COMMON EVALUATION PLATFORM

A Surrogate System on Chip (SoC) for Security Assessments

Brendon Chetwynd

10 April 2019

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

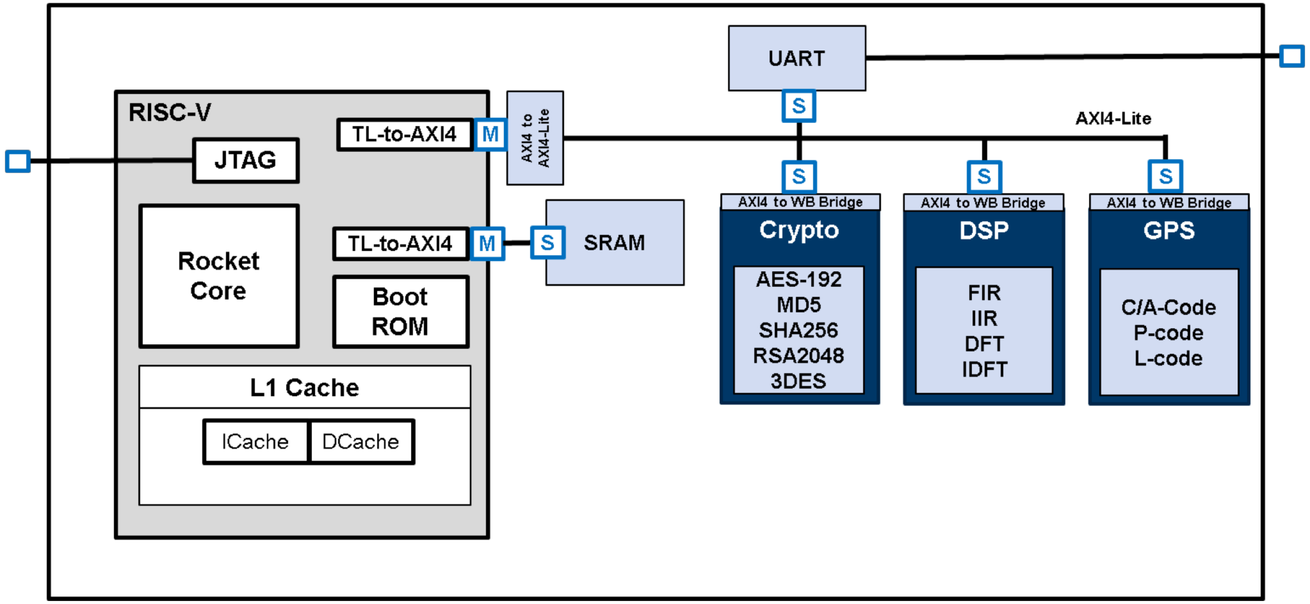
Outline

- CEP Background
- AISS Role
- Next Steps
- Summary

CEP Overview

COMMON EVALUATION PLATFORM

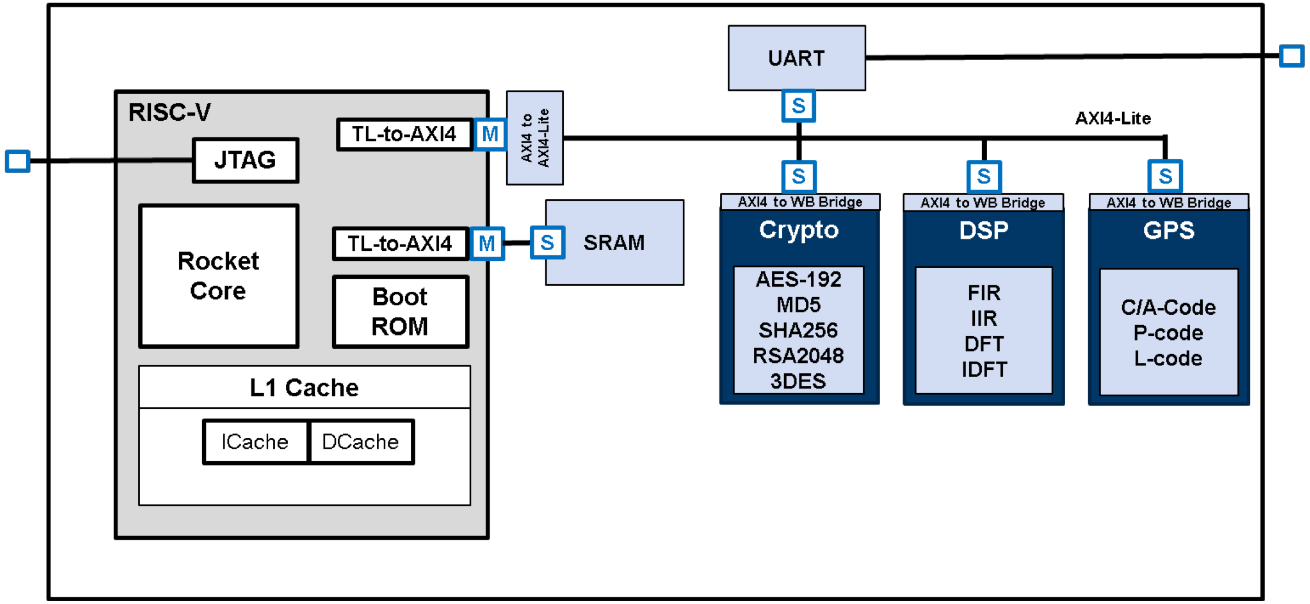
CEP 2.0 High-level Architecture



CEP Overview

COMMON EVALUATION PLATFORM

CEP 2.0 High-level Architecture



Feature Highlights

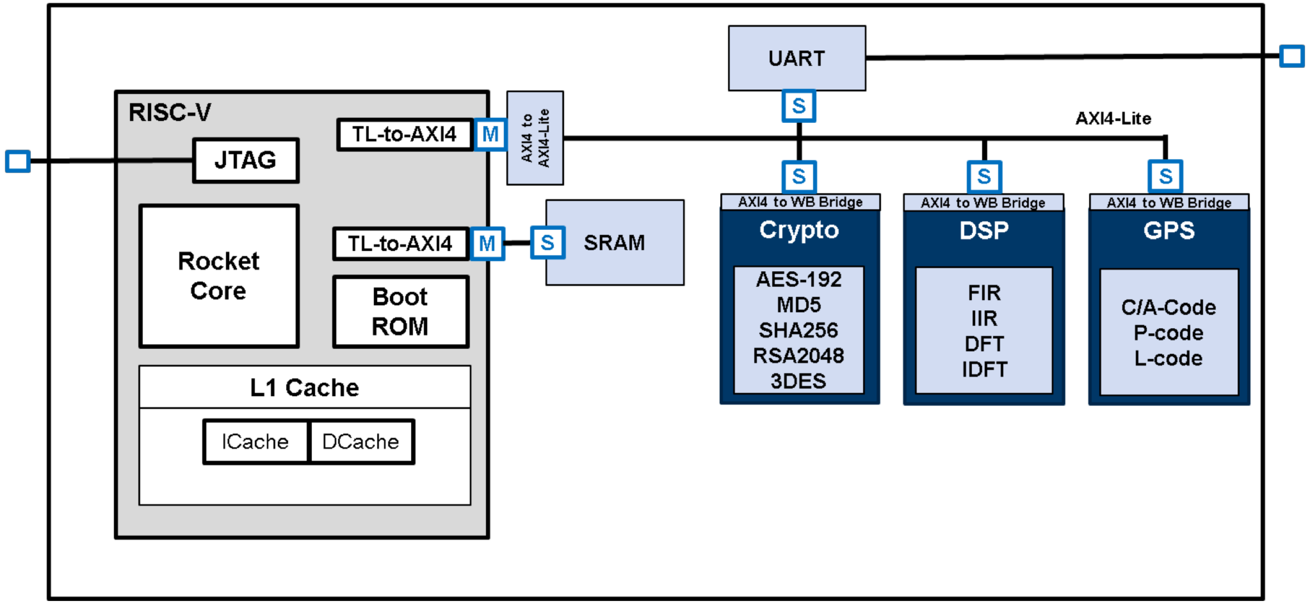
- Accelerators for common DoD functions including DSP and secure communications
- Verification test suite for validating baseline functionality
- Annotated / labeled security-sensitive design elements

DoD – Department of Defense, DSP – Digital Signal Processing

CEP Overview

COMMON EVALUATION PLATFORM

CEP 2.0 High-level Architecture



Feature Highlights

– Accelerators for common DoD functions including DSP and secure communications
– Verification test suite for validating baseline functionality
– Annotated / labeled security-sensitive design elements

An open-source benchmark-enabling design

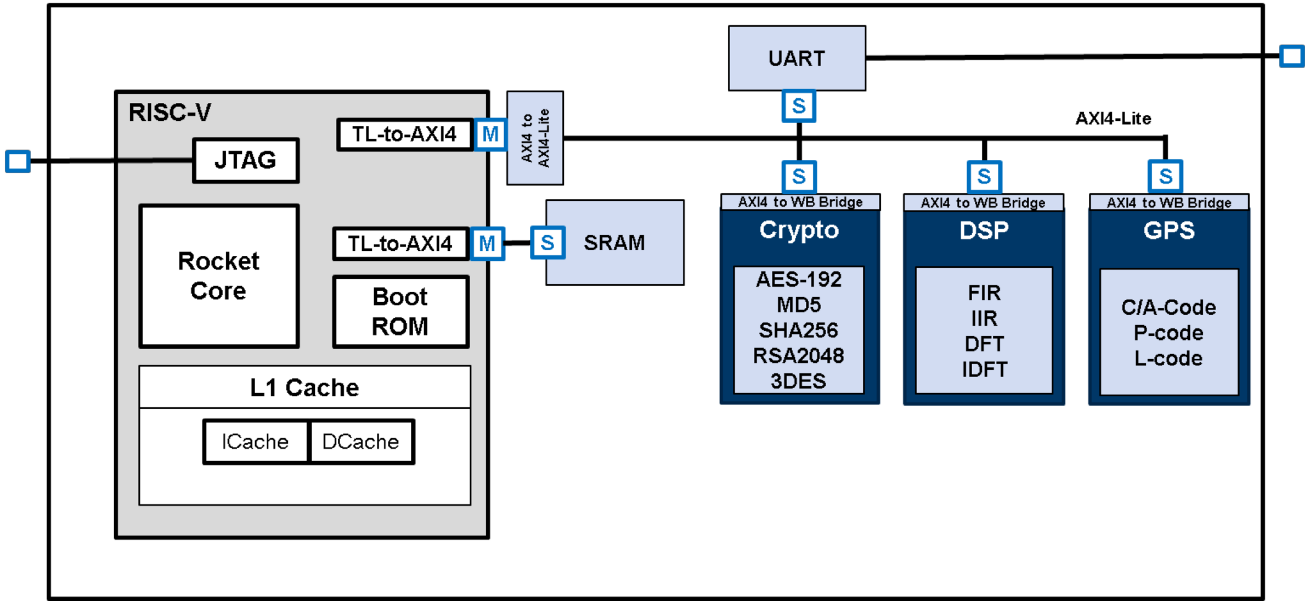
– **Scale**:
  - Sufficient SoC complexity to stress defensive tool-flows and IP
– **Diversity**:
  - Mission-relevant surrogate modules offer diversity of functions
– **Releasability**:
  - Open-source license module permits free distribution to all performers
– **Extensibility**:
  - Module approach offers easy adaptation to meet emerging program objectives

IP – Intellectual Property

CEP Overview

COMMON EVALUATION PLATFORM

CEP 2.0 High-level Architecture



Feature Highlights

- Accelerators for common DoD functions including DSP and secure communications
- Verification test suite for validating baseline functionality
- Annotated / labeled security-sensitive design elements

An open-source benchmark-enabling design

- **Scale**:
  - Sufficient SoC complexity to stress defensive tool-flows and IP
- **Diversity**:
  - Mission-relevant surrogate modules offer diversity of functions
- **Releasability**:
  - Open-source license module permits free distribution to all performers
- **Extensibility**:
  - Module approach offers easy adaptation to meet emerging program objectives

The CEP is an extensible, license-unencumbered surrogate SoC that will enable evaluation of AISS tools and techniques

CEP – Security Reference Architecture

COMMON EVALUATION PLATFORM

Benefit to performers:
Enables developmental test and evaluation of security techniques on surrogate system

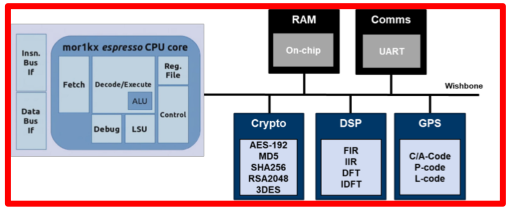
Benefits to transition partners:
Enables risk-reducing collaboration with sensitive project tapeouts and program schedules

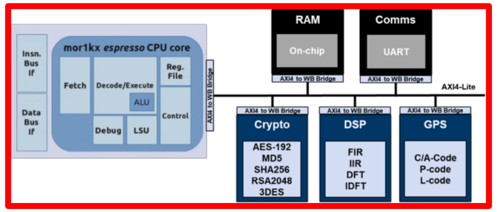
An open-source benchmark-enabling design

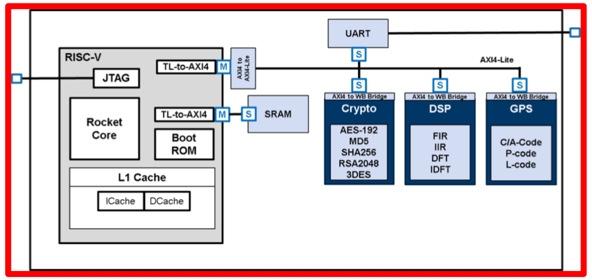
– **Scale:**
  - **Sufficient SoC complexity to stress defensive tool-flows and IP**
– **Diversity:**
  - **Mission-relevant surrogate modules offer diversity of functions**
– **Releasability:**
  - **Open-source license module permits free distribution to all performers**
– **Extensibility:**
  - **Module approach offers easy adaptation to meet emerging program objectives**

CEP Roadmap (to date)

COMMON EVALUATION PLATFORM







CEP Version	v1.1	v1.2	v2.0
Processor	mor1k	mor1k	RISC-V*
Bus	Wishbone	AXI4-Lite	AXI4-Lite
OS Support	None	None	None
ASIC Optimized	- Minimized FPGA specific logic		
Test Suite / Documentation / Other	• Unit C code (sim + HW) • Expanded documentation	• Unit C code (sim + HW) • Waveforms (sim) • Regression (sim + HW)	• Unit C code (sim + HW) • Waveforms (sim) • Regression (sim + HW)
Languages	Verilog	SystemVerilog, Verilog, VHDL	Mixed + Chisel
Release Date	July '18 ✓	Nov '18 ✓	Apr '19
Notes			• Labeled Security Targets • Misc. Code Cleanup

*Air Force Research Lab RISC-V / University of California Berkley Rocket Chip

OS – Operating System, RISC – Reduced Instruction Set Computer, AXI – Advanced Extensible Interface, FPGA – Field Programmable Gate Array, HW – Hardware, sim – Simulation, VHDL – VHSIC Hardware Description Language

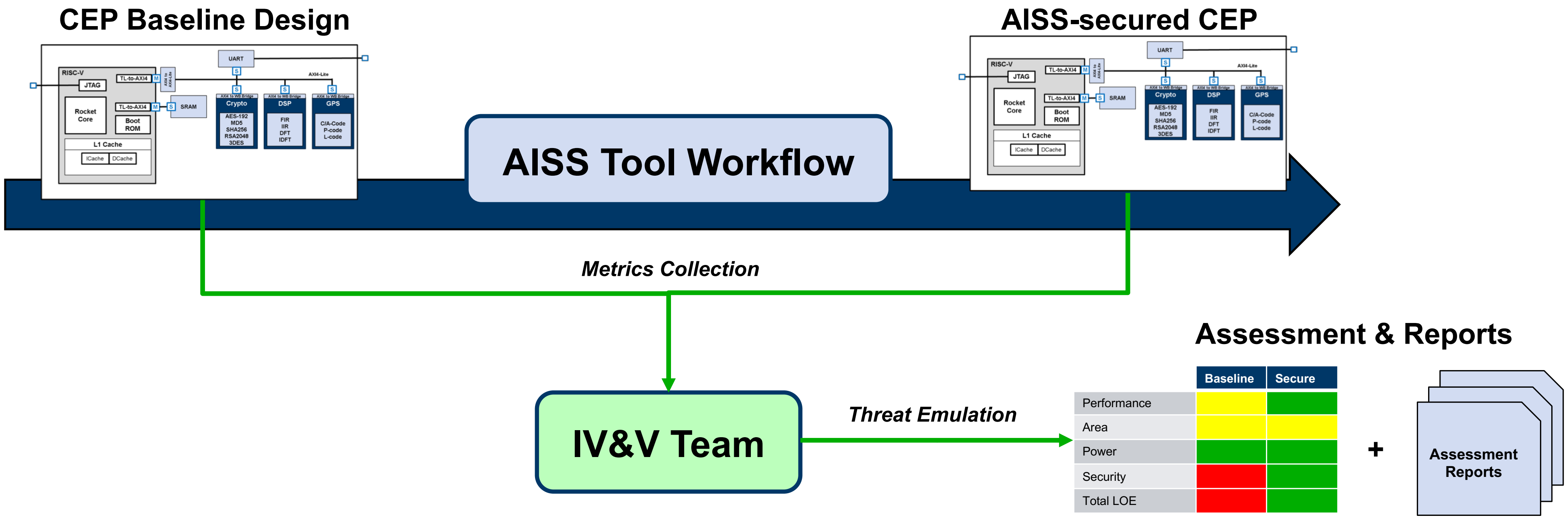
Outline

COMMON EVALUATION PLATFORM

- CEP Background
- AISS Role
- Next Steps
- Summary

AISS Application: Reference Architecture for IV&V

COMMON EVALUATION PLATFORM



- CEP reference architecture can be run through AISS tool workflow
- Independent Verification & Validation (IV&V) team collects metrics (performance, security, and design efficiency)
- Assessments and reports facilitated by reference architecture comparison

IC Security Challenges & CEP Role

DARPA On-chip Security Reference Model
Malicious Hardware insertion of hidden functionality secretly triggered to deliver disruptive payloads
Reverse Engineering interpret design intent from available and derived representation to understand secret or confidential algorithms
Side Channel extract secret information from the IC through communication channels other than those intended by the design
Supply Chain non-genuine IC sold as real, but realized through cloning, counterfeiting, recycling, remarking

IC – Integrated Circuit

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

IC Security Challenges & CEP Role

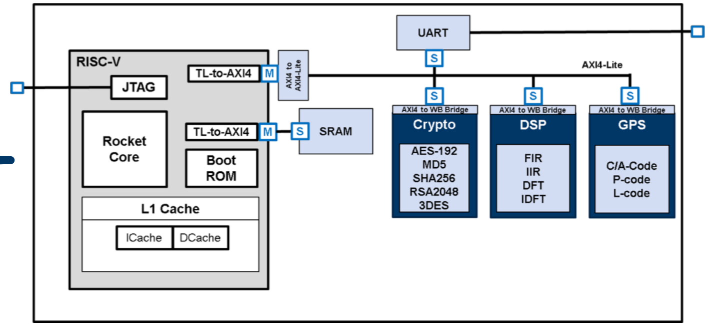
DARPA On-chip Security Reference Model	Security Objectives
Malicious Hardware insertion of hidden functionality secretly triggered to deliver disruptive payloads	**1. Design Integrity** USG seeks to make make malicious modifications either ***infeasible*** *or* readily ***detectable***
Reverse Engineering interpret design intent from available and derived representation to understand secret or confidential algorithms	**2. Design Confidentiality** USG seeks to make: 2.a. The SoC not available to non-approved users, or 2.b. RE intractable for the lifetime of the IP block
Side Channel extract secret information from the IC through communication channels other than those intended by the design	**3. Data Confidentiality** USG seeks to protect data running on the deployed chip, protecting critical information *in situ.*
Supply Chain non-genuine IC sold as real, but realized through cloning, counterfeiting, recycling, remarking	**4. Device Integrity** USG seeks to detect and prevent deployment of non-authentic or non-genuine parts

USG – United States Government, RE – Reverse Engineering, IP – Intellectual Property

IC Security Challenges & CEP Role

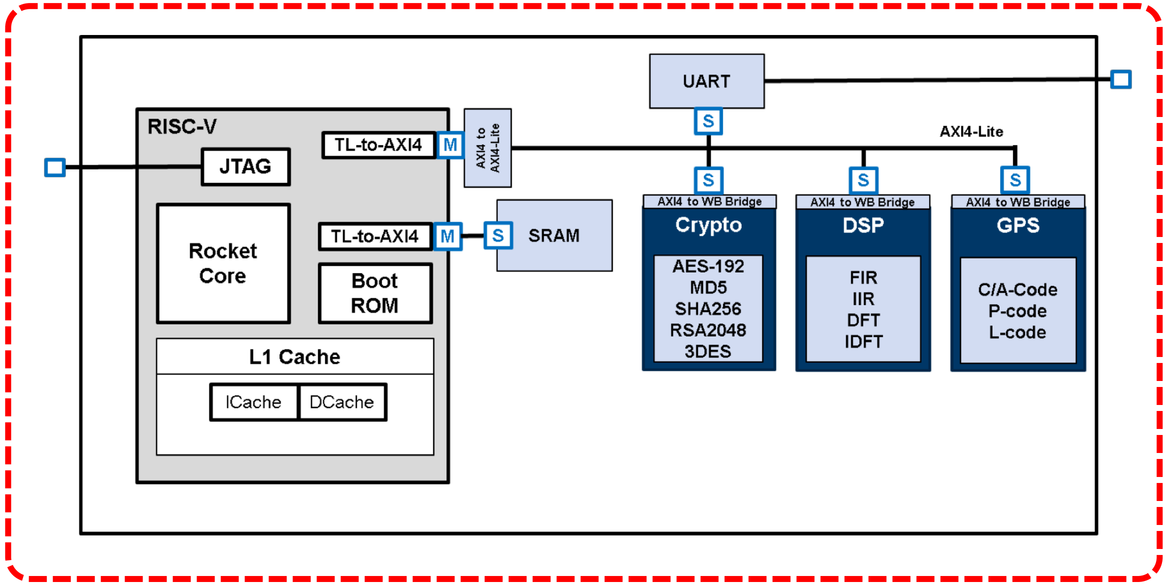
DARPA On-chip Security Reference Model	Security Objectives
Malicious Hardware insertion of hidden functionality secretly triggered to deliver disruptive payloads	**1. Design Integrity** USG seeks to make make malicious modifications either ***infeasible*** *or* readily ***detectable***
Reverse Engineering interpret design intent from available and derived representation to understand secret or confidential algorithms	**2. Design Confidentiality** USG seeks to make: 2.a. The SoC not available to non-approved users, or 2.b. RE intractable for the lifetime of the IP block
Side Channel extract secret information from the IC through communication channels other than those intended by the design	**3. Data Confidentiality** USG seeks to protect data running on the deployed chip, protecting critical information *in situ.*
Supply Chain non-genuine IC sold as real, but realized through cloning, counterfeiting, recycling, remarking	**4. Device Integrity** USG seeks to detect and prevent deployment of non-authentic or non-genuine parts

Common Evaluation Platform



AISS Application:
Benchmarking Security Techniques w/ Evaluation Targets

COMMON EVALUATION PLATFORM



1: Design Integrity: Labeled security-critical (SC) wires identify targets for Trojan to influence or effect

Enables evaluation *of AISS technique's ability to protect security-critical wires from modification, i.e. "Malicious Hardware"*

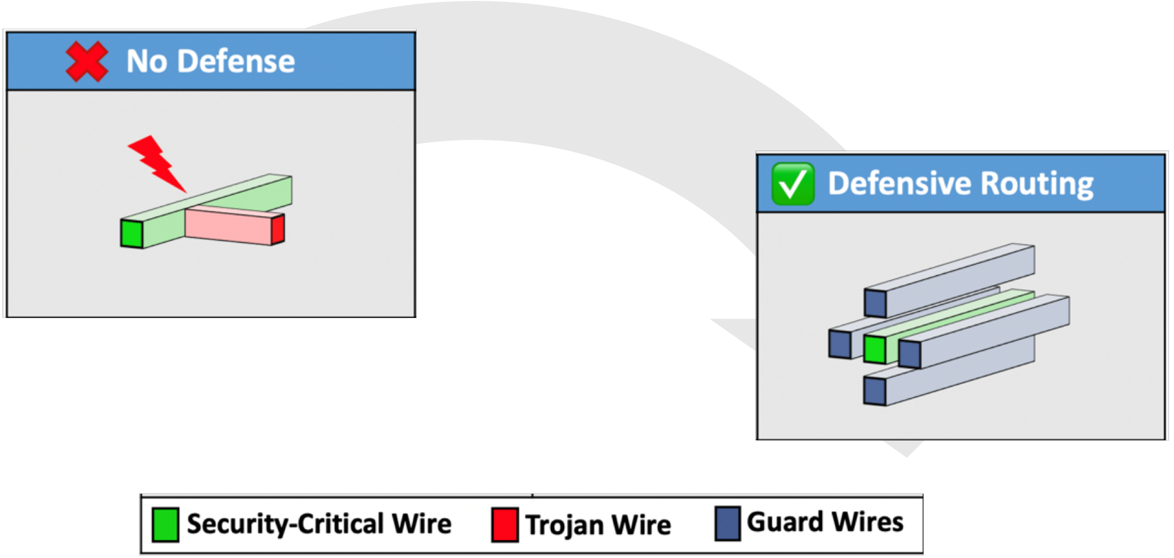
2: Design Confidentiality

3: Data Confidentiality

4: Device Integrity

Example: automated application of guard wires during routing, scaled to the available size tolerance

Increased quantity and diversity of guard wires

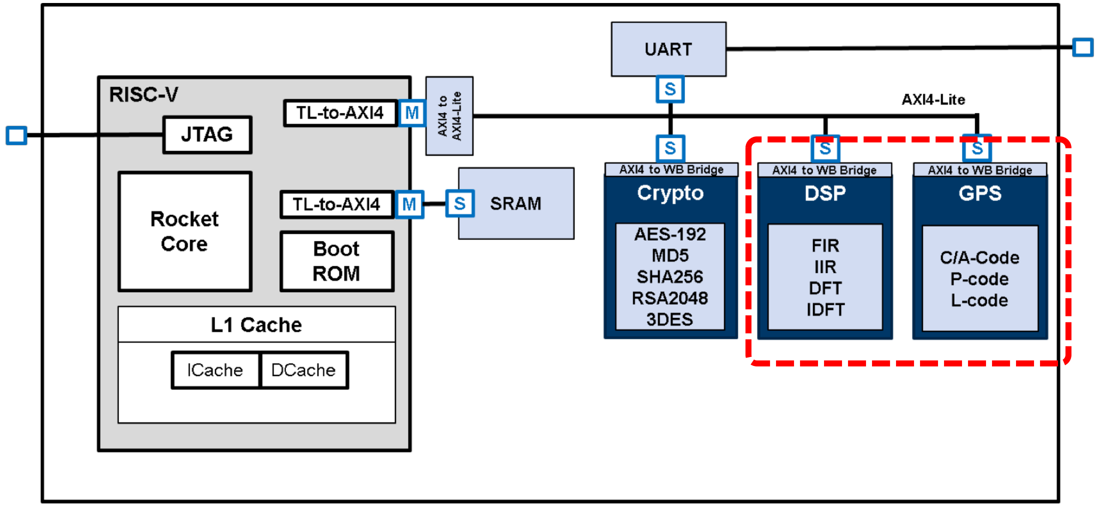


Bush, Hicks, Trippel, "Defensive Routing and Related Techniques", USPTO Provisional 62792012

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

AISS Application:
Benchmarking Security Techniques w/ Evaluation Targets

COMMON EVALUATION PLATFORM



1: Design Integrity

2: Design Confidentiality: Labeled accelerators representative of DoD protected designs

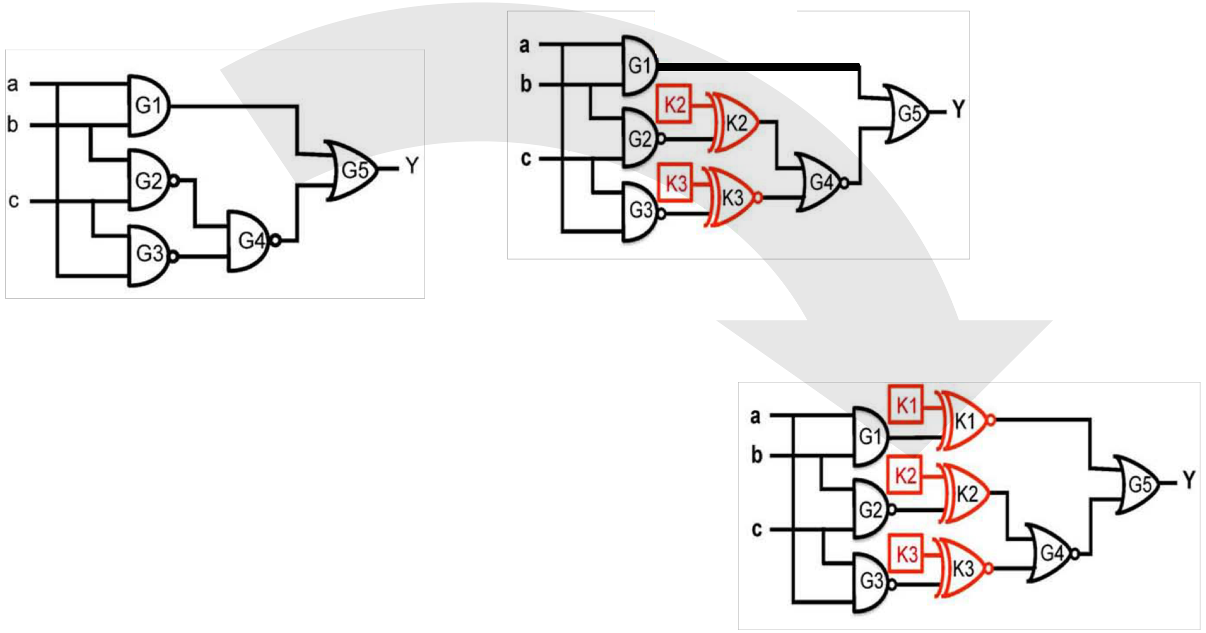
Enables evaluation *of AISS technique's ability to prevent IP theft or mis-use, i.e. "Reverse Engineering"*

3: Data Confidentiality

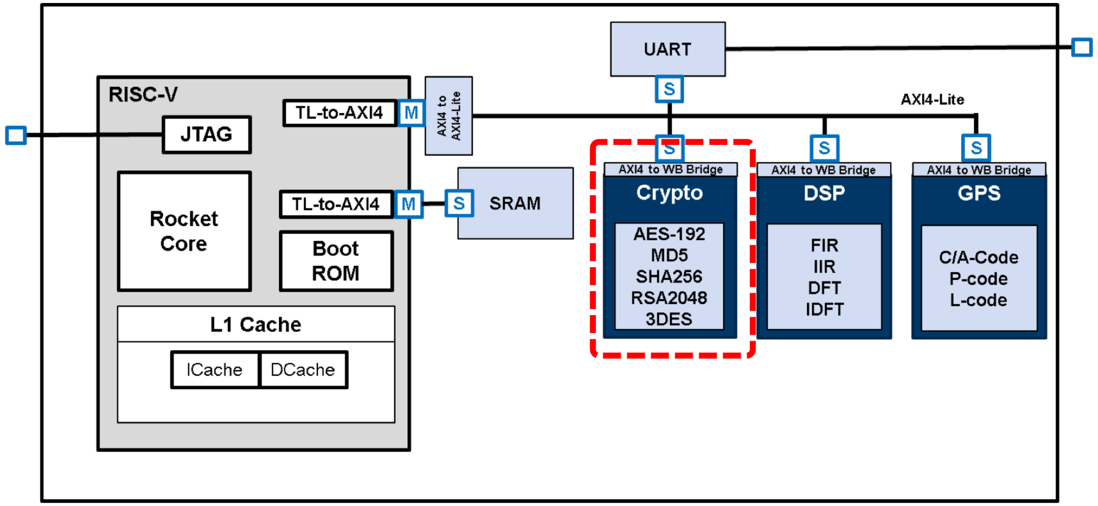
4: Device Integrity

Example: automated application of Logic Locking, scaled to the available size, area, and performance constraints

Scaled quantity and position of inverters and bits

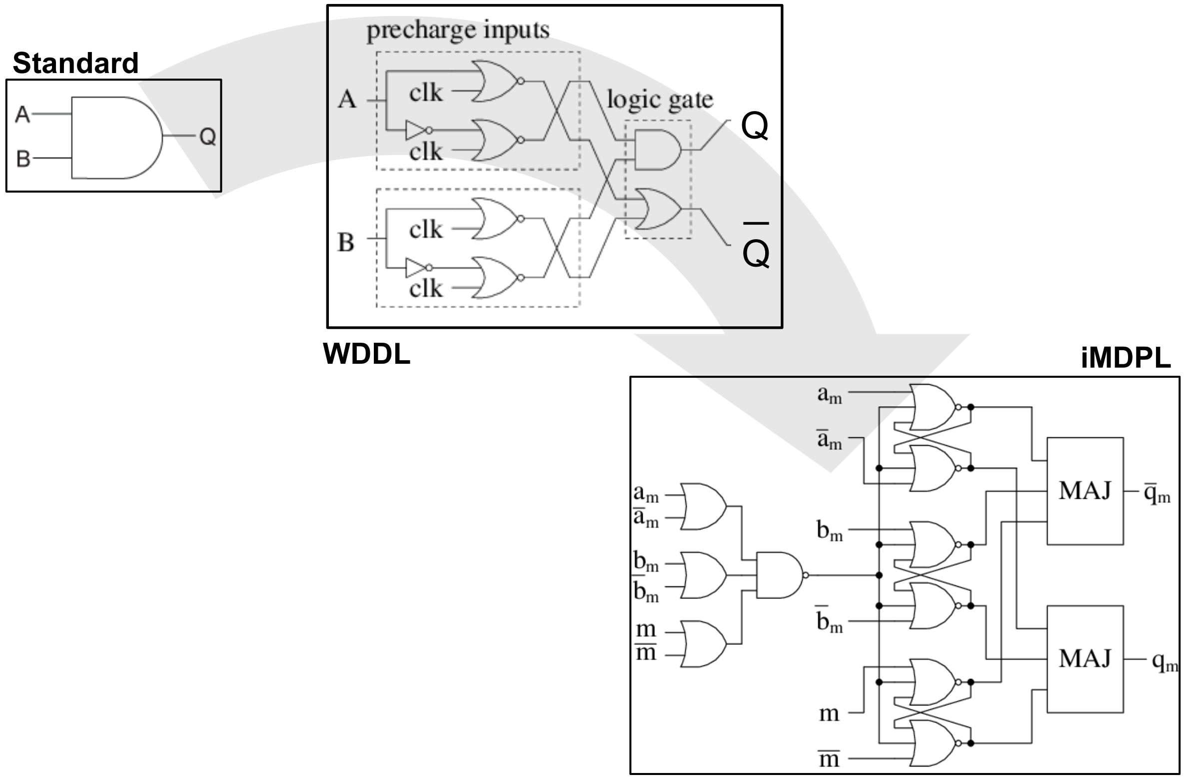


Muhammad Yasin and Ozgur Sinanoglu, "Evolution of Logic Locking," CHES, 2016



Example: automated synthesis / mapping tradeoffs between size + power vs. side channel leakage

Scaled overhead of side channel reduction cell size



1: Design Integrity

2: Design Confidentiality

3: Data Confidentiality: Labeled storage areas of crypto keys identify likely targets of an AT threat

***Enables evaluation** of AISS technique's ability to protect registers/wires with sensitive data from attacker, i.e. "Side Channel"*

4: Device Integrity

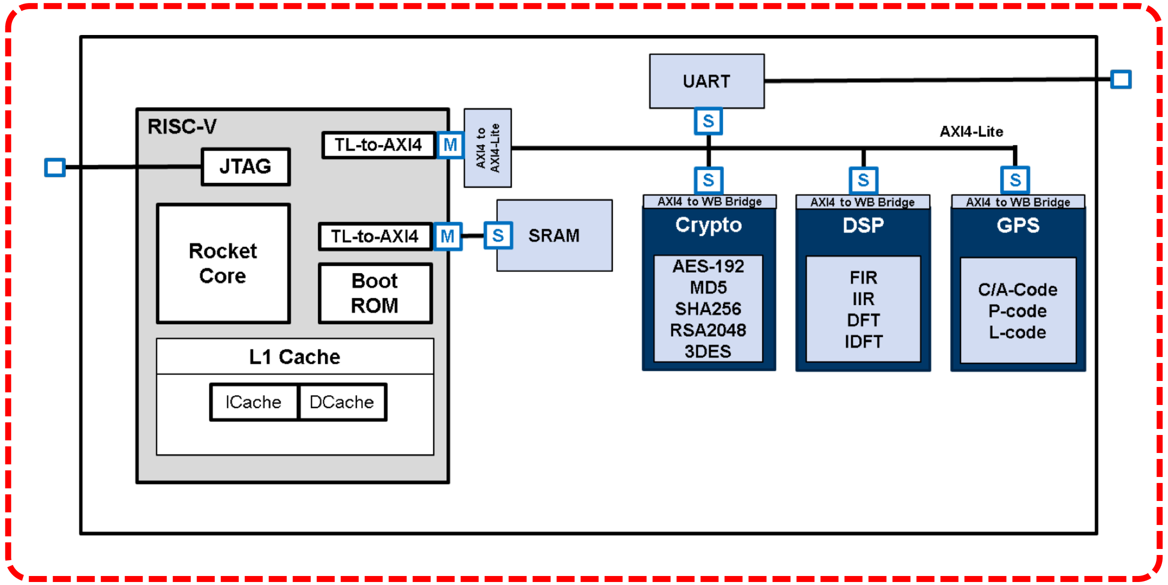
AT – Anti-Tamper, WDDL – Wave Dynamic Differential Logic, iMDPL – Improved Masked Dual-Rail Precharge Logic

Popp, Thomas, et al. "Evaluation of the masked logic style MDPL on a prototype chip." *CHES*, 2007
Batina, Lejla, Nele Mentens, and Ingrid Verbauwhede. "Side-channel issues for designing secure hardware implementations." *11th IEEE International On-Line Testing Symposium*. IEEE, 2005

AISS Application:

Benchmarking Security Techniques w/ Evaluation Targets

COMMON EVALUATION PLATFORM



1: Design Integrity

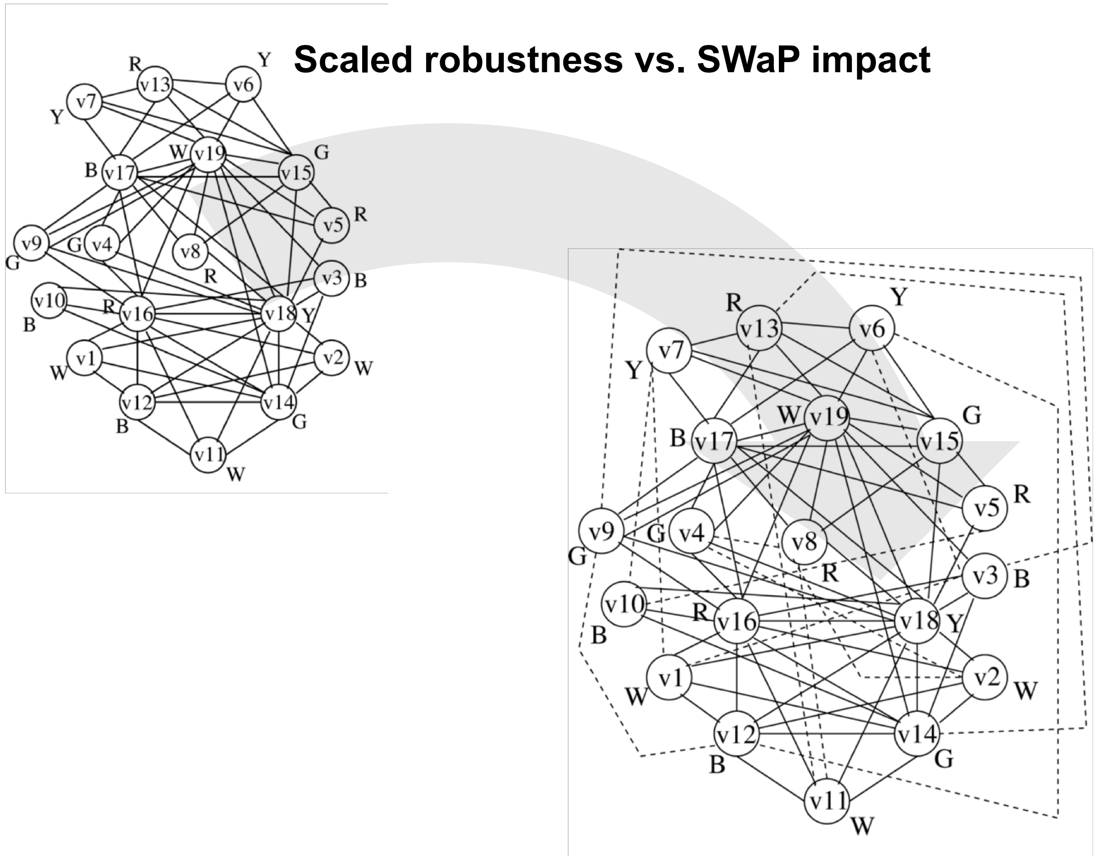
2: Design Confidentiality

3: Data Confidentiality

4: Device Integrity: Labeled device versions and pedigree

***Enables evaluation** of AISS techniques to protect device integrity, i.e. "Supply Chain"*

Example: automated design watermarking techniques during synthesis



SWaP – Size, Weight, and Power

Koushanfar, Farinaz, Inki Hong, and Miodrag Potkonjak. "Behavioral synthesis techniques for intellectual property protection." *ACM Transactions on Design Automation of Electronic Systems (TODAES)* 10.3 (2005): 523-545.

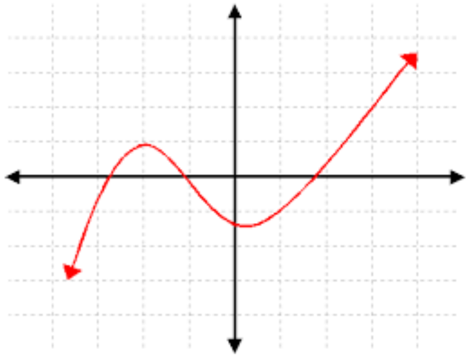
Outline

- CEP Background
- AISS Role
- Next Steps
- Summary

Generator-based CEP

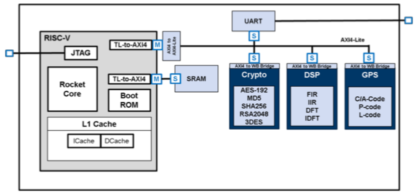
COMMON EVALUATION PLATFORM

f(Performance, Size, Power, Security)



Goal: Parameterized tool flow allowing optimization tradeoff between: Performance, Size, Power, and *Security*

Generator-based CEP enables parametric SoC configuration



+ Scala & Chisel

- **Better supports security-centric design optimization through parametric inclusion and enabling of security features**

Representative AISS and generator-based CEP enabled tool-flow

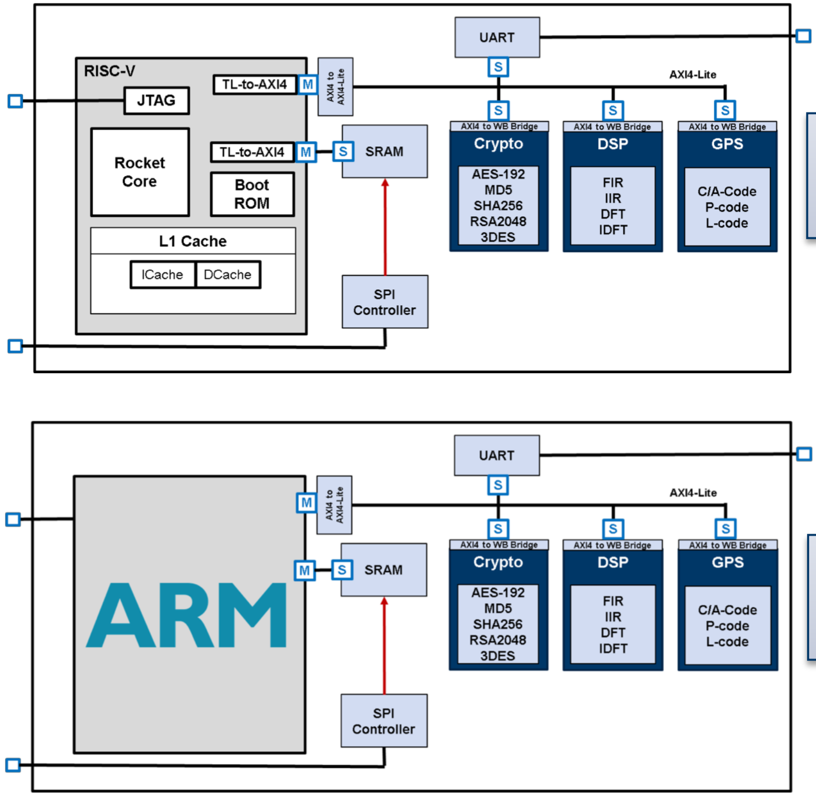
Specify Architecture → **Develop Behavioral Code** → **Synthesize Design** → **Place and Route Design**

Specify Architecture	Develop Behavioral Code	Synthesize Design	Place and Route Design
e.g., Provenance features	e.g., Side-channel resistance	e.g., Circuit obfuscation	e.g., Guard wires

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

CEP – Dual Baseline

COMMON EVALUATION PLATFORM



DoD Transition

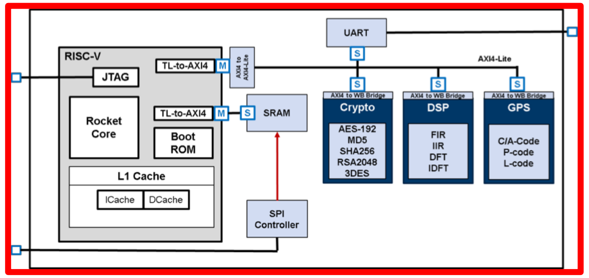
Common core base and verification suite

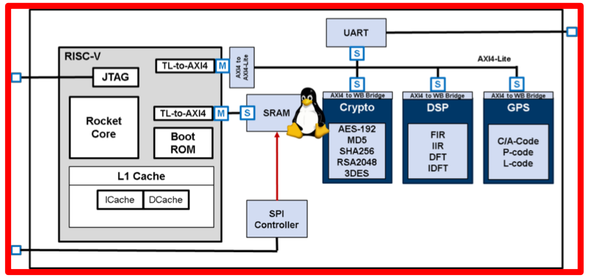
Commercial Transition

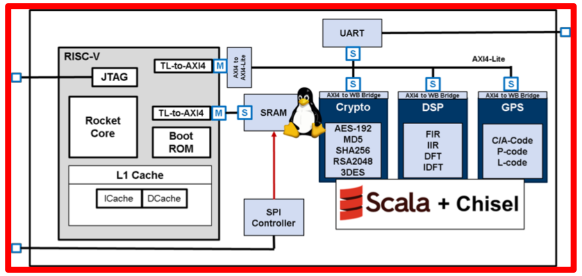
Provides dual platform independent validation paths

CEP Roadmap – Next Steps

COMMON EVALUATION PLATFORM







CEP Version	**v2.1**	**v2.2**	**v2.3**
Processor	RISC-V*	RISC-V*	RISC-V*
Bus	AXI4-Lite	AXI4-Lite	AXI4-Lite
OS Support	Transitional (See notes)	Linux	Linux
ASIC Optimized	• Optimized AES Core • Boot via SPI-based Flash • Design for Test	• Optimized AES Core • Boot via SPI-based Flash • Design for Test	• Optimized AES Core • Boot via SPI-based Flash • Design for Test
Test Suite / Documentation / Other	• Unit C code (sim + HW) • Waveforms (sim) • Regression (sim + HW)	• Unit C code (sim + HW) • Waveforms (sim) • Regression (sim + HW)	• Unit C code (sim + HW) • Waveforms (sim) • Regression (sim + HW)
Languages	Mixed + Chisel	Mixed + Chisel	Chisel + Verilog
Release Date	Aug ’19	TBD	TBD
Notes	• Additional hooks to enable future Linux support		• Accelerator cores ported to Chisel

**Air Force Research Lab RISC-V / University of California Berkley Rocket Chip*

AES – Advanced Encryption Standard, SPI – Serial Peripheral Interface, TBD – To be determined

Outline

- CEP Background
- AISS Role
- Next Steps
- Summary

Summary

COMMON EVALUATION PLATFORM

- CEP is a surrogate SoC that enables:
  - AISS IV&V activities
  - Development and test of AISS toolflows and techniques

- RISC-V based CEP release pending:
  - Leverages modified version of UCB Rocket Chip
  - Supports broad range of verification options
  - Contains labeled security targets

- Incremental CEP release schedule to deliver features to AISS performers

Contact Information

COMMON EVALUATION PLATFORM

CEP Repository: www.github.com/mit-ll/CEP.git

MIT LL Contact Information:

Brendon Chetwynd (781) 981-8212, brendon.chetwynd@ll.mit.edu

Kevin Bush (781) 981-7512, kevin.bush@ll.mit.edu