

## **CROSSCON** Novel TEE for Next Generation RISC-V MCUs

Matjaž Breskvar, Beyond Semiconductor Sandro Pinto, University of Minho







CROSSCON & (secure) Friends RSC-V Summit EU 2024 - Side Event 1

#### RISC-V Summit EU 2024 24-28, June 2024, Munich, Germany

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537



# Agenda

Introduction Security, TEEs, and RISC-V MCU Gap

Use Cases Motivation

Secure AI at the Edge and Domain/Zonal Controllers

03

05

01

02

04 Vali

#### Validation and Evaluation

**Design & Implementation** 

Hardware Resources and TCB Size

Background, Spike, BA51-H, and Bao

Conclusion Roadmap and Next steps

## Introduction

Security, TEEs, and RISC-V MCU Gap





MIRA

#### Security is paramount for the Internet of Things (IoT)



amazon webservices

......

FreeRTOS

......



"We are witnessing cyberattacks on critical infrastructure, health services systems captured and held to ransom and home electronics devices used as internet gateways by hackers."

FORESHADOW

arm, in Security Manifesto, 2017.





CART TECHNOLOGIES

At a me

where man

## CART TECHNOLOGIES TRUSTZONE FOR CORTEX-M

A

9

 $\bigcirc$ 

-0/

-0



## **RISC-V MCU TEE**

#### **IoT-based devices requirements**

- Connectivity (e.g WiFi, Bluetooh, ZigBee)
- Upgradability (e.g. firmware, features, security)
  - Sensitive information (e.g. keys, certificates)





#### **RISC-V TEE for MCU**

- No RISC-V TEE MCU related spec
- Existing solutions have limitations (performance & power)
- Evolving ecosystem

#### Isolate! TEE to the rescue

- Hardware-enforced Isolation
- Separate execution environment
  - Multiple protection models



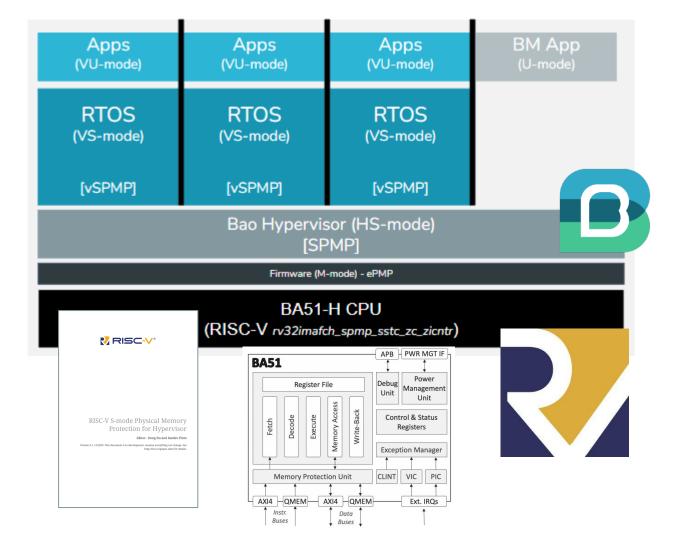


#### Can devs do something?

## Contribution: Novel TEE for RISC-V MCU

#### Central Novelty

- Virtualization-based TEE
- SPMP with Hypervisor support
- Implementation and Artifacts
  - SPMP for Hypervisor Spec
  - Spike (SPMP for Hypervisor) Model
  - BA51-H MCU
  - Bao SPMP-H port



## **Use Cases Motivation**

Secure AI at the Edge and Domain/Zonal Controllers

#### Best Practices for Armv8-R Cortex-R52+ Software Consolidation

Dr Paul Austin, Principal Software Engineer, ETAS Dr Andrew Coombes, Senior Product Manager, ETAS Paul Hughes, Lead System Architect and Distinguished Engineer ATG, Arm James Scobie, Director Automotive Product Management, Arm Bernhard Rill, Director Automotive Partnerships EMEA, Arm arm ET/\S Renesas 28nm Cross-Domain Flash MCU, RH850/U2A, Featuring Virtualization

AURIAMINEO

RHB50/UZA

## **Use Cases: Automotive Domain/Zonal Controllers**

#### ECU consolidation:

- Reduce complexity and cost
- Safety ISO26262 (FFI)
- High-performance
- Real-time (Predictability)

#### EV/HEV PowerTrain\*:

- Battery Management System (BMS)
- Chassis Control
- Power Management (DC/DC Inverter)
- Steering Control
- Model Predictive Control (MPC)
- Thermal Monitoring

...

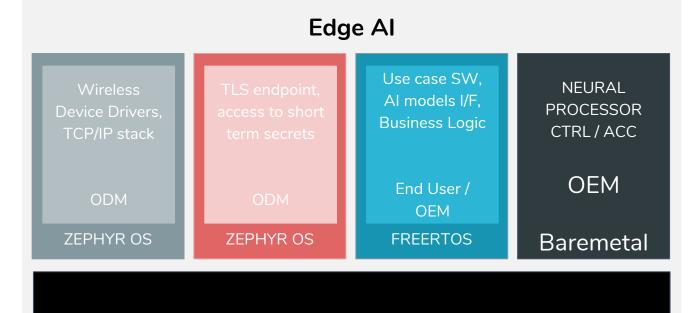
 BMS
 CHASSIS

 AUTOSAR OS
 AUTOSAR OS

#### Use Cases: Secure AI at the edge

#### Separation for Security/Resilience:

- Reduce complexity and cost
- Consolidation while avoiding Security issues
- End-User SW support
- Real-time Operation
- End User / OEM:
  - Simple use of ODM maintained on-chip services (e.g. Secure Channel to cloud)
  - Transparent software sandbox with software adjustable/assignable resources
  - Control / acceleration of on-chip Al (pre)processing, offload to cloud



# **Design & Implementation**

Background, Spike, BA51-H, and Bao

## MMU

#### Memory Management Unit

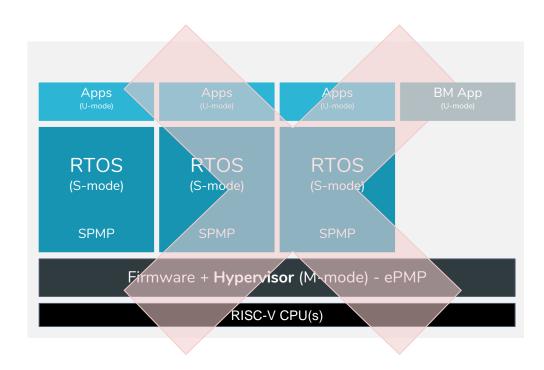
- Translation
- Protection
- Flexibility

#### **PMP** Physical Memory Protection

- Protection
- Predictability
- Simplicity

## **RISC-V TEE MCU-H Architecture**

Apps (VU-mode)	Apps (VU-mode)	Apps (VU-mode)	BM App (U-mode)				
RTOS (VS-mode)	RTOS (VS-mode)	RTOS (VS-mode)					
vSPMP	vSPMP	vSPMP					
ŀ	Hypervisor (HS-mode) - hgPMP						
Firmware (M-mode) - ePMP							
RISC-V CPU(s)							



Disadvantages:

- Hypervisor portability
- Firmware Reuse
- No platform-level domains

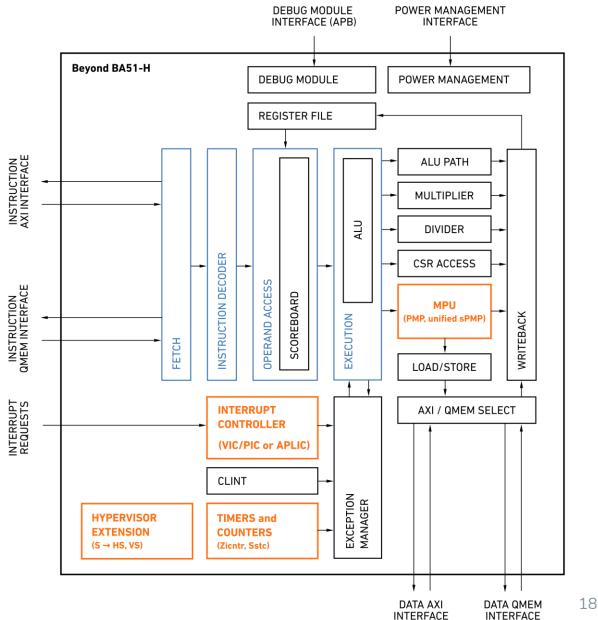
## **RISC-V SPMP (for Hypervisor)**



## **RISC-V Spike SPMP for Hypervisor**

← → C 😁 https://github.com/crosscon/	/riscv-isa-sim					\$
Product ~ Solutions ~ Open Sour	rce ~ Pricing				Q Search or jump to	
Grosscon / riscv-isa-sim					🗘 Notificati	ions & Fork 0
<> Code 🕢 Issues 👬 Pull requests	🕞 Actions 🖽 Projects 🕕 Security 🗠 Insights					
	💡 main 👻 🖓 1 Branch 🟷 0 Tags	Q Go to file	<> Code -	About		
	Zputrle SPMP: Use guest access fault causes.	b49e3a5 - last month	$\sim$	A modified riscv-is SPMP extension.	a-sim with unified	
	github/workflows	Attempt to fix Mac OS CI	7 months ago	🛱 Readme		
	arch_test_target/spike	update set_msw/clear_msw/set_mtimer/clear_mtimer	8 months ago	▲ View license ▲ Activity		
	Ci-tests	vSPMP: Apply several fixes.		<ul> <li>Custom propertie</li> </ul>	25	
	Customext	Remove decode_macros.h from disasm.h	last year	<ul> <li>☆ 0 stars</li> <li>⊙ 1 watching</li> </ul>		
	bug_rom	DSCRATCH is now called DSCRATCH0		%   0 forks		
	📄 disasm	Change disasm for $vset\{i\}vli$ with reserved vtypes to display t	6 months ago	Report repository		
	🗖 fdt	Install header files fdt.h and libfdt_env.h as needed by libfdt.h	7 months ago	Releases		
	esvr	Include cerrno in fesvr/elfloader.cc	7 months ago	No releases published		
	Tiscv	SPMP: Use guest access fault causes.	last month	Packages		
	scripts	Update config file to support aarch64	4 years ago	No packages published		
	softfloat	Add convertion function between binary float16 and float32 $\ldots$	10 months ago			
	<b>s</b> pike_dasm	Add config.h includes directly to source files instead of relyi	2 years ago	Contributors 142		
	<b>s</b> pike_main	vSPMP: Apply several fixes.	2 months ago			
	🗋 .gitignore	gitignore: ignore emacs backup files	last year	() 🙂 💮 (	S 🚱 🌑 🔀	
	ChangeLog.md	1.1.0 release	3 years ago	+ 128 contributors		
		Update LICENSE copyright date	7 years ago	Languages		

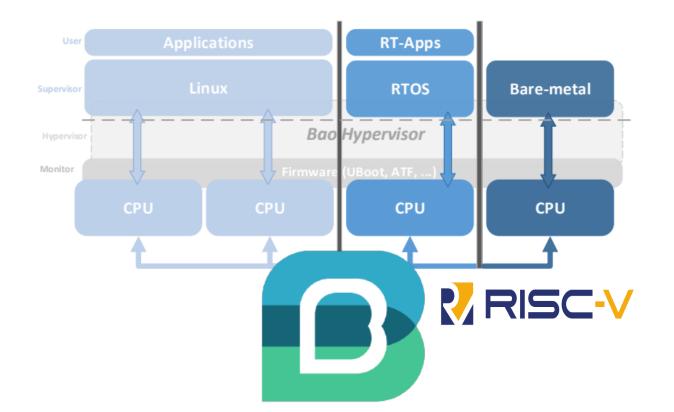
## Beyond BA51-H



- RISC-V RV32IMAFC
- Hypervisor Extension
- Unified SPMP extension:
  - Adds support for the supervisor mode physical memory protection;
- Zc Extension:
  - Reduces the code size by adding to the 16bit instruction set;
- Sstc Extension:
  - Timer services in supervisor mode;
- Advanced Platform-Level Interrupt Controller (APLIC):
  - Interrupt delegation;

## Bao Hypevisor

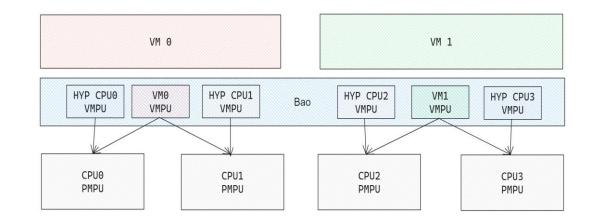
- Type-1 / Bare-metal
- Static Partitioning Architecture:
  - 1:1 vCPU-to-pCPU mapping
  - Static memory assignment
- Hardware-assisted
- Inter-VM communication
- Real-Time & Predictability
- No Dependencies (libraries / OS)
- RISC-V and Armv8-A ISA



## Bao RISC-V: SPMP Hypervisor

#### Two-layer MPU/PMP Design

- Top Layer Architecture-independent (VMPU)
- Bottom Layer Architecture-dependent (PMPU)
- Advantages of such Design
  - Agnostic memory management
  - Agnostic policy-checks
  - Optimized PMP entry management
- RISC-V SPMP Limitation
  - No shared regions between hypervisor and guest
  - Bao does not use shared permissions -> duplicated regions (flipped mode bit)



# Validation and Evaluation

Hardware Resources and TCB Size

OpenSBI v1.4-31-g322b598	
11_11_57_2_5	
``' ;' `' !_' !_	I/I/
i_i	
Platform Name	: ucbbar,spike-bare
Platform Features	: medeleg
Platform HART Count Platform IPI Device	: 1 : aclint-mswi
Platform IPI Device Platform Timer Device Platform Console Device	: aclint-mtimer @ 10000000Hz
Platform Console Device Platform HSM Device Platform PMU Device	: uart8250 :
Platform PMU Device Platform Reboot Device	: : htif
Platform Shutdown Device	: htif
Platform Suspend Device Platform CPPC Device	:
Firmware Base	: 0x80000000
Firmware Size Firmware RW Offset	: 315 KB : 0x40000
Firmware BW Size	: 59 KB
Firmware Heap Offset Firmware Heap Size	: 0x46000 : 35 KB (total), 2 KB (reserved), 9 KB (used), 23
free)	
Firmware Scratch Size Runtime SBI Version	: 4096 B (total), 188 B (used), 3908 B (free) : 2.0
Deve in O. News	
Domain0 Name Domain0 Boot HART	: 0
Domain0 HARTs Domain0 Region00	: 0× : 0×10000000-0×10000fff M: (I,R,W) S∕U: (R,W)
Domain0 Region01	() -1152 (11 C) -1M 333356602-6 60665609-6
Domain0 Region02 Domain0 Region03	: 0x02080000-0x020bffff M: (1,R,W) S/U: () : 0x800000000-0x020bffff M: (1,R,W) S/U: ()
Domain0 Region04	: 0x02000000-0x0207ffff M: (I.R.W) S/U: ()
Domain0 Region05 Domain0 Region06	: 0x0c000000-0x0cffffff M: (1,R,W) S/U: (R,W) : 0x0000000-0xffffffff M: () S/U: (R,W,X)
DomainO Next Address	: 0x80400000
Domain0 Next Arg1 Domain0 Next Mode	: 0x82200000 : S-mode
Domain0 SysReset	: yes
Boot HART ID Boot HART Domain	: 0 : root
Boot HART Priv Version Boot HART Base ISA	: v1.12
Boot HART Base ISA Boot HART ISA Extensions	: ru32imafdch : sstc,zicntr,zihpm,sdtrig
Boot HART PMP Count	: 16
Boot HART ISA Extensions Boot HART PMP Count Boot HART PMP Granularity Boot HART PMP Address Bits	: 2 bits s: 32
Boot HART MHPM Info	: 0 (0x00000000) : 4 triggers
Boot HART Debug Triggers Boot HART MIDELEG	: 0x00001666
Boot HART MEDELEG Bao Hypervisor	: 0x0010b509
DHU WHENING: Trying to III	ish caches but the operation is not defined for th
atform BAO WARNING: trying to flu	ush caches but the operation is not defined for th
atform	
[guest 0] Bao bare-metal † [guest 0] cpu 0 up	test guest
fauget 11 Rao have-metal t	teet mueet
Iguest 11 cpu 0 up Iguest 01 cpu0: timer_hand	ller
Iguest 11 cpu0: timer_ham Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham	ller
lguest 0] cpu0: timer_hand [guest 1] cpu0: timer_hand [guest 0] cpu0: timer_hand	ller ller
[guest 0] cpu0: timer_hand	ller
[guest 0] cpu0: timer_hand [guest 0] cpu0: timer_hand	ller
fouget 11 could: times have	ller
[guest 0] onu0: times have	
[guest 0] cpu0: timer_hand [guest 1] cpu0: tim <u>er_hand</u>	ller
Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham	ller ller
[guest 1] cpu0: timer_hand	ller
Iguest 01 cpu0: timer_ham Iguest 11 cpu0: timer_ham Iguest 01 cpu0: timer_ham Iguest 11 cpu0: timer_ham	ller Ller Ller
Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham	ller Iler Iler Iler Iler
Iguest 01 cpu0: timer_ham Iguest 01 cpu0: timer_ham	ller ller ller ller ller ller
[guest 1] cpu0: timer_ham [guest 0] cpu0: timer_ham [guest 0] cpu0: timer_ham [guest 1] cpu0: timer_ham [guest 1] cpu0: timer_ham [guest 1] cpu0: timer_ham [guest 1] cpu0: timer_ham	Uer Uer Uer Uer Der Der Der
rguest 1) cpu0 timer_man (guest 1) cpu0 timer_han (guest 10 cpu0 timer_han (guest 10 cpu0 timer_han (guest 01 cpu0 timer_han (guest 11 cpu0 timer_han	ler ler ler ler ler ler ler ler ler
[guest 1] cpu0: timer_ham [guest 0] cpu0: timer_ham [guest 0] cpu0: timer_ham [guest 1] cpu0: timer_ham [guest 1] cpu0: timer_ham [guest 1] cpu0: timer_ham [guest 1] cpu0: timer_ham	lee Lee Lee Lee Lee Lee Lee Lee Lee Lee

## Bao @ Spike Validation

: 0 Boot HART ID Boot HART Domain : root : v1.12 Boot HART Priv Version Boot HART Base ISA : ru32imafdch Boot HART ISA Extensions : sstc,zicntr,zihpm,sdtrig Boot HART PMP Count : 16 Boot HART PMP Granularity : 2 bits Boot HART PMP Address Bits: 32 Boot HART MHPM Info  $: 0 (0 \times 0 0 0 0 0 0 0 0)$ Boot HART Debug Triggers : 4 triggers Boot HART MIDELEG : 0x00001666 Boot HART MEDELEG : 0x00f0b509 Bao Hypervisor BAO WARNING: trying to flush caches but the operation is not defined for this pl atform BAO WARNING: trying to flush caches but the operation is not defined for this pl atform [guest 0] Bao bare-metal test guest [guest 0] cpu 0 up [guest 1] Bao bare-metal test guest [guest 1] cpu 0 up [quest 0] cpu0: timer handler

Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1) BA51 CC	25,239	100%	5%	12%	3%
(#2) BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3) BA51 FRC	206,430	818%	38%	100%	28%
(#4) BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
APLIC	1,403	5.6%	0.3%	0.7%	0.2%
Sstc	904	3.6%	0.2%	0.4%	0.1%
Zc	1,287	5.1%	0.2%	0.6%	0.2%

8x Area difference between **compact** and **feature rich configuration** of the processor

Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1) BA51 CC	25,239	100%	5%	12%	3%
(#2) BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3) BA51 FRC	206,430	818%	38%	100%	28%
(#4) BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
					•
Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
APLIC	1,403	5.6%	0.3%	0.7%	0.2%
Sstc	904	3.6%	0.2%	0.4%	0.1%
Zc	1,287	5.1%	0.2%	0.6%	0.2%

#### SRAM Area dominates

Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1) BA51 CC	25,239	100%	5%	12%	3%
(#2) BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3) BA51 FRC	206,430	818%	38%	100%	28%
(#4) BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
APLIC	1,403	5.6%	0.3%	0.7%	0.2%
Sstc	904	3.6%	0.2%	0.4%	0.1%
Zc	1,287	5.1%	0.2%	0.6%	0.2%

PMP is the main area contributor

• 1600 gates per entry for (S)PMP

Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1) BA51 CC	25,239	100%	5%	12%	3%
(#2) BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3) BA51 FRC	206,430	818%	38%	100%	28%
(#4) BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%

Hypervisor extension
PMP (16e) + unified SPMP (16e)
PMP (32e)
APLIC
Sstc
7c

7,685	30.4%	1.4%	3.7%	1.1%
51,223	203.0%	9.3%	24.8%	7.0%
50,733	201.0%	9.2%	24.6%	6.9%
1,403	5.6%	0.3%	0.7%	0.2%
904	3.6%	0.2%	0.4%	0.1%
1,287	5.1%	0.2%	0.6%	0.2%

#### S $\rightarrow$ HS + VS is important area contributor

Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1) BA51 CC	25,239	100%	5%	12%	3%
(#2) BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3) BA51 FRC	206,430	818%	38%	100%	28%
(#4) BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
APLIC	1,403	5.6%	0.3%	0.7%	0.2%
Sstc	904	3.6%	0.2%	0.4%	0.1%
Zc	1,287	5.1%	0.2%	0.6%	0.2%

Delegation & Zc instructions are **net area gain** due to code size savings

Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1) BA51 CC	25,239	100%	5%	12%	3%
(#2) BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3) BA51 FRC	206,430	818%	38%	100%	28%
(#4) BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
APLIC	1,403	5.6%	0.3%	0.7%	0.2%
Sstc	904	3.6%	0.2%	0.4%	0.1%
Zc	1,287	5.1%	0.2%	0.6%	0.2%

Virtualization and Physical Memory Protection hardware (area) cost is easily offset by reduced SRAM overprovisioning and flexibility improvements

# Bao RV64 (Application) G.9 K SLoC Trusted Computing Base 31 KiB (.text)

#### Bao SPMP Hypervisor Trusted Computing Base

- 6.4 K SLoC
- 29.5 KiB (.text)
- WiP Optimizations



Roadmap and Next steps

## Status, Road Ahead

#### Spike reference implementation

- unified SPMP and hypervisor extensions
- available from CROSSCON github
- Bao initial version
  - validated in Spike

#### BA51-H implementation

- includes all virtualization relevant extensions (for MMU-less processor)
- unified SPMP and hypervisor extensions

- RISC-V standardization activities
  - finalize ongoing standardization efforts
  - memory address translation
- Bao memory footprint reduction
  - free unused memory after init,...

#### BA51-H optimizations

- hardware support for inter VM communication
- optimized PMP implementation

# THANK YOU!

<matjaz.breskvar@beyondsemi.com>

<sandro.pinto@dei.uminho.pt>

