北京开源芯片研究院
BEIJING INSTITUTE OF OPEN SOURCE CHIP

# Enabling Confidential Computing on RISC-V

## An Open-Source MPT Implementation

**Haoyuan Liu**
Beijing Institute of Open Source Chip (BOSC)
RISC-V Summit Europe, June 2026

# SMMPT Motivation: The Memory Isolation Problem

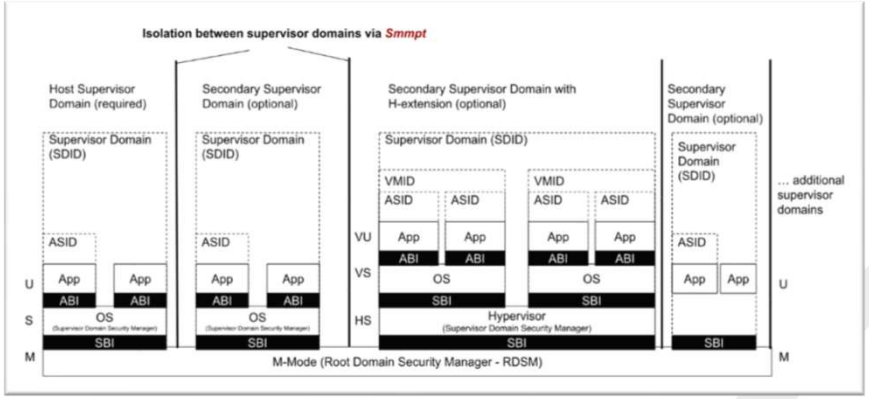
**Problem: Traditional solution fails for Confidential computing and multi-tenant cloud environments**

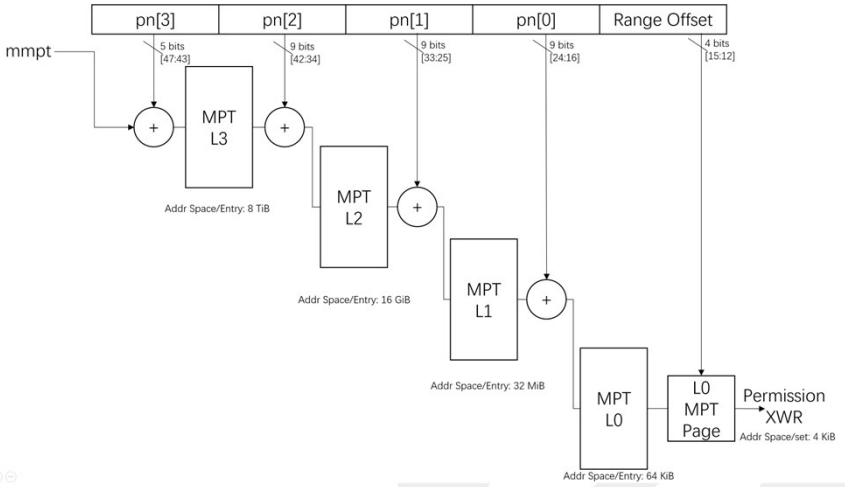
- No per-domain fine-grained runtime isolation

**Solution: SMMPT (Supervisor Domain Memory Protection Tables)**

- Hardware-enforced Hierarchical page-based physical memory isolation between supervisor domains

**Our Job:**
**First open-source hardware implementation of SMMPT v0.4**



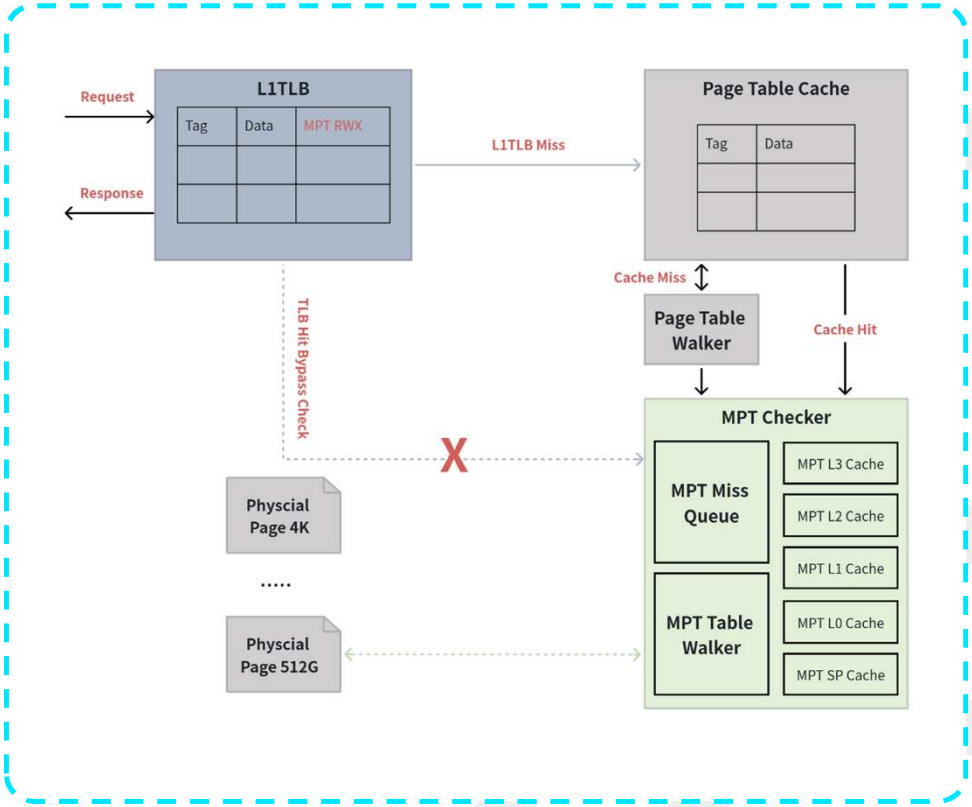
# Design Philosophy: Decoupled Architecture

## Core Decision

Implementing the **MPT Checker** as a fully independent hardware module, rather than tightly integrating it with the existing MMU.

## Key Advantages

- **High Portability:** Easy integration and porting to any RISC-V core.
- **Minimal Impact:** Requires very few changes to the existing MMU/TLB subsystem.
- **Flexibility:** Enables independent performance optimization of the checker.



# Optimization 1: Multi-level Non-Blocking Cache

**OBSERVATION:** MPT table walks are extremely expensive, becoming a critical bottleneck for SMMPT performance.

## Solution 1: 5-level dedicated MPT Cache

- Aligns perfectly with SMMPT hierarchical table structure
- Caches both leaf and intermediate nodes for faster lookups

## Solution 2: Non-blocking MSHR

- Buffers 4 outstanding miss requests
- Eliminates pipeline stalls on misses & merges duplicates

**PERFORMANCE IMPACT:** Reduced baseline overhead from >100% to ~5%

# Optimization 2: L1TLB Permission Caching

**OBSERVATION:** MPT performance loss is proportional to L1TLB miss rate.

**Solution :**

We extended the L1TLB structure to store MPT R/W/X permission bits together with the virtual-to-physical translation entries, eliminating MPT cache query cost when L1TLB hit.

**PERFORMANCE IMPACT:** Zero MPT queries on L1TLB hits

Complete elimination of permission lookup overhead for the most frequent case.

# Optimization 3: Security-Performance Trade-off

## OBSERVATION

The attack surface for PTW intermediate nodes is extremely narrow, and no practical attack exploiting these nodes have been demonstrated or documented to date.

## OPTIMIZATION

Skip Memory Protection Table (MPT) permission checks for PTW intermediate nodes to eliminate redundant computation.

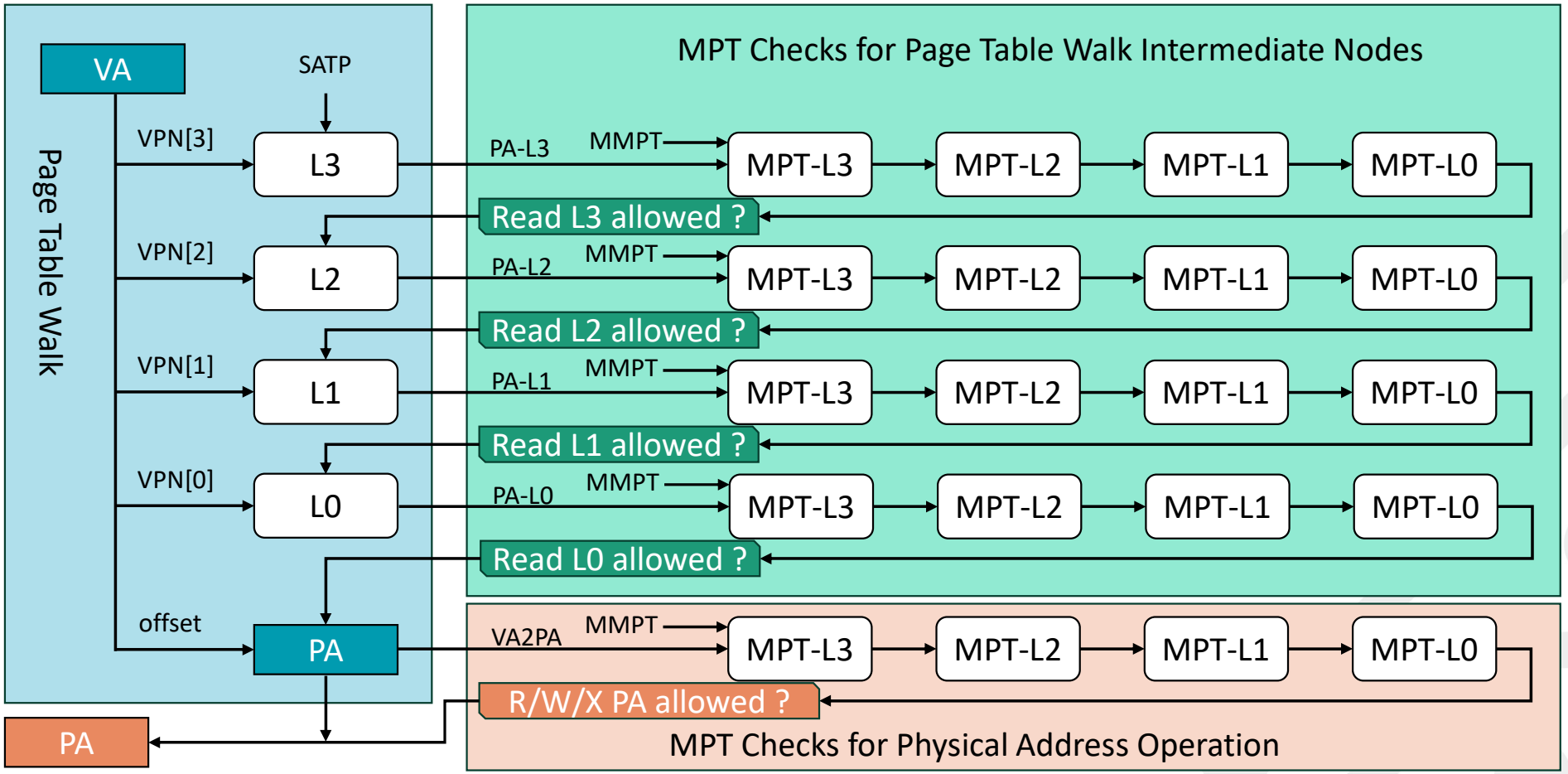
## CONTROL MECHANISM

Configurable via a 1-bit custom Control and Status Register (CSR). Allows the OS to enable or disable the optimization at runtime.

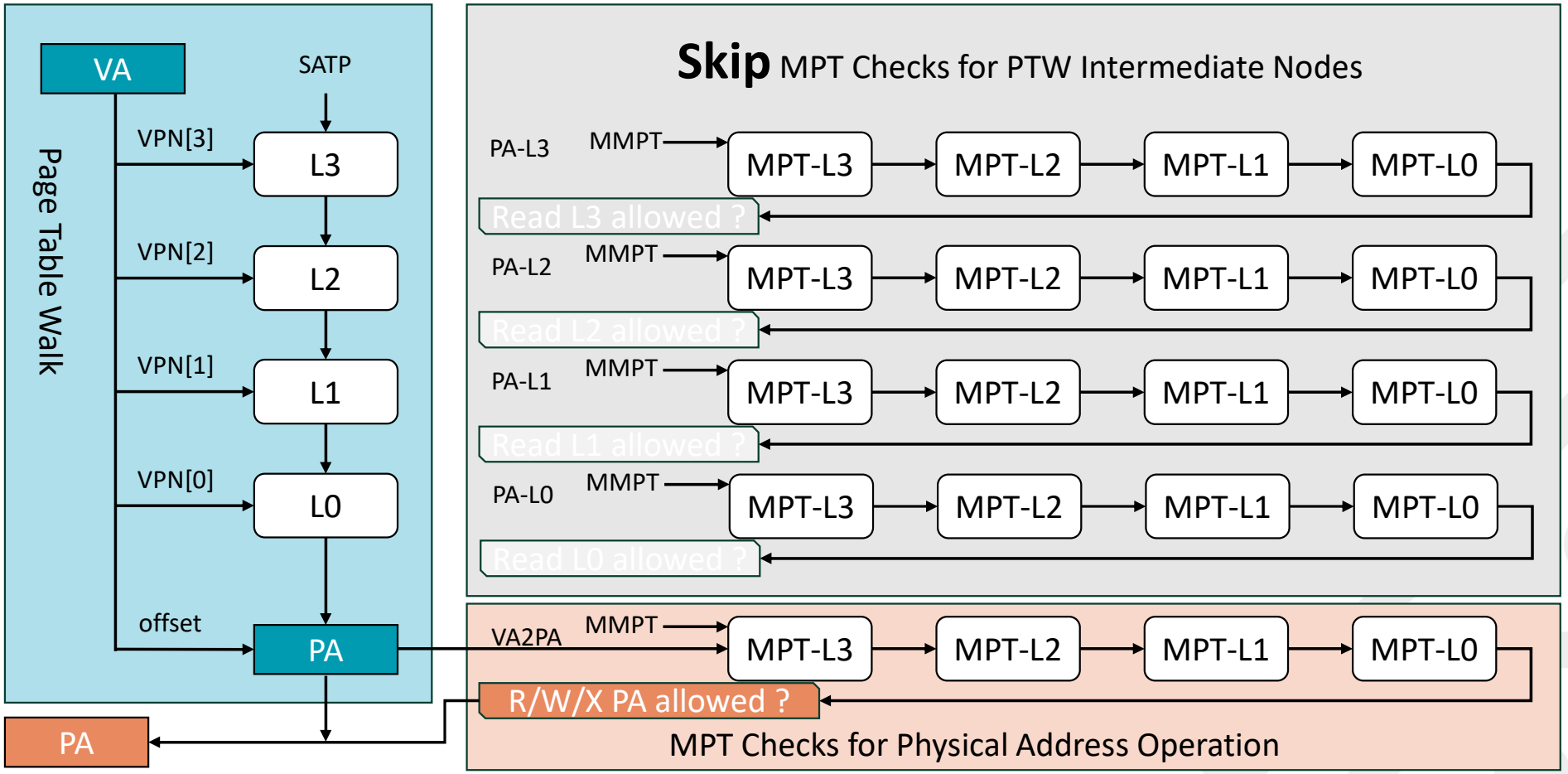
## THE FINAL TRADE-OFF

**Negligible Security Loss→Significant Performance Gain**

# Optimization 3: Security-Performance Trade-off



# Optimization 3: Security-Performance Trade-off



# Optimization 3: Security-Performance Trade-off

## OBSERVATION

The attack surface for PTW intermediate nodes is extremely narrow, and no practical attack exploiting these nodes have been demonstrated or documented to date.

## OPTIMIZATION

Skip Memory Protection Table (MPT) permission checks for PTW intermediate nodes to eliminate redundant computation.

## CONTROL MECHANISM

Configurable via a 1-bit custom Control and Status Register (CSR). Allows the OS to enable or disable the optimization at runtime.

## THE FINAL TRADE-OFF

**Negligible Security Loss→Significant Performance Gain**

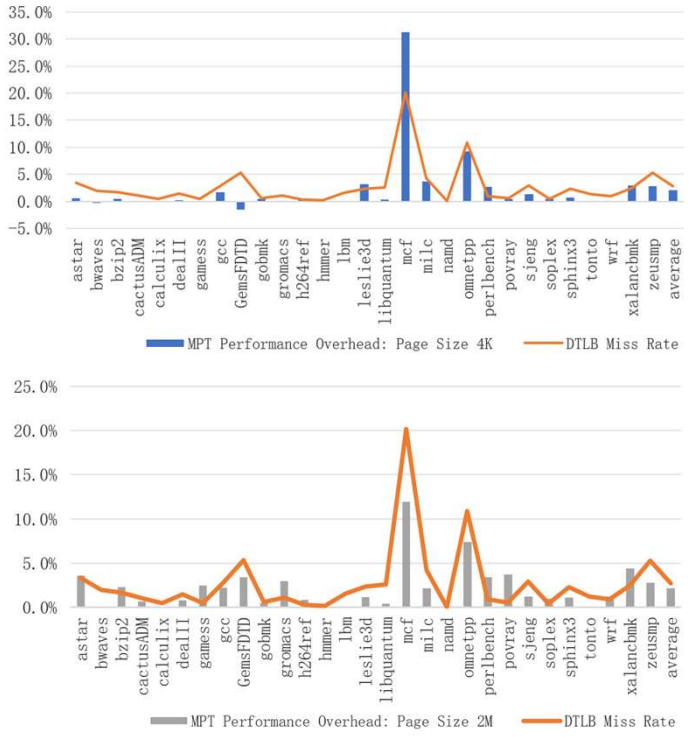
# Evaluation Results

Platform: **OpenXiangshan KMH core**
Benchmark: **SPEC CPU2006**

## KEY PERFORMANCE METRICS

**2.32%**
Avg. Overhead (4KB Pages)

**2.16%**
Avg. Overhead (2MB Large Pages)



# Evaluation Results

### Total MPT Area

**4880 µm²**

Total silicon cell area of the entire MPT Checker module

### Core Area Ratio

**0.244%**

Proportion of the total processor core area occupied

# Thank You