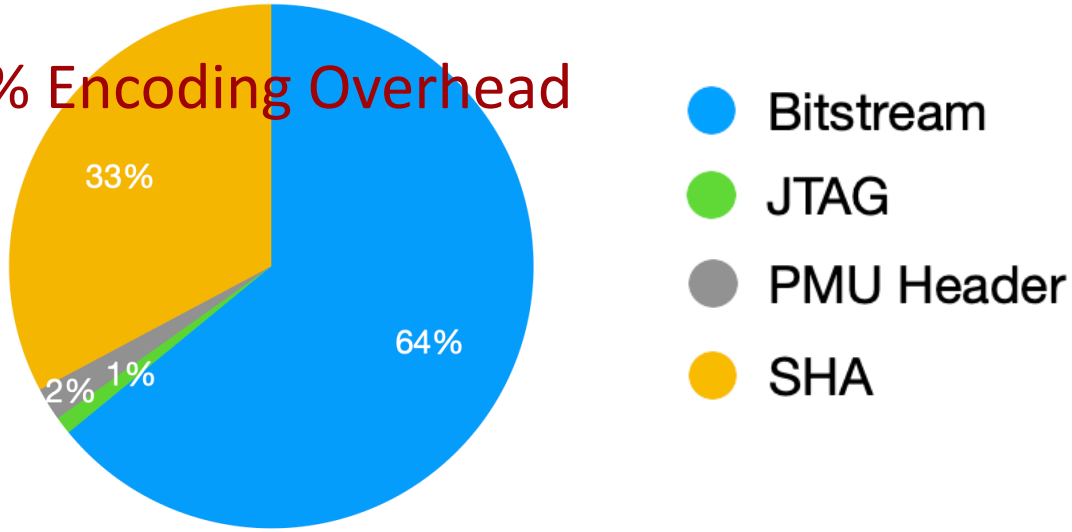
	5-bits	K-bits		32-bits	12-bits
JTAG TDI	tdi footer	SHA(AES n + 1 + AES n)	AES(bitstream block n + 1)	AES(bitstream block n)	PMU Header	tdi header

JTAG TMS	tms footer	'0' * K + '0' * 32	tms header

(MSB) (LSB)

- Consider 1000-bit bitstream
  - SHA evaluation every 500-bits

36% Encoding Overhead



Encoding Scheme

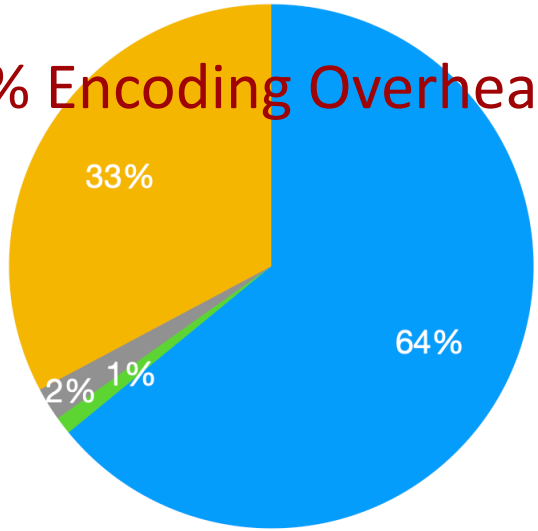
	5-bits	K-bits			32-bits	12-bits
JTAG TDI	tdi footer	SHA(AES n + 1 + AES n)	AES(bitstream block n + 1)	AES(bitstream block n)	PMU Header	tdi header

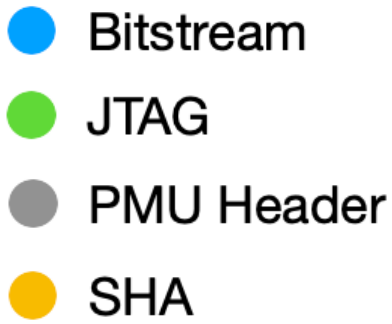
JTAG TMS	tms footer	'0' * K + '0' * 32	tms header

(MSB) (LSB)

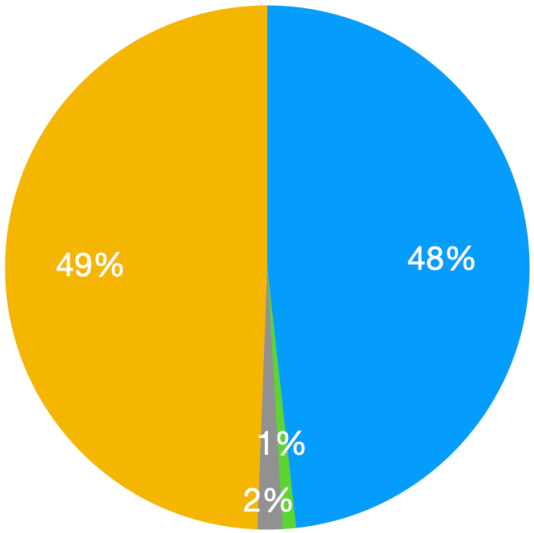
- Consider 1000-bit bitstream
  - SHA evaluation every 500-bits

36% Encoding Overhead





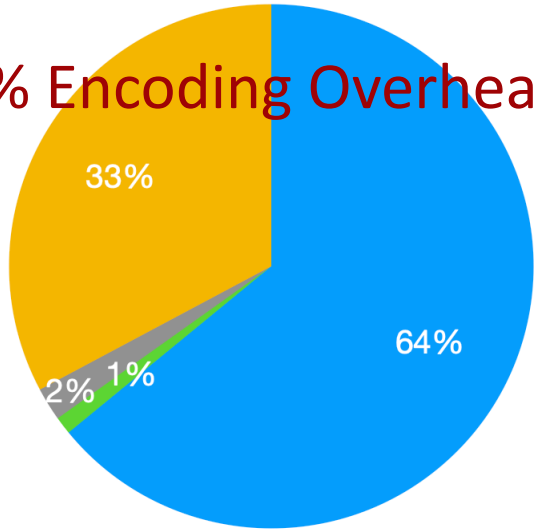
- Consider 1000-bit bitstream
  - SHA evaluation every 250-bits

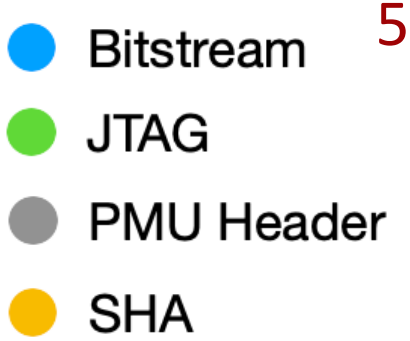


Encoding Scheme

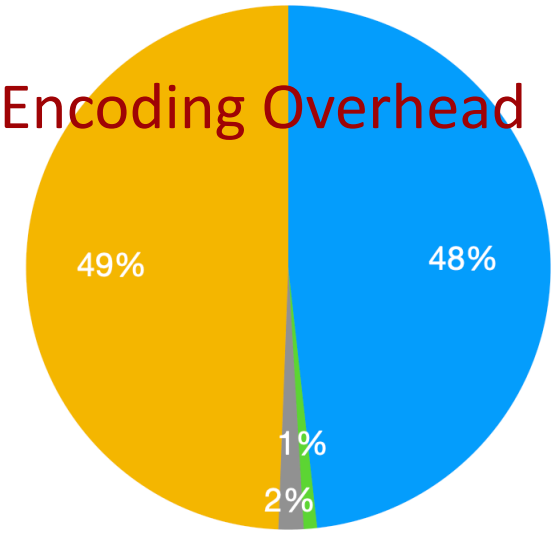
	5-bits	K-bits			32-bits	12-bits
JTAG TDI	tdi footer	SHA(AES n + 1 + AES n)	AES(bitstream block n + 1)	AES(bitstream block n)	PMU Header	tdi header
JTAG TMS	tms footer	'0' * K + '0' * 32				tms header
	(MSB)					(LSB)

- Consider 1000-bit bitstream
  - SHA evaluation every 500-bits

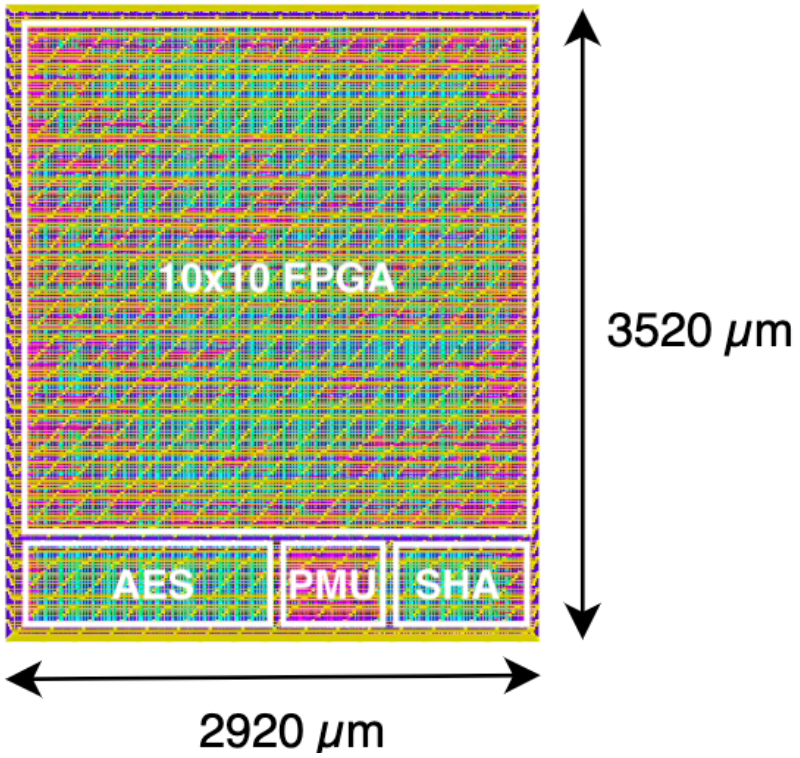




- Consider 1000-bit bitstream
  - SHA evaluation every 250-bits



Silicon Integration to Caravel SoC



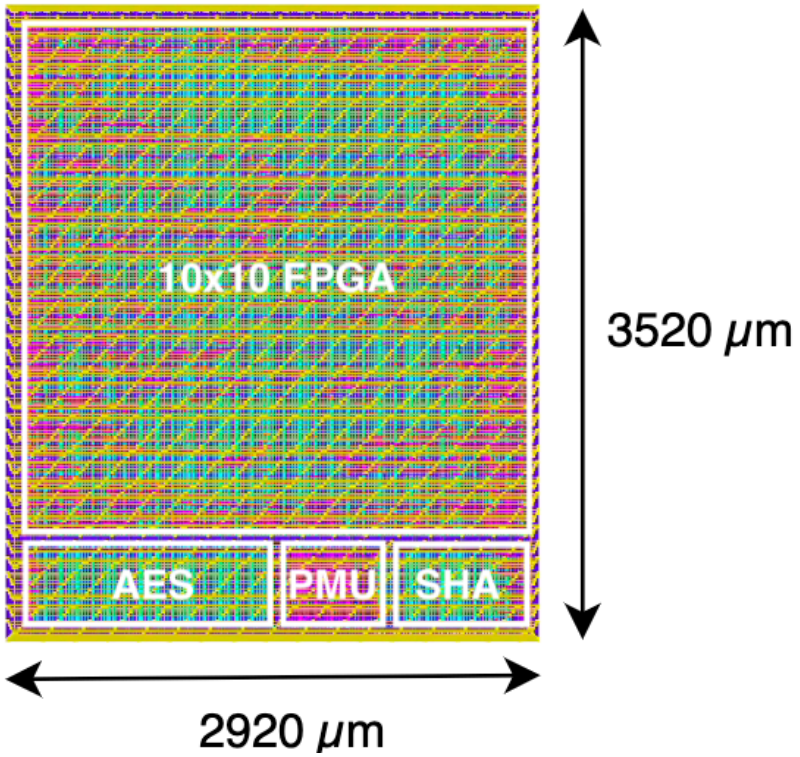
SiliconCompiler

Google + efabless.com

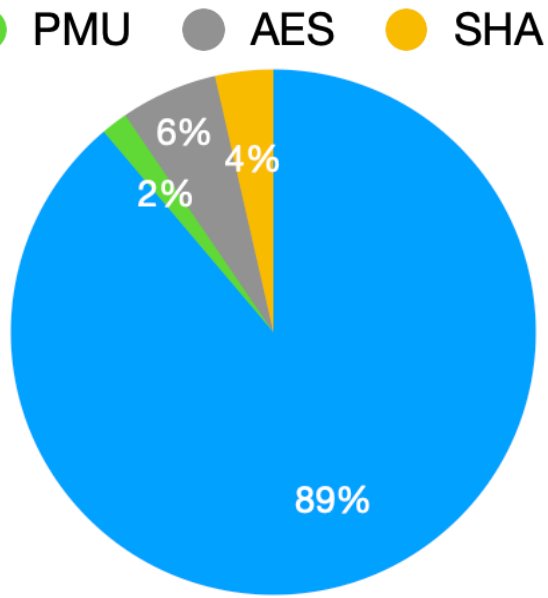
skywater TECHNOLOGY

PENFPGA

Silicon Integration to Caravel SoC



- Area (µm²)



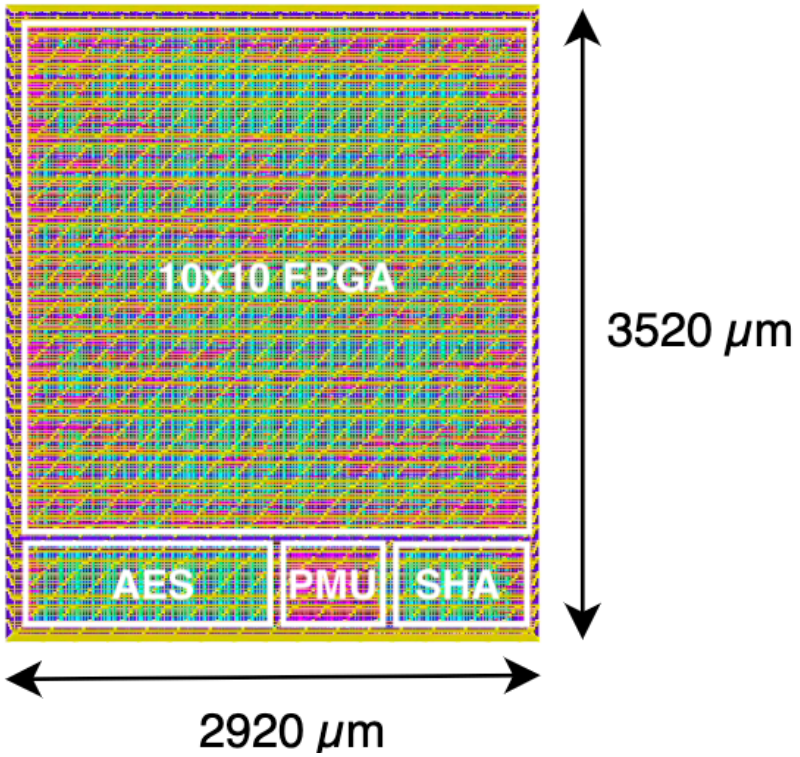
SiliconCompiler

Google + efabless.com

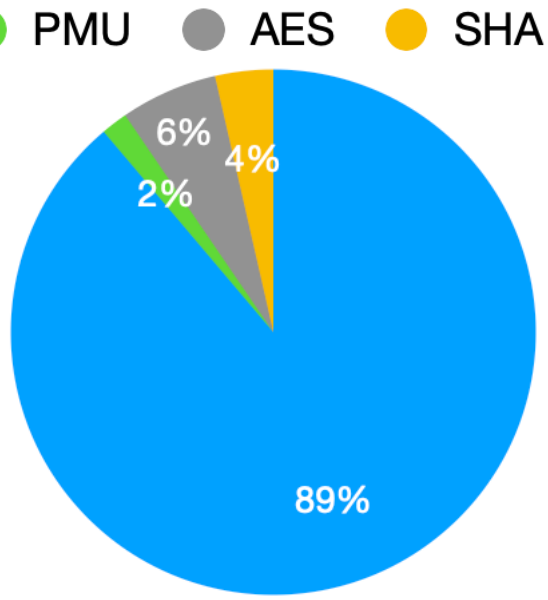
skywater TECHNOLOGY

PENFPGA

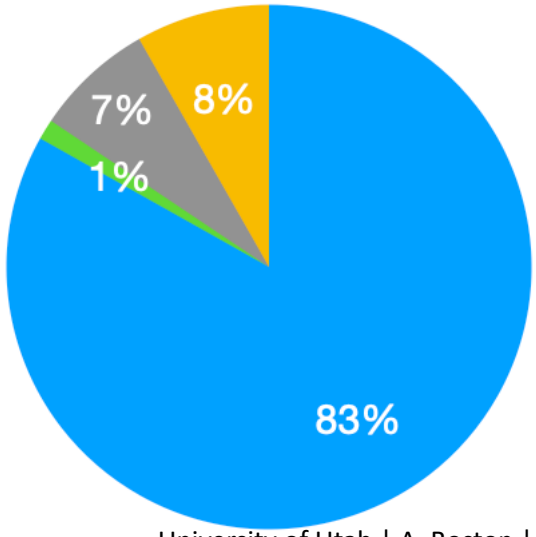
Silicon Integration to Caravel SoC



- Area (µm²)



- Power (W)



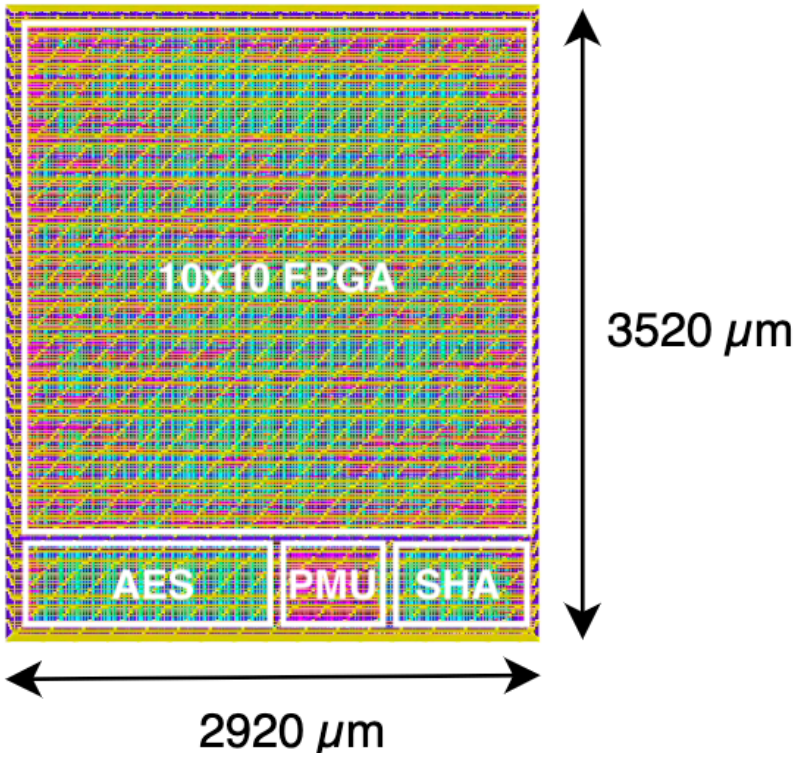
SiliconCompiler

Google + efabless.com

skywater TECHNOLOGY

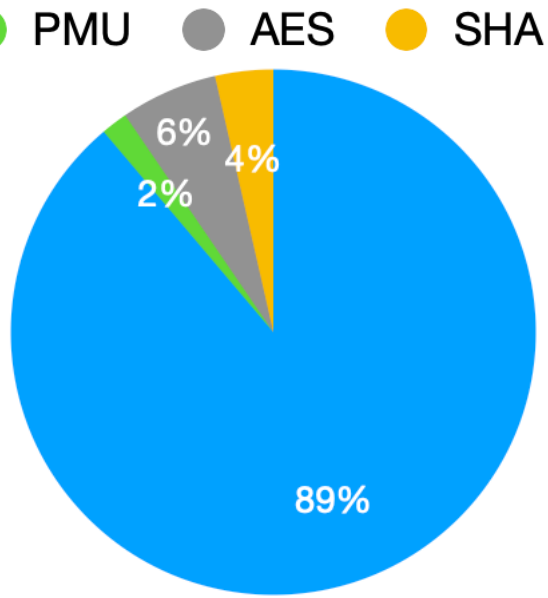
PENFPGA

Silicon Integration to Caravel SoC



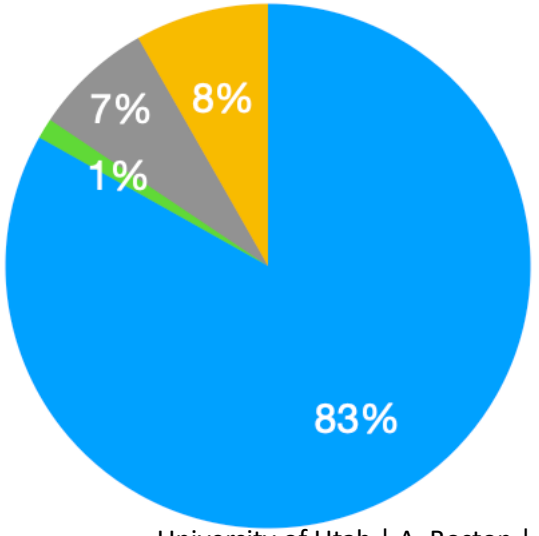
- Area (µm²)

12% Area Overhead



- Power (W)

16% Power Overhead



SiliconCompiler

Google + efabless.com

skywater TECHNOLOGY

PEN FPGA

Summary

- First open-source core specifically dedicated to FPGA configuration
- Flexible HW/SW template framework
- Enables secure and accurate FPGA configuration
- Demonstrated system integration utilizing open-source ecosystem

PMU Github:

https://github.com/lnis-uofu/FPGA_Secured_Bitstream

LNIS Laboratory for NanoIntegrated Systems

Thank you for your attention

Laboratory for NanoIntegrated Systems
Department of Electrical and Computer Engineering
MEB building – University of Utah – Salt Lake City – UT – USA