芯来科技
NUCLEI

高可靠性高安全性RISC-V处理器设计与实现

彭剑英 @芯来科技

芯来科技
NUCLEI

About Nuclei System Technology
关于芯来科技

芯来科技（Nuclei System Technology）是中国领先的RISC-V处理器内核IP和解决方案公司，聚焦RISC-V处理器内核研发，赋能本土AIoT产业生态。

- 公司产品处于RISC-V嵌入式处理器自主研发与产业化的最前列，具备高性能、低功耗和易用的特点，已应用在兆易，晶晨等多家知名客户量产产品中。
- 提供针对安全，汽车、工业控制和AI等领域的RISC-V处理器及配套解决方案。
- 创立以来发展迅速，并受到资本的青睐，目前已经完成知名投资机构数轮投资。
- RISC-V基金会银级会员、中国RISC-V产业联盟副理事长单位、中国开放指令生态(RISC-V)联盟会员单位。

信息请访问: www.nucleisys.com

请扫码关注我们：

官方公众号

硅农亚历山大

芯来科技 NUCLEI

芯来科技RISC-V处理器可满足AIoT的各种场景需求

	N级别 32位架构 MCU, 边缘计算, AIoT, 安全		NX级别 64位架构 存储, AR/VR, AI			UX级别 64位架构 Linux, 数据中心, 网络设备, 基带		
900系列 9 Stages Dual-issue	**N900**	对标 ARM Cortex M7 ARM Cortex R4 ARM Cortex R5 ARM Cortex R7	**NX900**	**NX900 多核**	对标 ARM Cortex M7 ARM Cortex R5 ARM Cortex R7 ARM Cortex R8	**UX900**	**UX900 多核**	对标 ARM Cortex A9 ARM Cortex A53
600系列 6 Stages Single-issue	**N600**	对标 ARM Cortex M7 ARM Cortex R4 ARM Cortex R5	**NX600**	**NX600 多核**	对标 ARM Cortex M7 ARM Cortex R4 ARM Cortex R5	**UX600**	**UX600 多核**	对标 ARM Cortex A5 ARM Cortex A7
300系列 3 Stages Single-issue	**N300**	对标 ARM Cortex M33 ARM Cortex M4 ARM Cortex M4F						
200系列 2 Stages Single-issue	**N200**	对标 ARM Cortex M0 ARM Cortex M0+ ARM Cortex M3 ARM Cortex M23						
100系列 2 Stages Single-issue	**N100**	对标 8位/16位内核 ARM Cortex M0 ARM Cortex M0+						

可选特性

- 安全
- 可靠
- 扩展
- DSP
- 浮点
- 矢量
- NN

芯来科技 NUCLEI

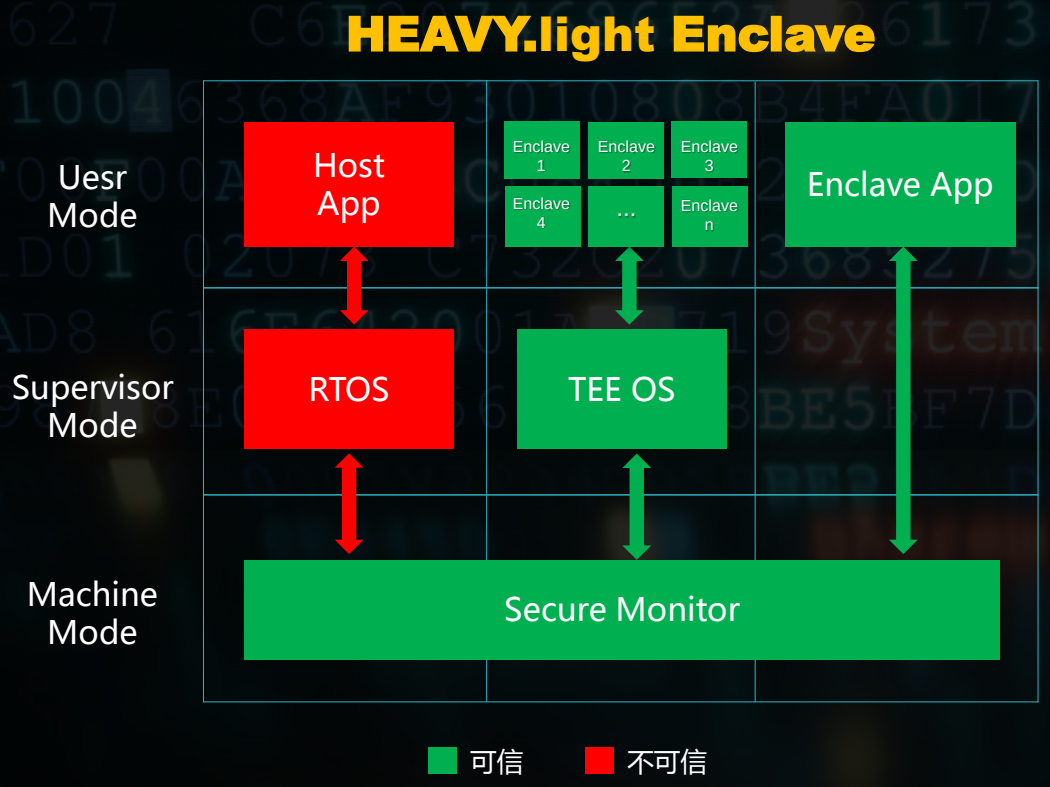
安全和靠性是AIoT的基础

AIoT具备**场景丰富**，**万物互联**，**智能化**但同时如何保护数据和连接安全，如何保证在汽车，工业和医疗等领域高可靠性成为AIoT落地的基础。

TEE方案保证应用安全

芯来科技 NUCLEI + TrustKernel 上海瓶钵信息科技有限公司

芯来科技联合瓶钵科技联合推出基于RISC-V的TEE方案**HEAVY.light Enclave**，为AIoT应用安全保驾护航

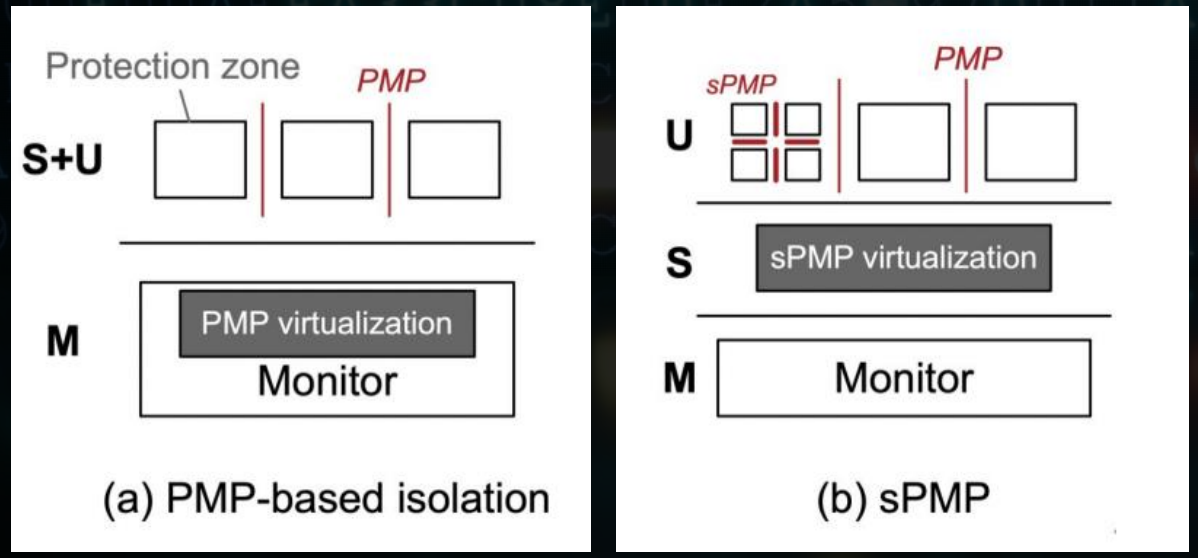


- 基于RISC-V Privileged ISA的软硬件协同设计的TEE安全架构
- 极小的TCB (Trusted Computing Base)
- 对Enclave和其他应用或OS之间提供硬件隔离
- 对单Enclave提供无需TEE OS参与的轻量级的物理隔离
- 对多Enclave则由TEE OS提供物理隔离
- 对于同一TEE OS管理的Enclave之间通讯高效快速
- Secure Boot和Remote Attestation

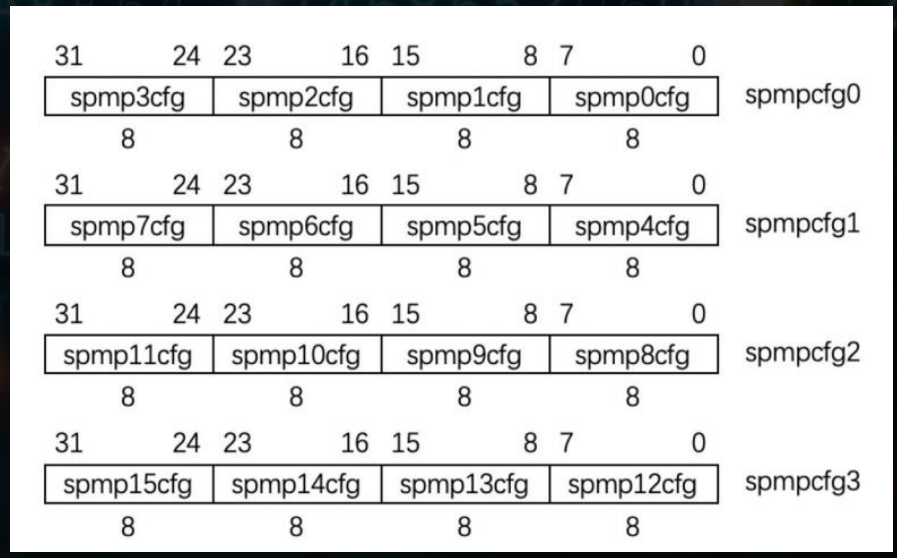
基于sPMP的TEE方案

相对于基于PMP的TEE方案，基于sPMP方案减少了TCB（Trusted Computing Base）增加了灵活性。芯来科技32位内核增加4组CSR，每个sPMP entry占用8bit，共计16个sPMP entries。

sPMP更具灵活性



16个sPMP Entries

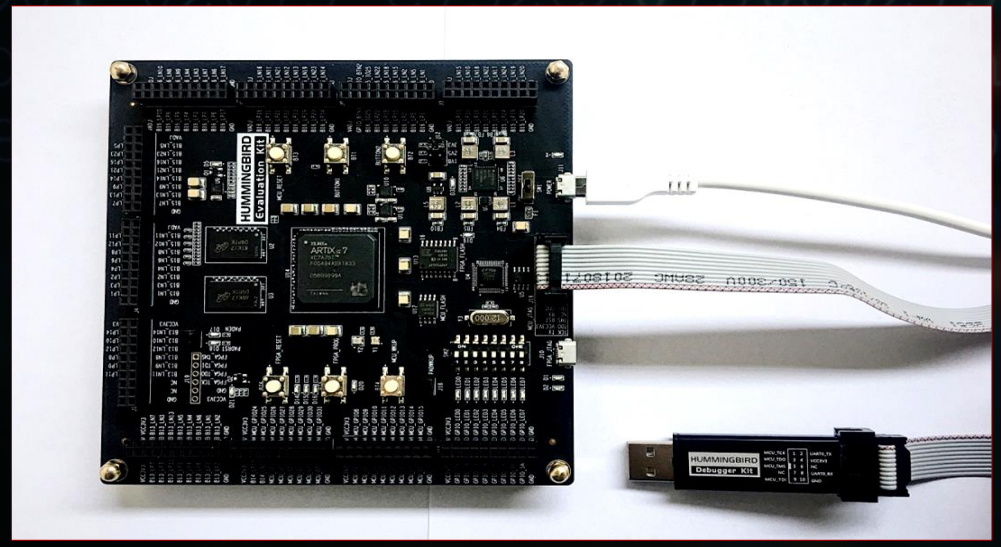


同其他方案的比较

System	Cache side channel	Enter/exit	Enclaves communication	Scalability	MM granularity
ARM PSA	Physical partition	medium	fast	no limited	fine
Sanctum	DRAM partition	slow	slow	Limited by DRAM Region	coarse
KeyStone	No defense	(Ecall) medium	(Ecall) medium	Limited by PMP registers	coarse
MultiZone	No defense	(Ecall) medium	(Ecall) medium	PMP reuse	coarse
SoftwareTEE	No defense	(Ecall) medium	(Ecall) medium	PMP reuse	coarse
Heavy.light Enclave	Dynamic partition*	(Ecall) medium	fast in the same TEE OS	no limited	fine

TEE运行实测

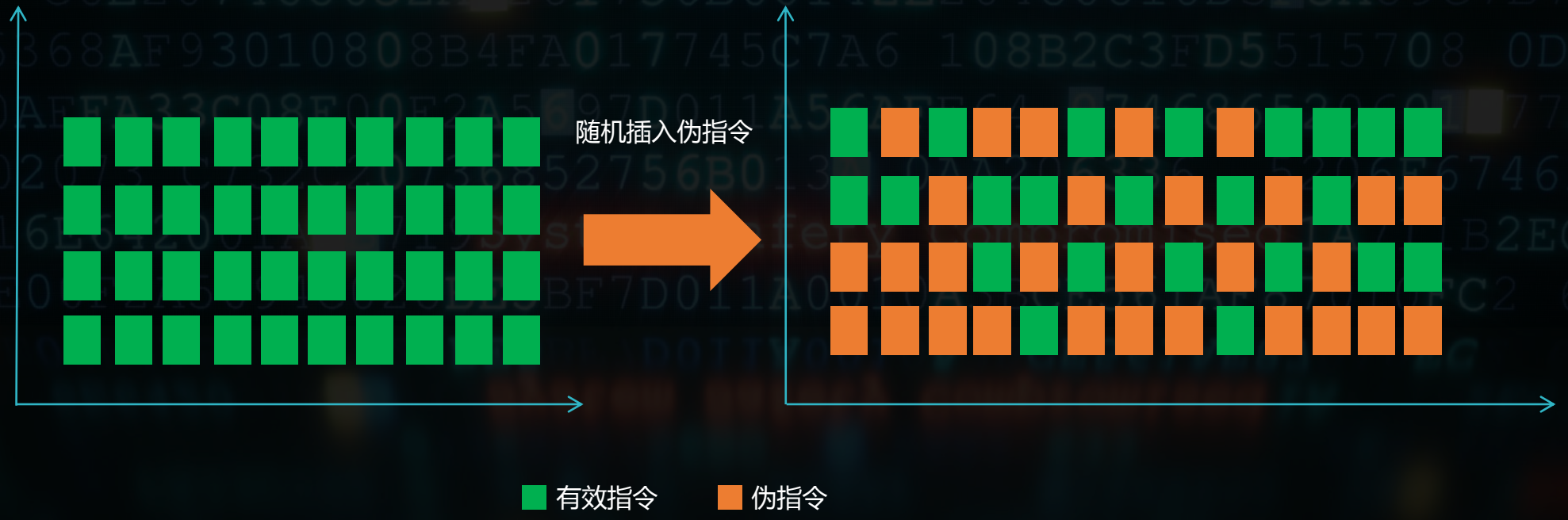
- 基于芯来科技N200内核在芯来FPGA EVB上的实际运行效果
- Blackwater为TEE
- 该Demo演示了链式Enclave创建以演示多Enclave能力




```
*                                    *
**************************************
**************************************
[Log] Blackwater init start
[Log] Blackwater init done
In the ret_to_payload, the payload addr is 0x80006000
Untrusted is invoking enclave
Enclave[id:0] handle request
Enclave[id:0] starts to invoke Enclave[id:1]
Enclave[id:1] handle request
Enclave[id:1] starts to invoke Enclave[id:2]
Enclave[id:2] handle request
Enclave[id:2] starts to invoke Enclave[id:3]
Enclave[id:3] handle request
Enclave[id:3] starts to invoke Enclave[id:4]
Enclave[id:4] handle request
Enclave[id:4] starts to invoke Enclave[id:5]
Enclave[id:5] handle request
Enclave[id:5] starts to invoke Enclave[id:6]
Enclave[id:97] handle request
Enclave[id:97] starts to invoke Enclave[id:98]
Enclave[id:98] handle request
Enclave[id:98] starts to invoke Enclave[id:99]
Enclave[id:99] handle request
Enclave[id:99] starts to invoke Enclave[id:100]
Enclave[id:100] handle request
```

通过随机化防止物理旁路攻击

可以支持通过插入随机伪指令达到功耗随机化以防止电磁，功率和时间旁路攻击



通过扩展机制可以增加加密算法等的支持

芯来NICE(Nuclei Instruction Co-Unit Extension)扩展方案通过四个步骤且无需修改编译器便可以获得领域处理器和领域SDK，助力客户快速开发出面向领域架构具备差异化的产品。

1. 扩展自定义指令集

- 根据领域应用分析需要硬件加速的算法和对应指令
- 在RISC-V指令集预留的扩展指令空间中分配所需要指令

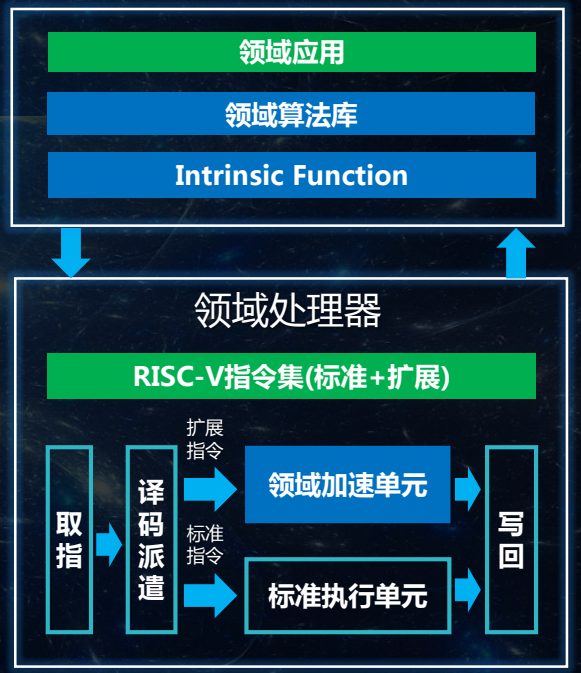
2. 实现领域加速单元

- 基于处理器微内核预留了NICE接口实现针对特定领域的加速单元
- 通过和微内核结合形成面向领域的处理器
- 领域加速单元可以和处理器微内核共享存储等资源，面积，功耗和性能优于一般总线外挂协处理器方式

3. 实现面向领域函数和库

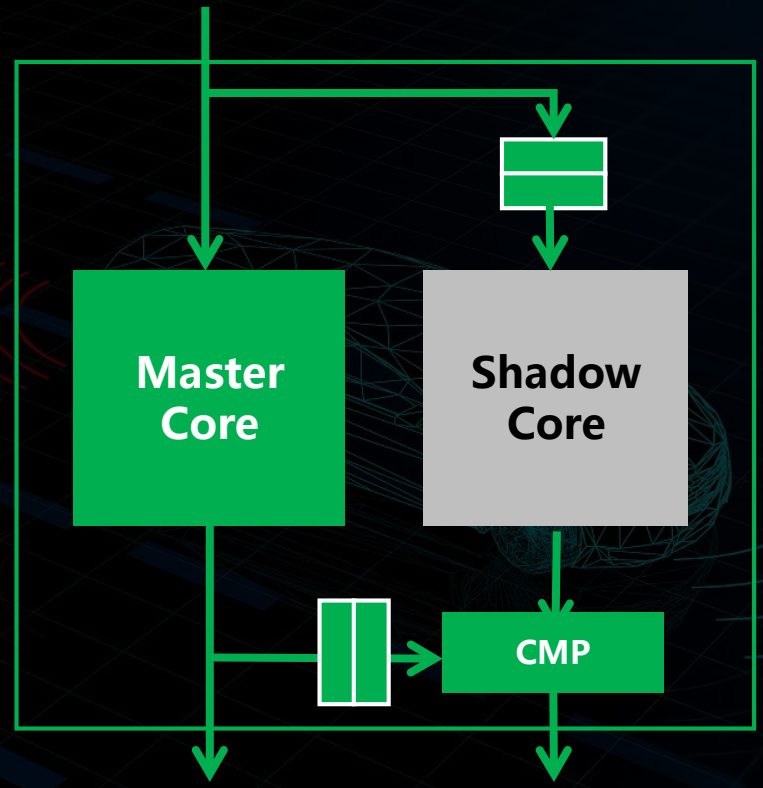
- 由于RISC-V工具链能自动识别扩展汇编指令，因此扩展指令不需要修改编译器
- 软件在使用自定义扩展指令时以Intrinsic Function的形式对扩展的汇编指令进行封装，然后以库的形式提供给应用，应用程序调用库函数。

4. 面向领域应用开发



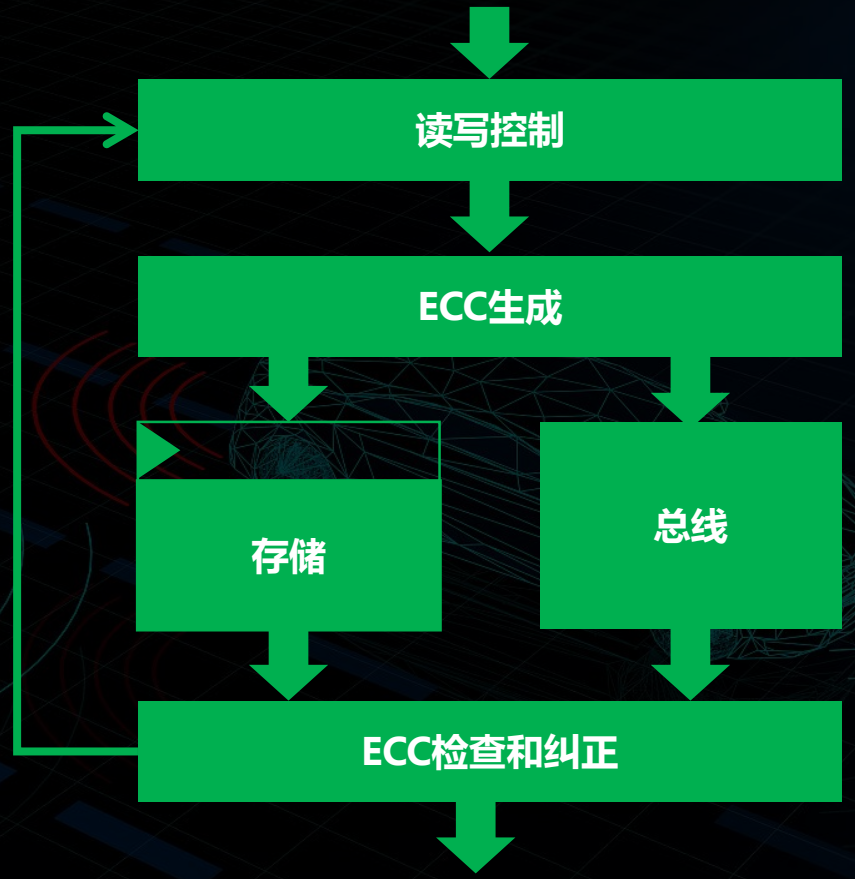
双核锁步保证逻辑可靠性

- 输入被送到主核和从核，送到从核的输入被延迟2个周期
- 主核和从核的输出被进行比较，主核的输出被延迟2个周期
- 比较主从双核的输出何关键内部状态，例如PC， ILM/DLM读写口，外部总线接口输出等如果不匹配则抛出错误
- Delay Flops使用奇偶校验的方式进行保护
- CMP逻辑被Dual-Rail Logic的方式进行保护
- 可以通过CSR开启关闭双核锁步，结果比较
- 可以通过CSR进行故障注入用作测试的目的



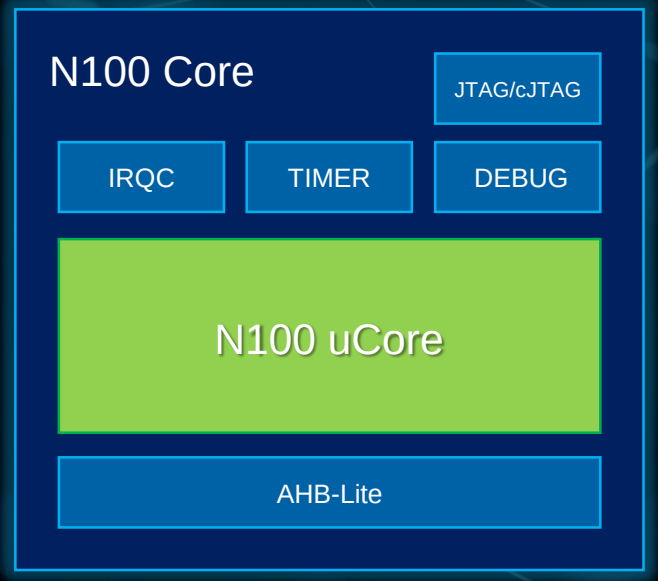
通过ECC对存储和总线进行保护

- 在写入SRAM或总线前增加ECC生成逻辑
- 目前遵循的是SECDEC（Single-Error shiand Double Error Detection）方案即单位错误纠正，多位错误则抛出Bus Error Exception，因此ECC需要额外7位数据保存
- 可以根据客户实际需要纠错的位数定制额外的ECC编码长度
- 可以通过CSR来控制ECC特性的开启和关闭



N100系列极低功耗RISC-V处理器

N100系列处理器内核是由芯来科技开发的一款商用RISC-V处理器内核系列，主要面向极低功耗与极小面积的场景而设计，非常适合传统的8位内核或16位内核升级需求，可广泛应用于模混合、IoT或其他超低功耗场景。



9K
门数可小至9K

RISC-V
RV32EC指令集

两级变长流水设计

机器模式

20位寻址位宽

AHB-Lite 32位总线

RISC-V调试标准

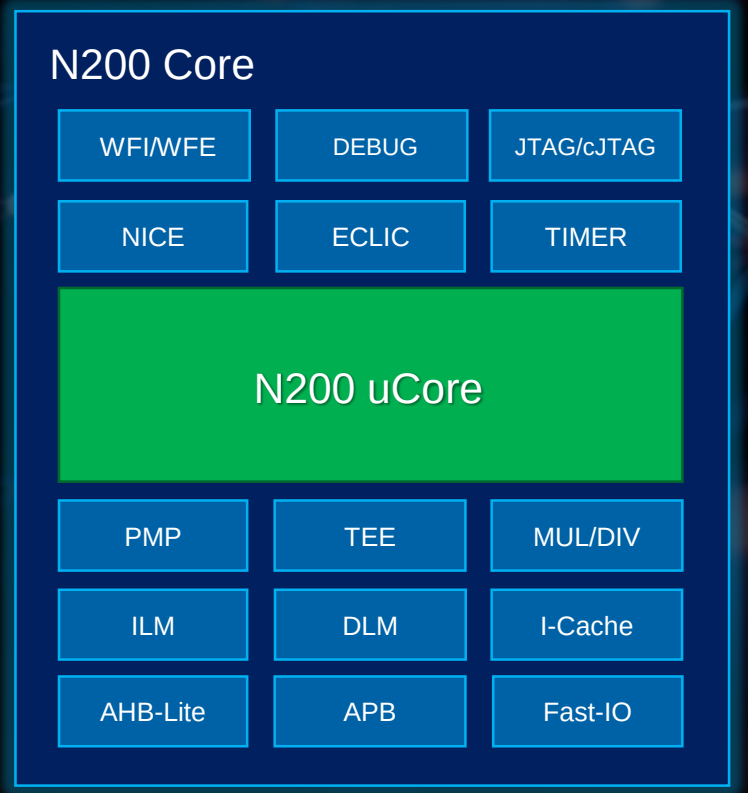
标准JTAG和两线调试接口

高实时性中断机制

成熟的开发调试环境

N200系列超低功耗RISC-V处理器

N200系列32位超低功耗RISC-V处理器为物联网IoT终端设备的**感知**，**连接**，**控制**以及**轻量级智能应用**而设计。



面向超低功耗场景

RV32I/E/M/A/C

两级变长流水设计

机器模式用户模式监督模式

支持PMP和TEE等多种安全机制

AHB-Lite和APB 32位总线

RISC-V调试标准

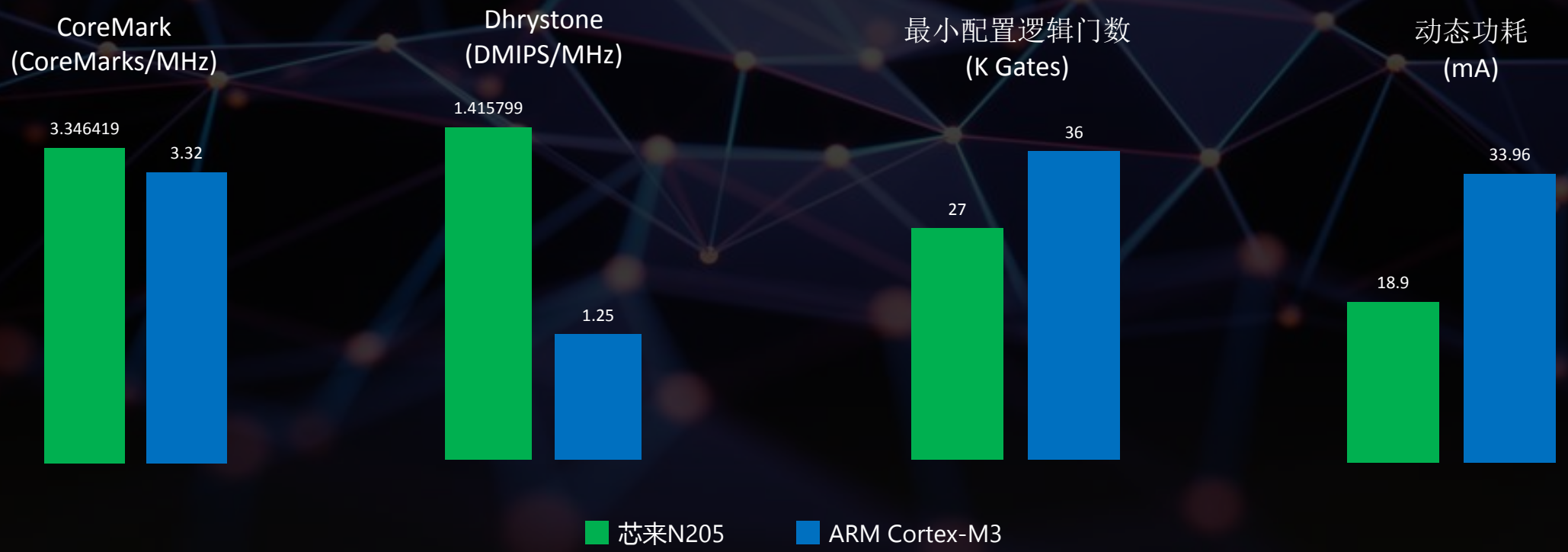
标准JTAG和两线调试接口

高实时性中断机制

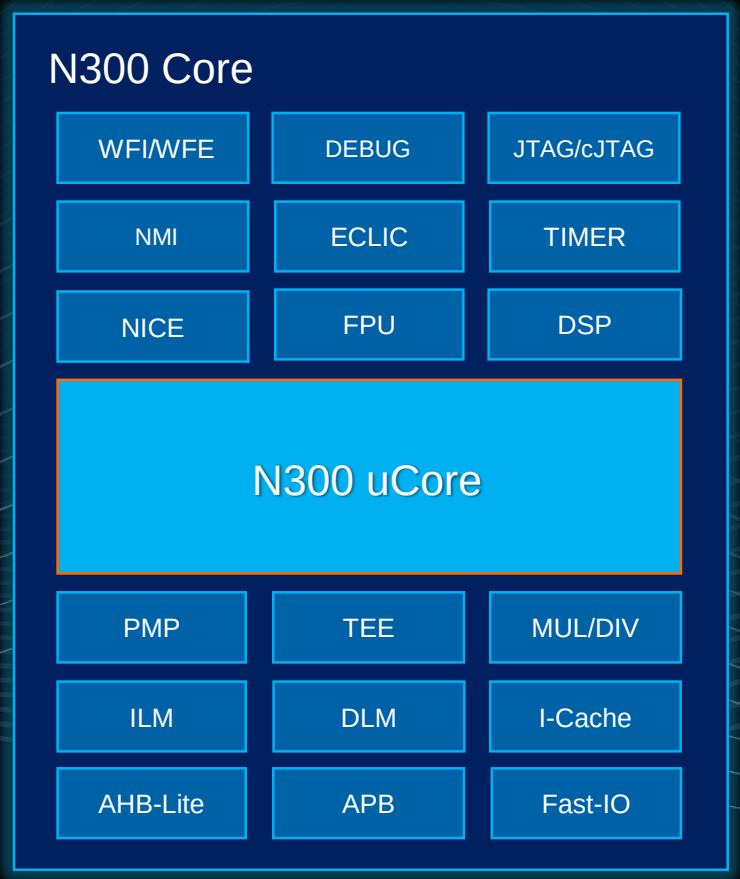
成熟的开发调试环境

N200系列超低功耗RISC-V处理器

芯来200系列通过把低功耗设计思想贯穿整个处理器设计，以及高效的取指单元以及中断处理机制，例如N205达到M3级别的性能，M0+级别的功耗。



N300系列低功耗处理器



N300系列32位超低功耗RISC-V处理器面向机制能效比且需要DSP，FPU特性的场景而设计，非常适合对标ARM Cortex-M4/M4F/M33内核，应用于IoT和工业控制等场景。

- 追求极致能效比
- RV32I/E/M/A/C/F/D/P
- 三级变长流水设计
- 支持指令缓存I-Cache
- PMP和TEE等多种安全机制
- 单双精度浮点和DSP单元
- NICE指令扩展机制
- AHB-Lite和APB 32位总线 Fast-IO, ILM, DLM 32位接口
- RISC-V调试标准
- 标准JTAG和两线调试接口
- 高实时性中断机制
- 成熟的开发调试环境

N600系列高性能处理器

N600系列32位RISC-V处理器面向实时控制或高性能嵌入式应用场景，非常适合对标ARM Cortex-M7，R4, R5，R7等内核，应用于AIoT边缘计算，存储或其他实时控制应用。

- 高性能 高实时性
- RV32I/M/A/ C/F/D/P
- 六级变长 流水设计
- 支持指令缓存 和数据缓存
- PMP和TEE等 多种安全机制
- 单双精度浮 点和DSP单元
- NICE指令 扩展机制
- 32位AXI总线和 ILM, DLM 接口
- RISC-V调 试标准
- 标准JTAG 调试接口
- 高实时性中 断机制
- 成熟的开发 调试环境
- 双核锁步 (Lock-Step)
- ECC或Parity保 护

芯来科技 NUCLEI

NX600系列64位高性能处理器

NX600系列64位RISC-V处理器面向实时控制或高性能嵌入式应用场景，非常适合对标ARM Cortex-M7，R4, R5，R7等内核，应用于AIoT边缘计算，存储或其他实时控制应用。

- 高性能 高实时性
- RV64I/M/A/ C/F/D/P
- 六级变长 流水设计
- 支持指令缓存 和数据缓存
- PMP和TEE等 多种安全机制
- 单双精度浮 点和DSP单元
- NICE指令 扩展机制
- 64位AXI总线 和ILM, DLM 接口
- RISC-V调 试标准
- 标准JTAG 调试接口
- 高实时性中 断机制
- 成熟的开发 调试环境
- 双核锁步 (Lock-Step)
- ECC或Parity保 护

芯来科技 NUCLEI

芯来科技
NUCLEI

期待与您的合作