Jintide® : A Hardware Security Enhanced Server CPU

with Xeon® Cores under Runtime Surveillance by an In-Package Dynamically Reconfigurable Processor

Ao Luo

Research Scientist of the Institute of Microelectronics, Tsinghua University, China

CEO of Cataphract Microelectronics - a Startup from Tsinghua University, China

Authors: Leibo Liu[1], **Ao Luo[1]**, Guanhua Li[1], Jianfeng Zhu[1]*, Yong Wang[2], Gang Shan[2], Jianfeng Pan[3], Shouyi Yin[1], Shaojun Wei[1]

1 Institute of Microelectronics, Tsinghua University, China;

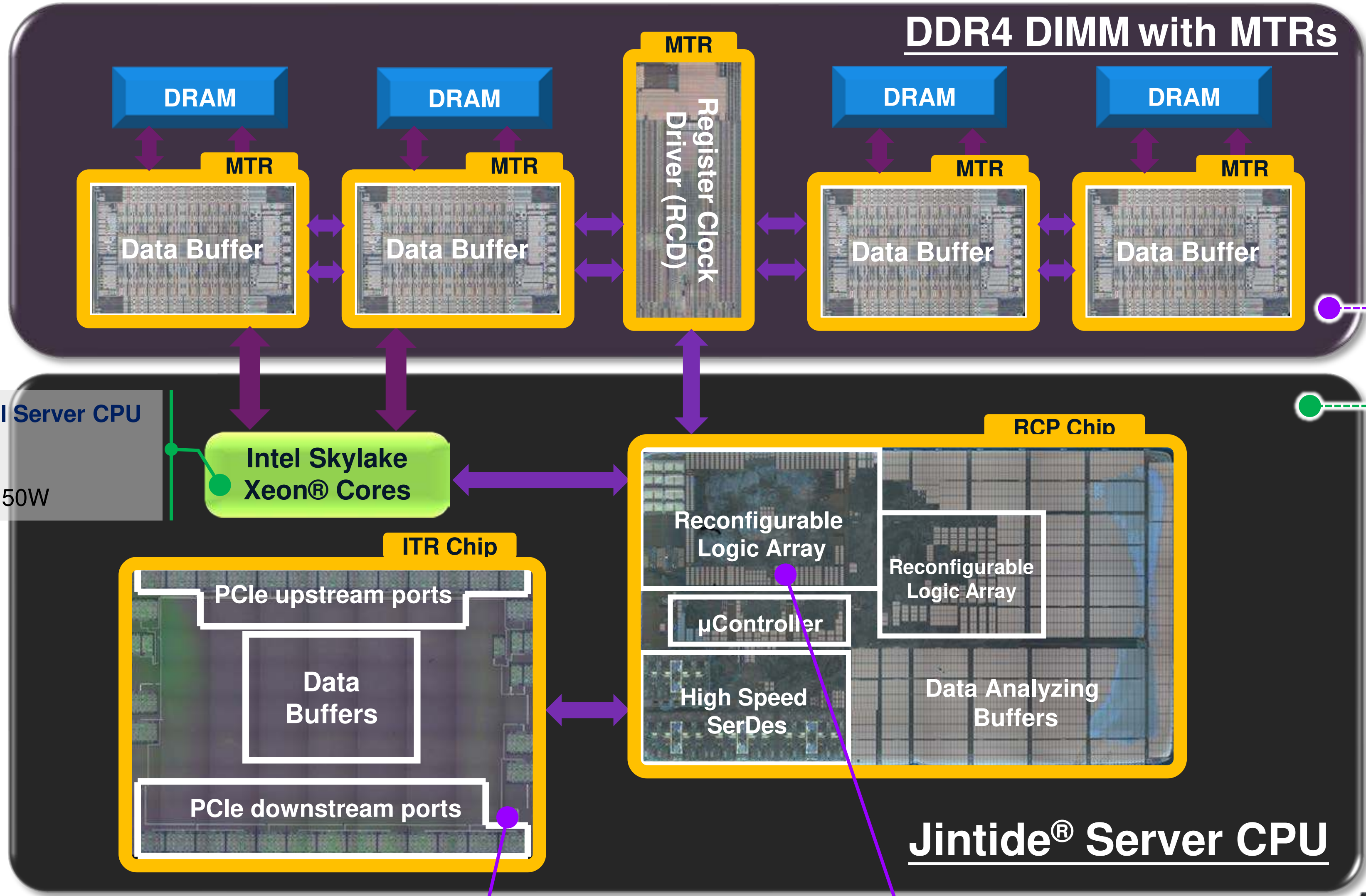
2 Montage Technology Co., Ltd.;

3 Qihoo 360 Technology Co., Ltd.;

** Corresponding Author: zhujianfeng@tsinghua.edu.cn*

HOTCHIPS 31, Aug 20, 2019

Jintide®



Industrial Server CPU
2.0 GHz
24 Cores
TDP 95-150W

Lenovo ThinkSystem **SR651**

Trace Peripheral Communication
TSMC 28nm
15 ╳ 20 mm^2
0.5 GHz
TDP 40 W
Sample length 100us
Sample Frequency <10 Hz

RCP =Reconfigurable Computing Processor
ITR =IO TRacing
MTR =Memory TRacing

Monitor and Control CPU
TSMC 28nm
15 ╳ 7 mm^2
1.0 GHz
TDP 15W

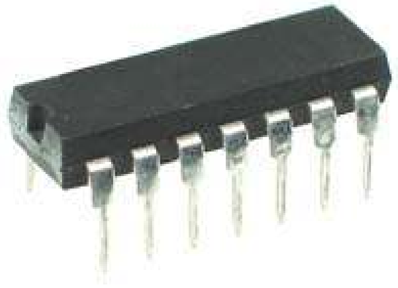
Outline

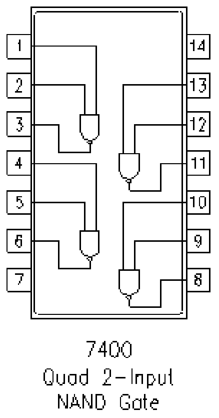
- **Motivation:** Hardware Security and Dynamic Security Check
- **Jintide Platform:** Architecture and System Features
- **Jintide Chips:** Specification and Tapeout Results
- **Conclusion**

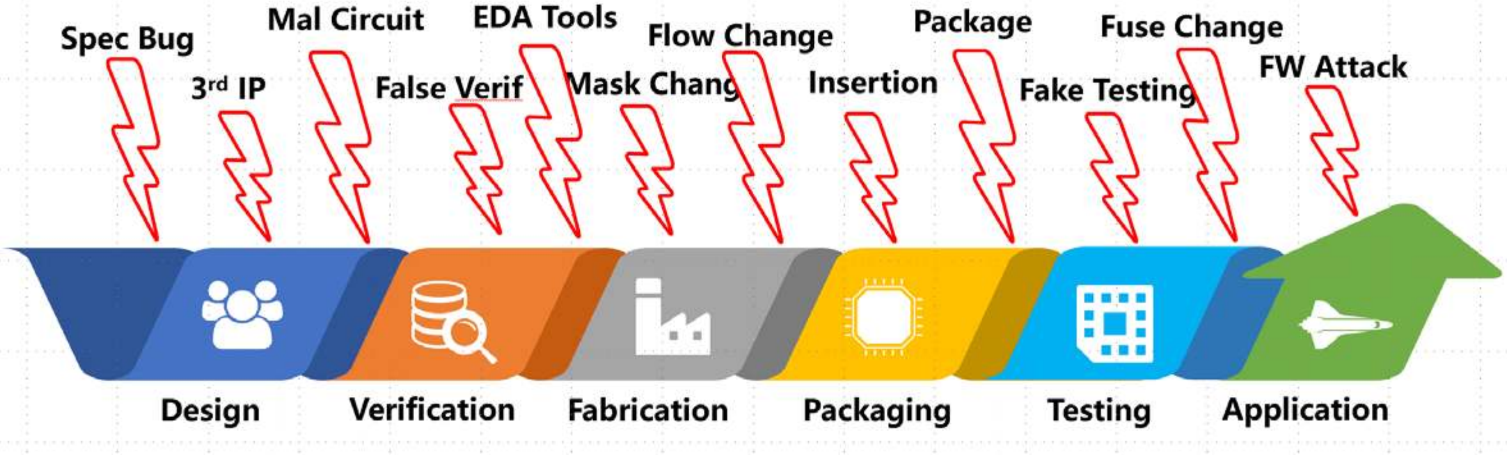
Outline

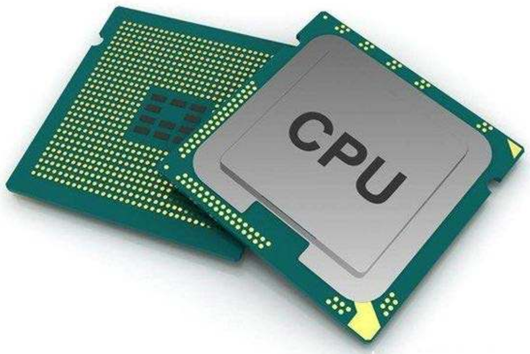
- **Motivation:** Hardware Security and Dynamic Security Check
- **Jintide Platform:** Architecture and System Features
- **Jintide Chips:** Specification and Tapeout Results
- **Conclusion**

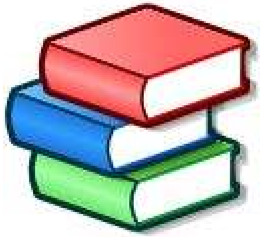
Motivation

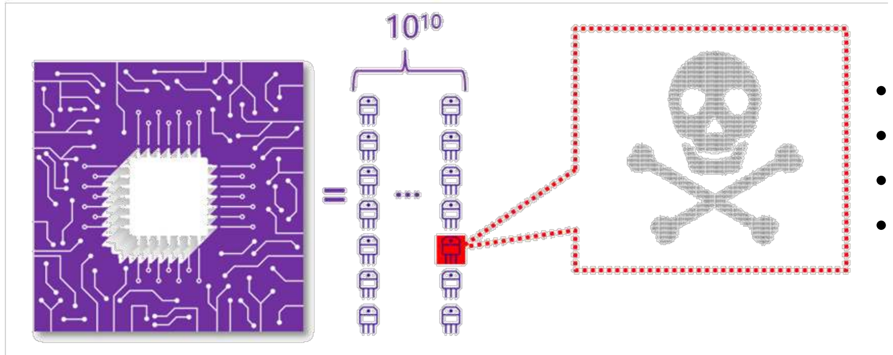












- A few logic gate…
- Parasitic Cap …[2]
- Doping …[3]
- Vulnerabilities…

- Impossible to prove if a chip is secure/trustworthy[1]
- Hardware Trust Concern : Runtime Surveillance

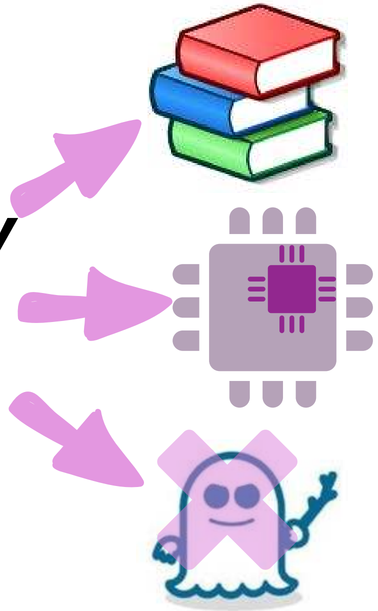
[1] Bhunia S, et al. Hardware Trojan attacks: threat analysis and countermeasures. Proceedings of the IEEE, 2014, 102(8): 1229-1247.
[2] X. Guo, H. Zhu, Y. Jin and X. Zhang. When Capacitors Attack: Formal Method Driven Design and Detection of Charge-Domain Trojans. 2019 Design, Automation &
[3] Test in Europe Conference & Exhibition (DATE), Florence, Italy, 2019, pp. 1727-1732.
Becker G.T., Regazzoni F., Paar C., Burleson W.P. Stealthy Dopant-Level Hardware Trojans. Cryptographic Hardware and Embedded Systems - CHES 2013.

Motivation

- Design a CPU chip that supports user to verify the behaviors
  - **Trace** CPU/System behavior
  - **Check** if the behavior matches **EXPECTATION**.
  - Trace and Check is done at **RUNTIME**

} **D**ynamic **S**ecurity **C**heck

User Security Expectation



Work as the Manual/Datasheet Indicated

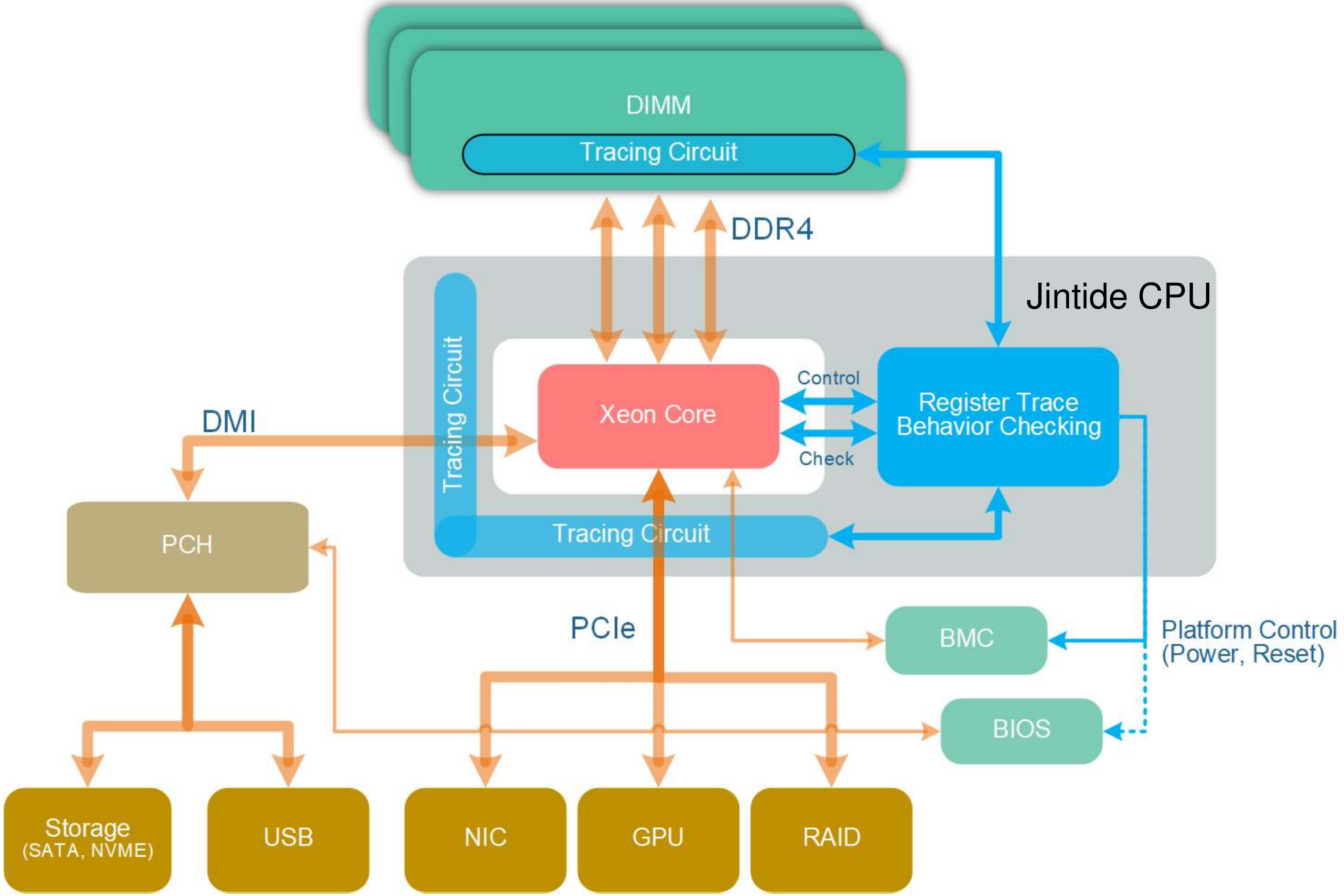
No Unrevealed Subsystem Activated

No Vulnerability / Debug Features Abuse

Outline

- **Motivation:** Hardware Security and Dynamic Security Check
- **Jintide Platform:** Architecture and System Features
- **Jintide Chips:** Specification and Tapeout Results
- **Conclusion**

Jintide Platform: System Level View



Jintide Platform: Questions

#1 : How to perform check ?

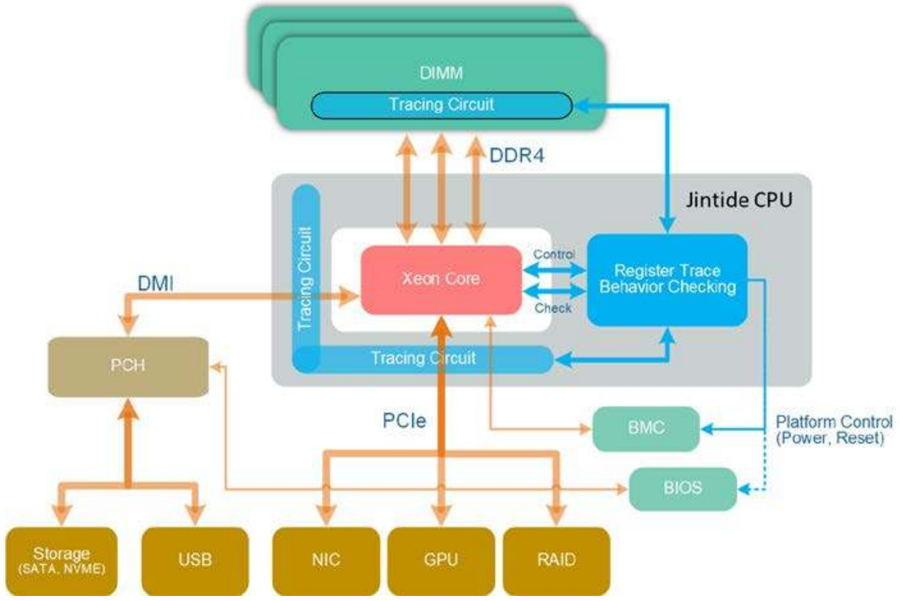
- **Identify** Legal (expected) Behavior, e.g. comparing to a golden model (ISA)
- **Ignore** No-harmful Behaviors , e.g. extra memory READ
- **Report** Suspicious Behaviors, e.g. incorrect memory / arch state update

#2: What needs to be traced?

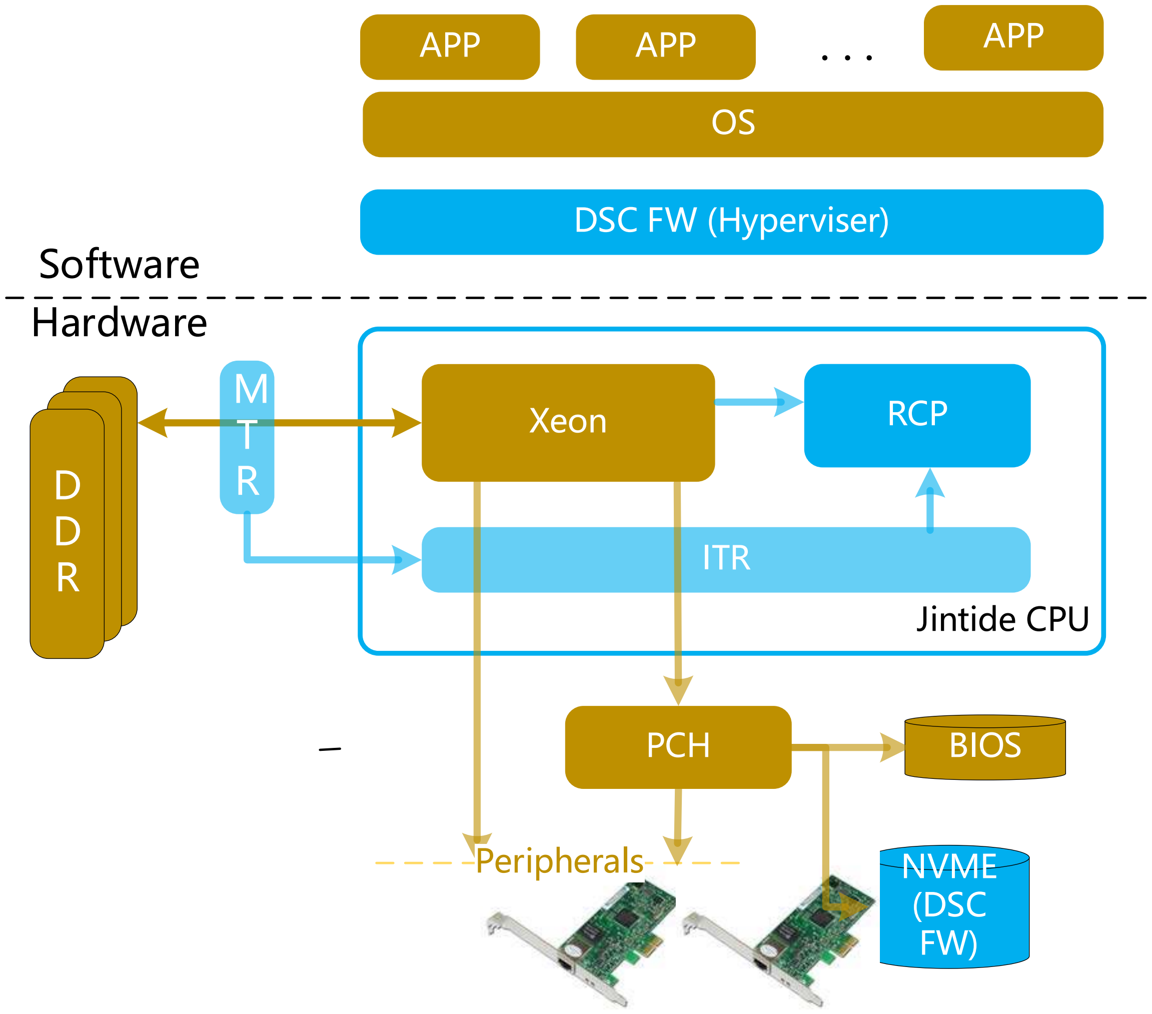
- Arch State at beginning of the Interval
- Memory R/W record during Interval
- IO record during Interval
- Arch State at the end of Interval

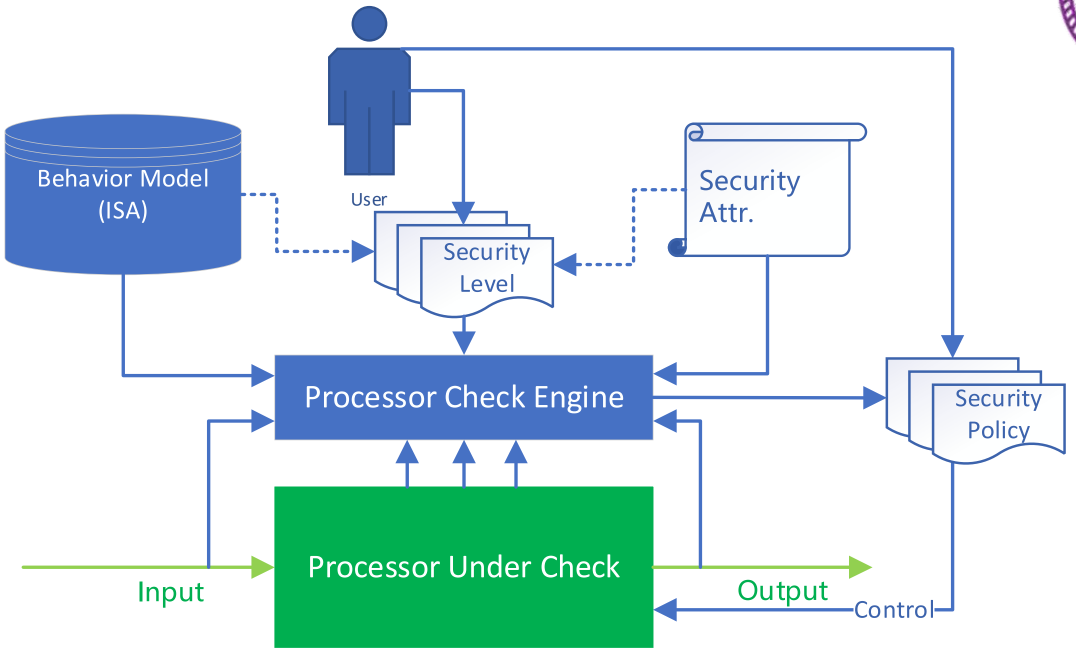
#3: How to reduce performance impact?

- Sample Approach

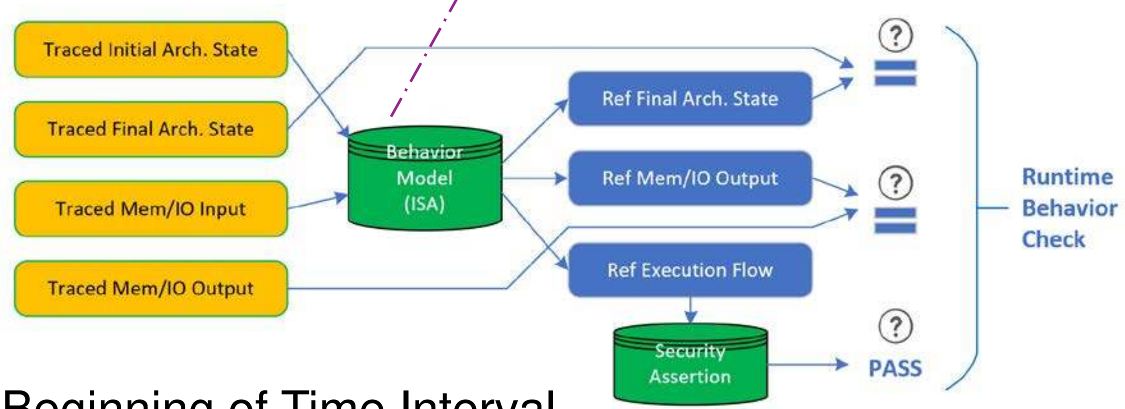


Jintide Platform: Architecture and Check Flow





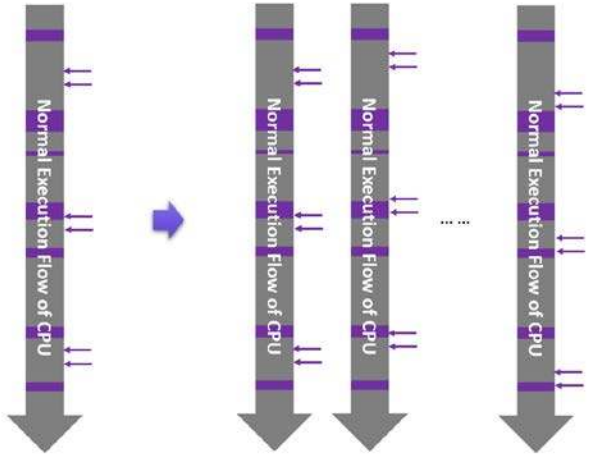
Deterministic Replay



Initial = Beginning of Time Interval
Final = End of Time Interval

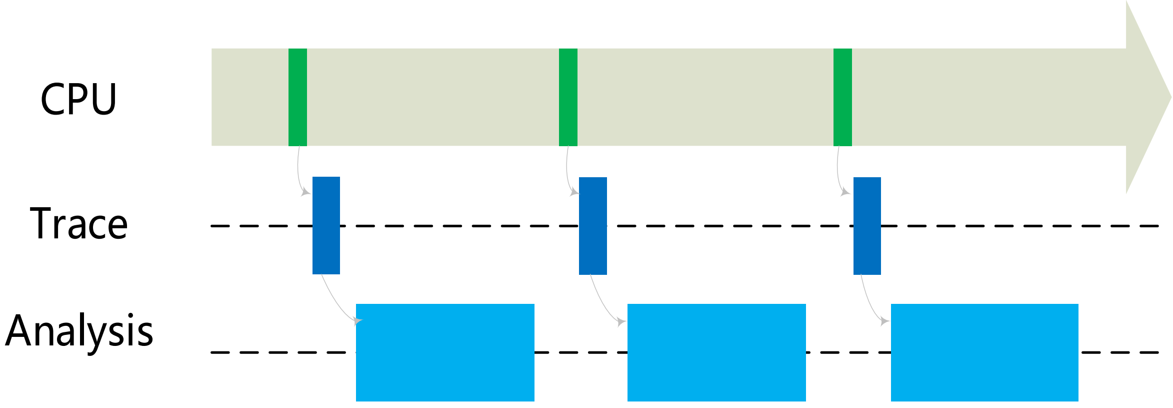
Jintide Platform: Sample Approach

- **Sample Window : <u>>100us</u>**
  - DIMM Trace Buffer Size per DIMM: 2.56 MB
  - PCIe Trace Buffer Size per Link per Lane: 8*100000/8 = 100KB
  - Total: 52 Lane UP+DOWN Stream = 10.4MB
- **Sample Frequency: <u>> 1Hz</u>**
  - Reduce one-time performance cost : e.g. Cache flush



Normal Execution Flow of CPU
Normal Execution Flow of CPU
Normal Execution Flow of CPU
Normal Execution Flow of CPU
… …

Increase HW Threat Detection Ratio through Massive Deployment



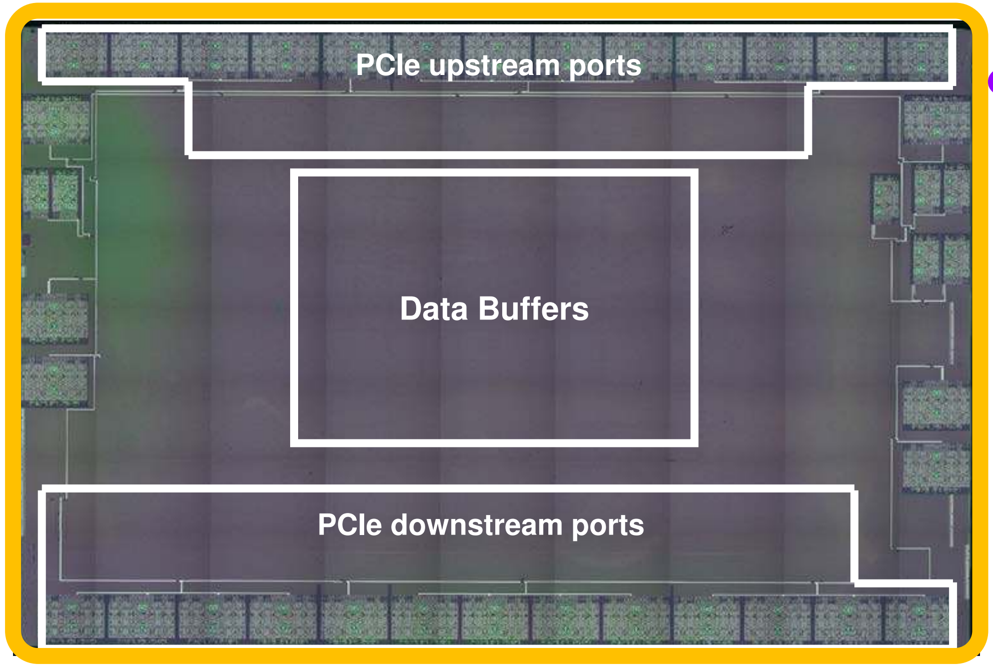
Sample (Trace and Analysis) Model

Outline

- **Motivation:** Hardware Security and Dynamic Security Check
- **Jintide Platform:** Architecture and System Features
- **Jintide Chips:** Specification and Tapeout Results
- **Conclusion**

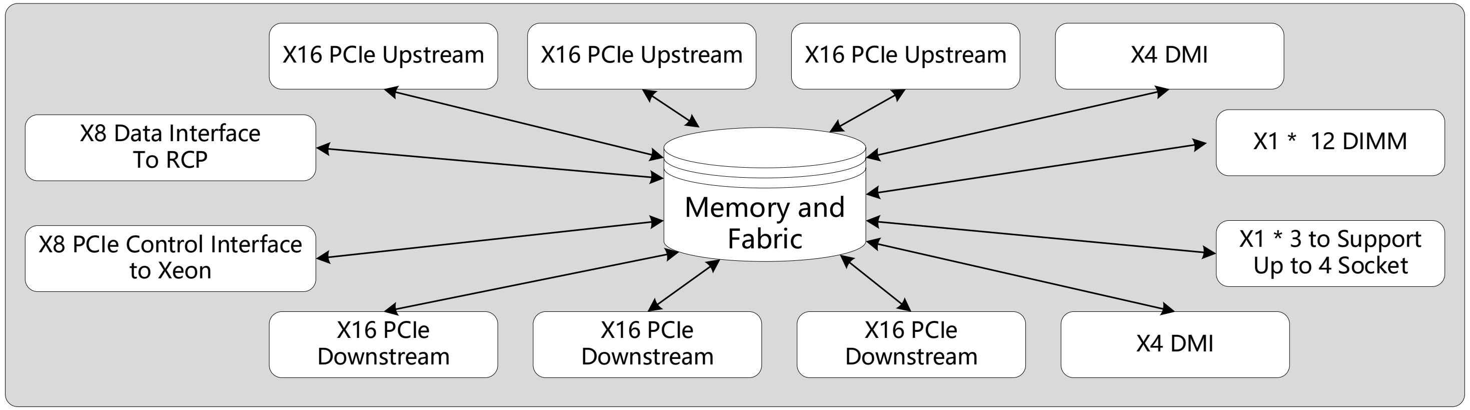
Jintide Chips: ITR

IO Tracing Chip For Skylake



Trace Peripheral Communication

- TSMC 28nm
- 15 ╳ 20 mm^2
- 0.5 GHz
- TDP 40 W
- Sample length >100us
- Sample Frequency >1 Hz



X16 PCIe Upstream

X16 PCIe Upstream

X16 PCIe Upstream

X4 DMI

X8 Data Interface To RCP

X1 * 12 DIMM

Memory and Fabric

X8 PCIe Control Interface to Xeon

X1 * 3 to Support Up to 4 Socket

X16 PCIe Downstream

X16 PCIe Downstream

X16 PCIe Downstream

X4 DMI

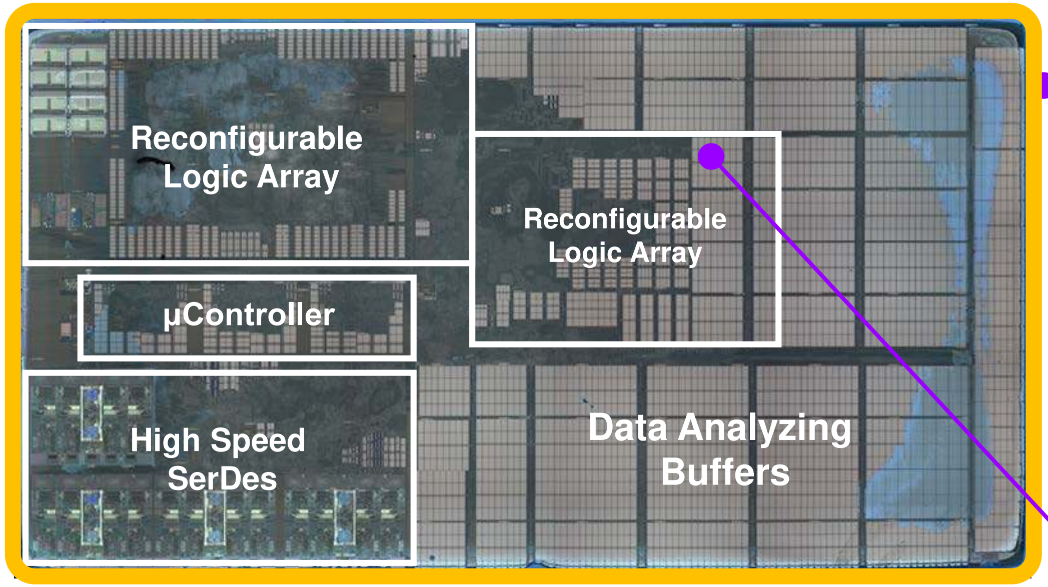
Key Parameters

- 60+ MB on chip memory
  - 2.56 MB *12 for DIMM
  - 10MB+ for PCIe
- 136 PCIe Gen3 Lanes
  - X16*3+X16*3 For PCIe
  - X4+X4 for DMI
  - X1*12 for DIMM data collection
  - X8 for Xeon Connection
  - X8 for RCP Connection
  - X1*3 UDI for Up to 4S support

Full bifurcation support : 16/8*2/4*4

Jintide Chips: RCP

RCP Chip for Data Analysis

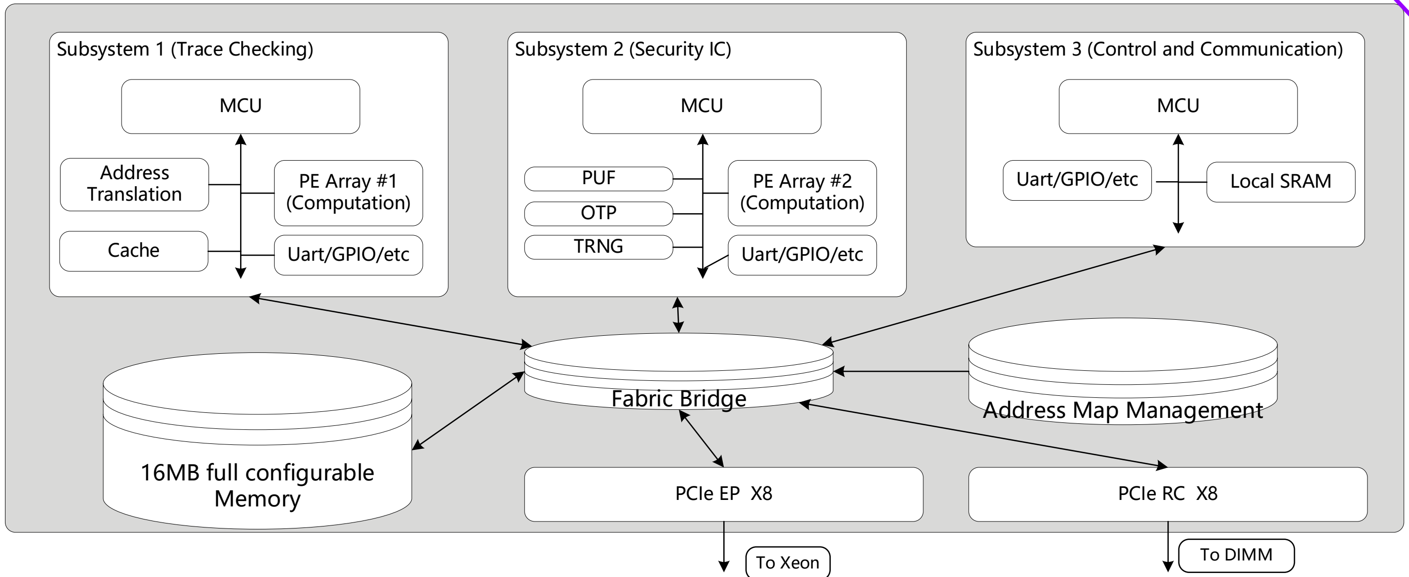


Monitor and Control CPU

TSMC 28nm
15 ╳ 7 mm^2
1.0 GHz
TDP 15W

Key Parameters

- 16 MB on chip memory
- 3 * MCU running @ 1GHz
- Two PCIe Ports
  - X8 EP
  - X8 RC
- 3 Subsystem
- Two Reconfigurable Logic Array
- to accelerate behavior analysis (instruction emulation)

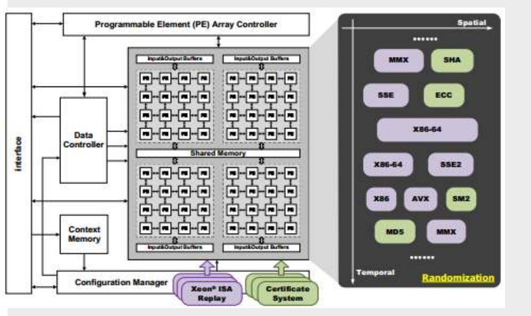


Subsystem 1 (Trace Checking)
MCU
Address Translation
Cache
PE Array #1 (Computation)
Uart/GPIO/etc

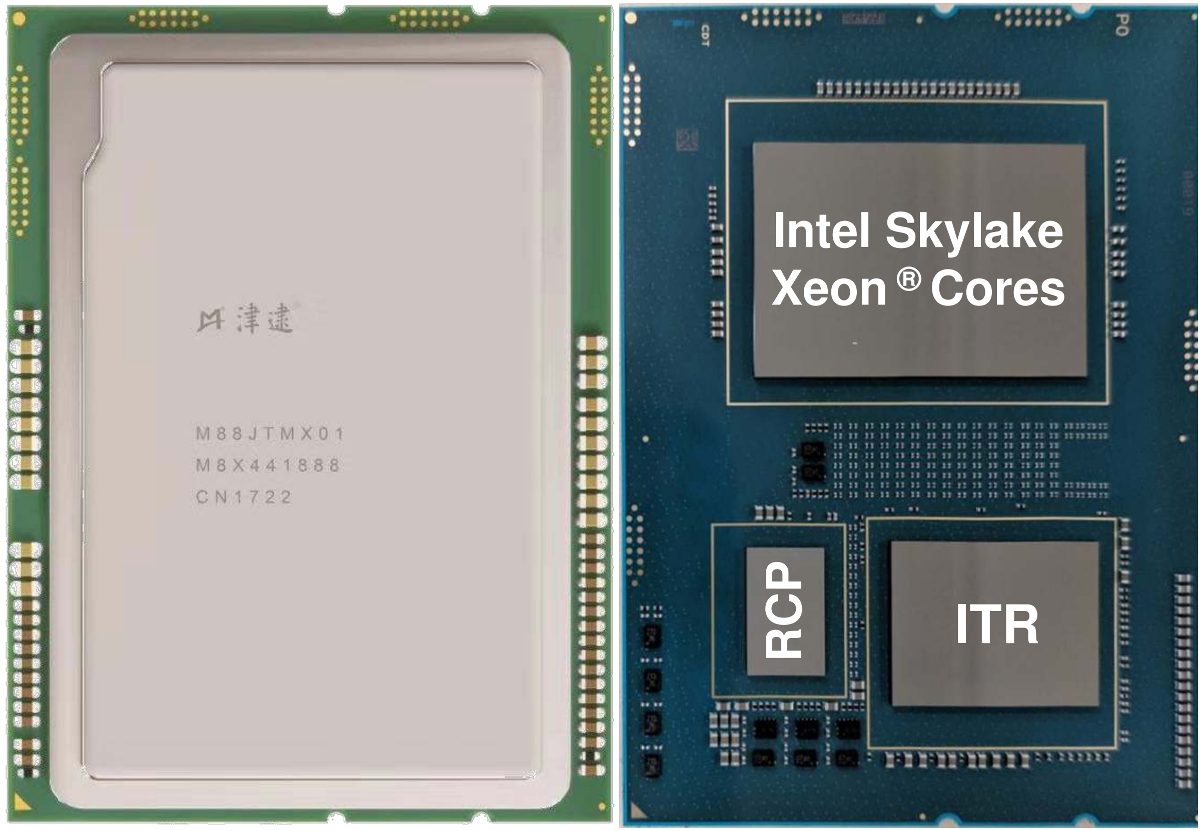
Subsystem 2 (Security IC)
MCU
PUF
OTP
TRNG
PE Array #2 (Computation)
Uart/GPIO/etc

Subsystem 3 (Control and Communication)
MCU
Uart/GPIO/etc
Local SRAM

16MB full configurable Memory
Fabric Bridge
Address Map Management
PCIe EP X8
PCIe RC X8
To Xeon
To DIMM

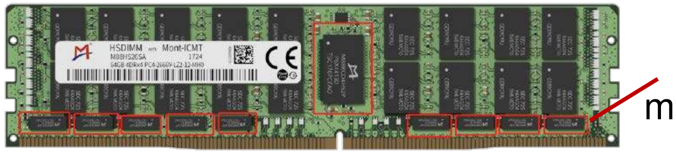


Jintide Chips: MCP (Multi-Chip Package)



Jintide® Server CPU

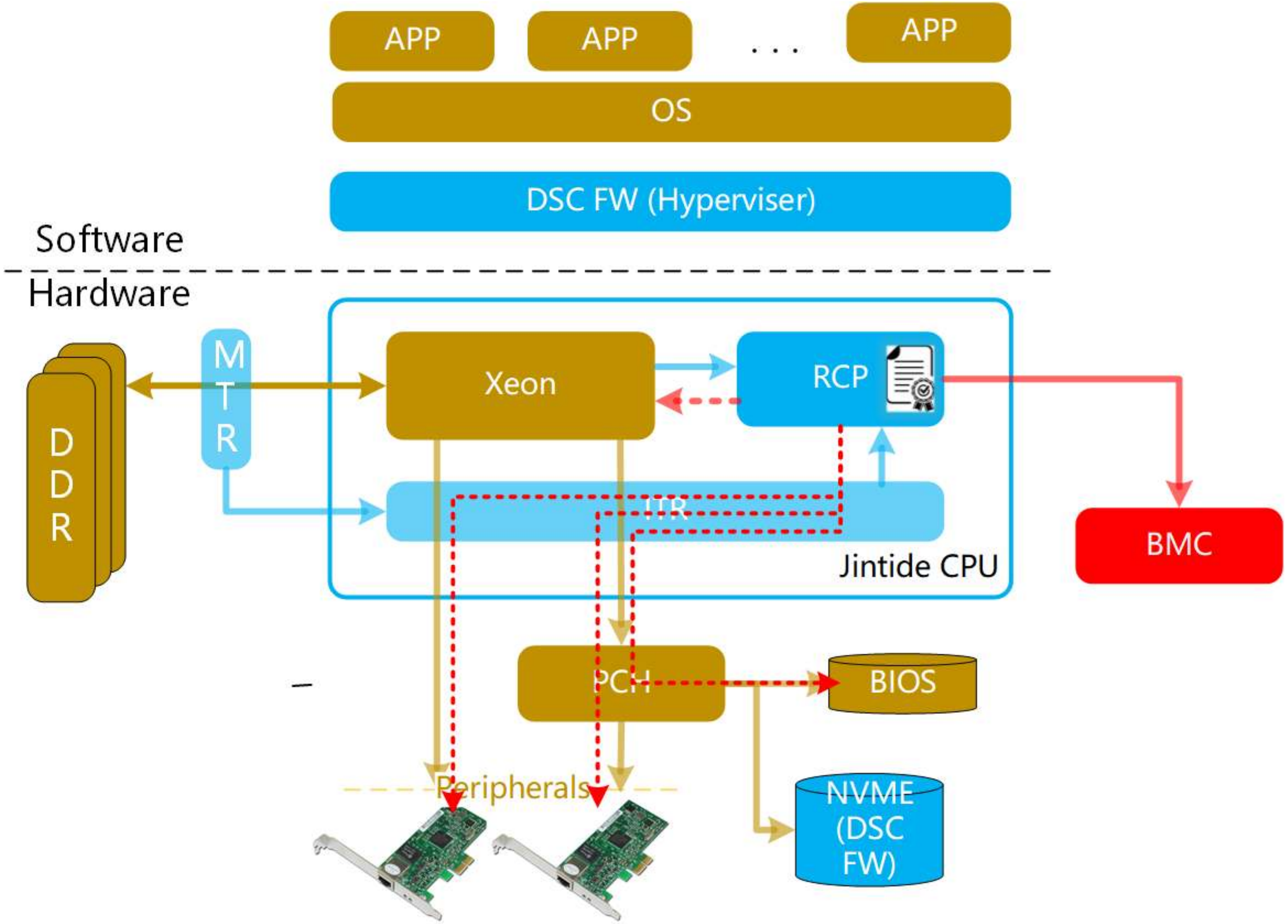
Performance	Description
# of Cores	Up to 24, Hyper-Threading
Base Frequency	2.0G, 2.1G, 2.2G
TDP	145W – 205W
Scalability	1S, 2S, 4S
UPI Speed	9.6 GT/s, 10.4 GT/s
PCH Supported	C620 series
DMI3	DMI3 x4 8GT/s
PCIe	PCIe Gen3 x48



RCD+DB = MTR,
modified from LRDIMM
buffer

DDR4 DIMM with MTRs

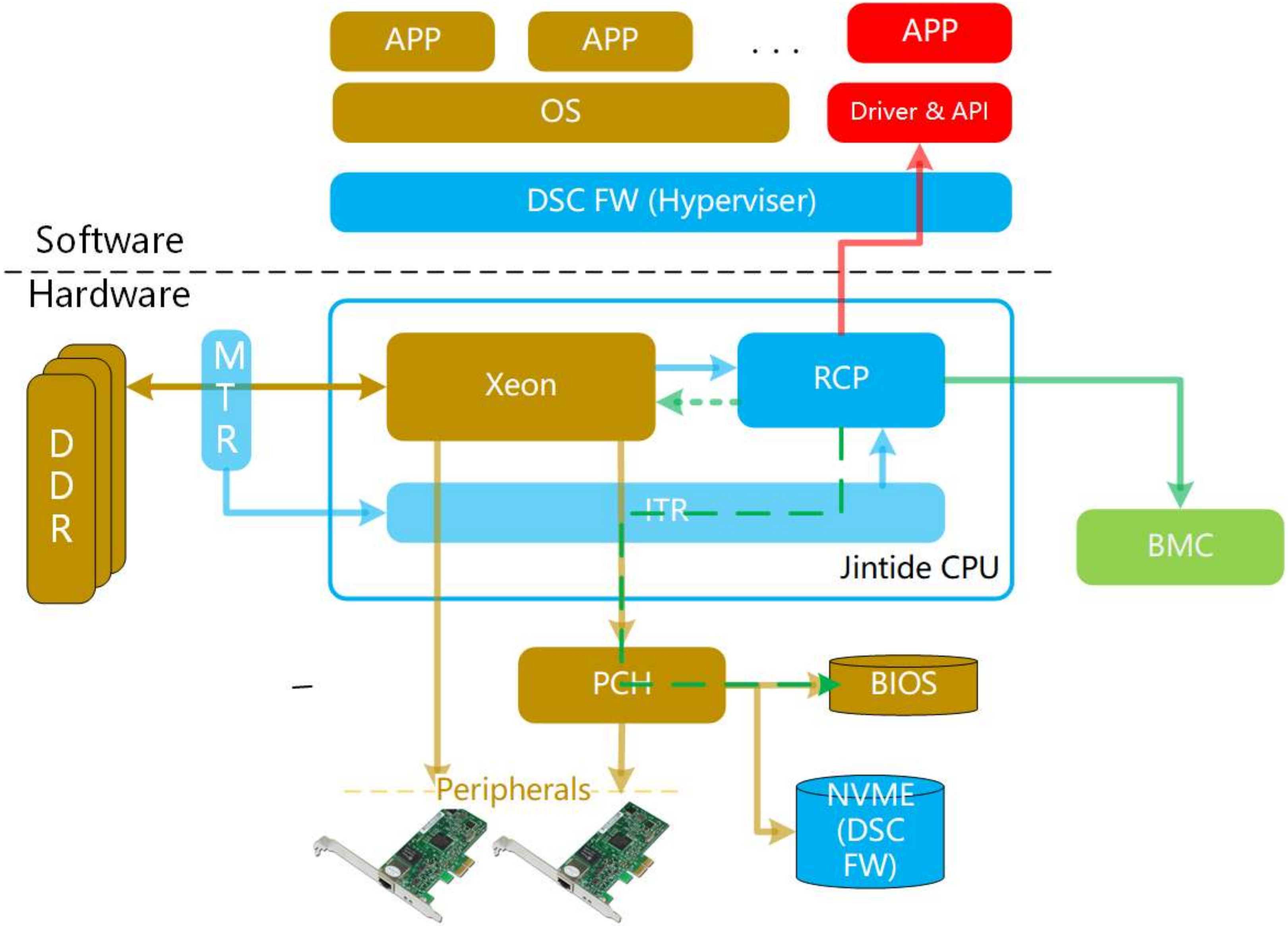
Jintide Chips: Features



Jintide Secure Boot

- Root of Trust in MCP Package
- CPU Reset Hold
- BIOS Access Through PCH
- Certificate Based
- Device Verification (In Dev.)

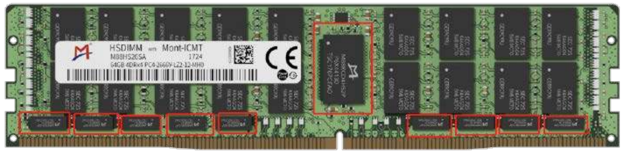
Jintide Chips: Features



Jintide Open API (WIP)

- Encryption
- Identity (PUF)
- Key Gen/Management
- External Bahav. Tracing
  - IO Trace API
  - Memory Trace API
  - Execution Flow Rebuild

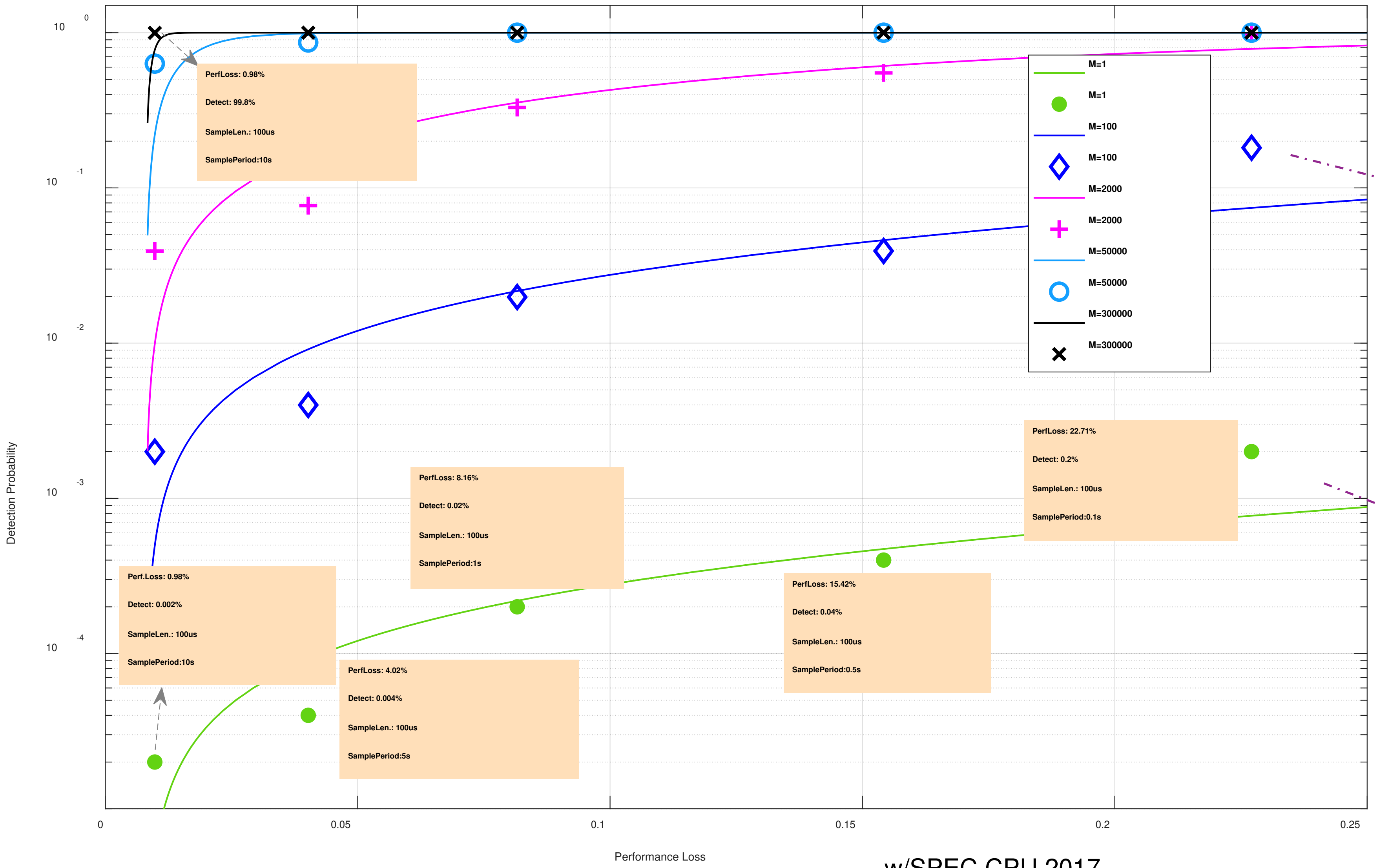
Jintide Platform and Chips: Summary



Jintide®

- □ X86 Processor with Dynamic Security Check
  - □ 1Hz Check Freq. Perf Loss< 10%
  - □ 100 us Check Interval Length
  - □ Physical Memory/IO Trace
  - □ Replay Based Behavior Analysis
- □ Other Values
  - □ Security Boot Support
  - □ Encryption Offloading & API

Jintide Chips: Perf. Loss vs Detection



Others:
Calculated result

Green dot:
measured result

w/SPEC CPU 2017

Jintide Chips: Detection of Trojan

Example: Microcode Attack (Trojan) -- Only to illustrate detection

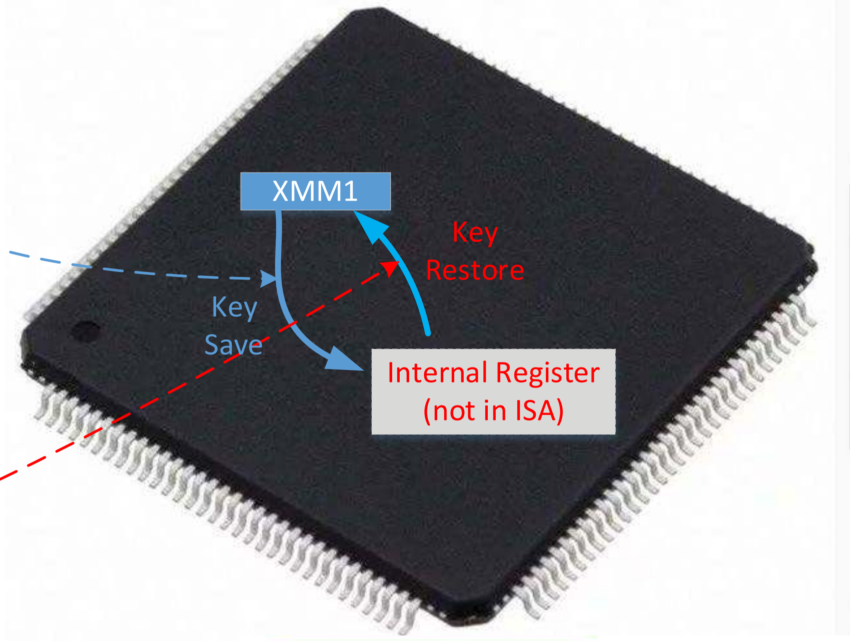
CPU: CPU Execution Flow

Victim Process:

```
        move xmm1, aes_key
RoundKeyGen:
        aeskeygenassist xmm2, xmm1, 0x01
        ......
```

Hacker Process

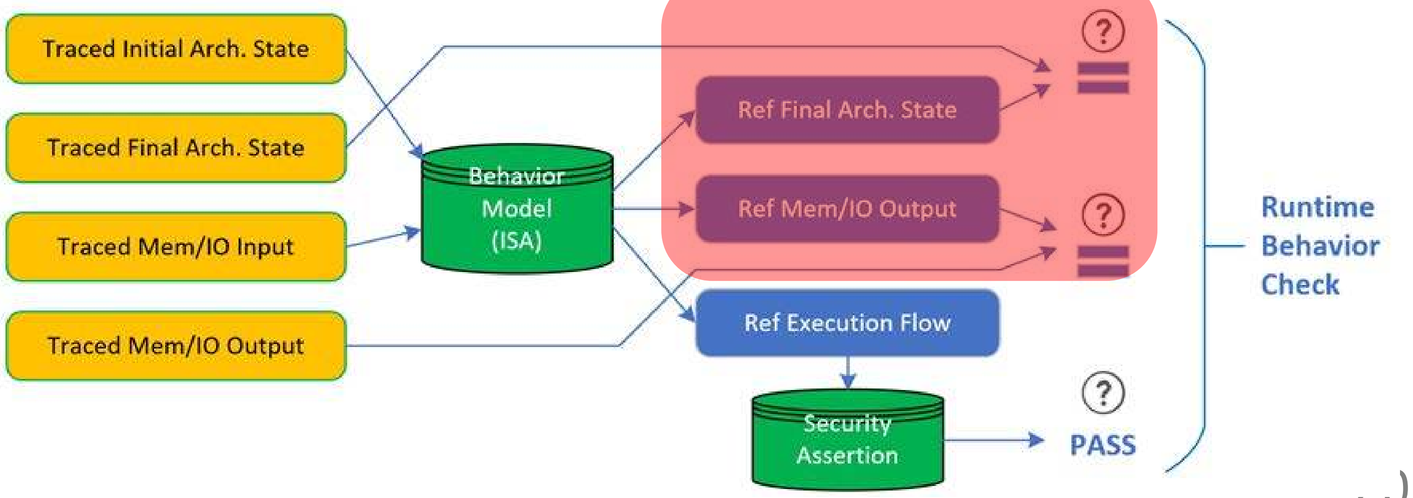
```
        move xmm1, PASS_key
RoundKeyGen:
        aeskeygenassist xmm2, xmm1, 0x01
        ......
```



Checked CPU Execution Flow Restore

```
        move xmm1, PASS_key
RoundKeyGen:
        aeskeygenassist xmm2, xmm1, 0x01
        ......
```

Mismatch Found!



Jintide Chips: Detection of Vulnerabilities

Example: Spectre Attack Detection

```
if (x < array1_size) {
    temp &= array2[array1[x] * 512];
}
```

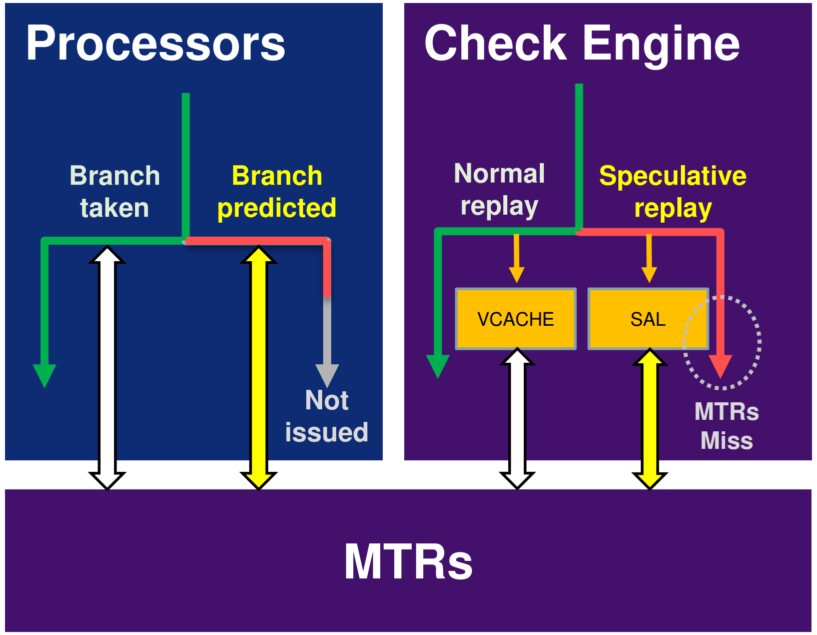
◆ **Spectre Attacks (two-stage):**

Access secrets
Transient instructions

⇨

Recover secrets
Flush + Reload

◆ **Detection Strategy (Speculative Replay):**



SAL= Speculative Address List
VCACHE = Virtual Cache

- Step 1: Enable Speculative Replay
  - Length bounded : MTR trace availability
- Step 2: Record in one speculative branch, SAL contains
  - Access to *array1[x]*   *--- Leaked Secret*
  - Access to *array2[array1[x]]*   *--- Probe Target*
- Step 3: Side channel attack detect : *array2[0-255]*
  - ***Probe Target is loaded by Prediction Branch***
    - *Probe Target In SAL, not in VCACHE*
  - Secret *: array1[x]*

Spectre Attack Demo: https://github.com/flxwu/spectre-attack-demo.

Jintide Chips: Detection of Vulnerabilities

- **Behavior Check Model Selection**
  - Current : ISA Model
  - Move to : Micro-Architecture Model (non-deterministic?)
- **Based on Characteristic of the Attack**
  - No General Rule to Detect All Attacks
  - Not All Attacks Can be Detected by Rules

Outline

- **Motivation:** Hardware Security and Dynamic Security Check
- **Jintide Platform:** Architecture and System Features
- **Jintide Chips:** Specification and Tapeout Results
- **Conclusion**

Conclusion

Jintide® : A Hardware Security Enhanced Server CPU

- **Goal**: Hardware Security by Runtime Tracing/Checking
- **Jintide Solution**:
  1. **Tracing (Arch. State, IO, Memory) with Low Sample Rate to reduce perf. impact**
  2. **ISA-model Replay and Assertions** to check hardware behaviors
- **Jintide ICs:**
  1. **Hardware Tracing Chips**
  2. **Reconfigurable Chip**
  3. **Tape out:** TSMC 28nm, MCP
- **Experiment :** Performance vs Detection Ratio, Trojans/Spectre

Acknowledgement

- Gil Neiger
- Asit Mallick
- Eddie Dong
- Akhilesh Kumar
- Shalesh Thusoo
- Luke Chang
- Roy Zeng

- Sailesh Kottapalli
- Ronak Singhal
- Tejas Desai
- Howard Borchew
- Guntram Wolski
- Anitha Loke