
IP Reuse
SoC Design
IP与SoC设计
TLP
HBM
一种针对高压双向
ESD防护的栅控二极管
触发SCR的设计
MM
LATCH-UP
www.ip-soc.com
免费订阅
关注我们

CEC 中国电子 | Empyrean 华大九天

# 一站式EDA及相关服务提供商

## 极具规模与实力的EDA龙头企业

## 为中国集成电路产业健全发展保驾护航


**电子设计自动化（EDA）软件—工业软件皇冠上的明珠**

## 关于我们

**服务全球近400家客户**

北京华大九天软件有限公司（简称“华大九天”）成立于2009年，致力于面向泛半导体行业提供一站式EDA及相关服务，是极具规模和实力的EDA龙头企业。

在EDA方面，华大九天可提供模拟/数模混合IC设计全流程解决方案、数字SoC IC设计与优化解决方案、晶圆制造专用EDA工具和平板显示设计（FPD）全流程解决方案，拥有多项全球独创的领先技术。

围绕EDA提供的相关服务包括设计服务及晶圆制造工程服务，其中晶圆制造工程服务包括PDK开发、模型提取以及良率提升大数据分析等。

华大九天总部位于北京，在南京、成都和深圳设有全资子公司，并在上海、日本、韩国、东南亚等地设有分支机构。

**北京华大九天软件有限公司**

北京·南京·成都·上海·深圳

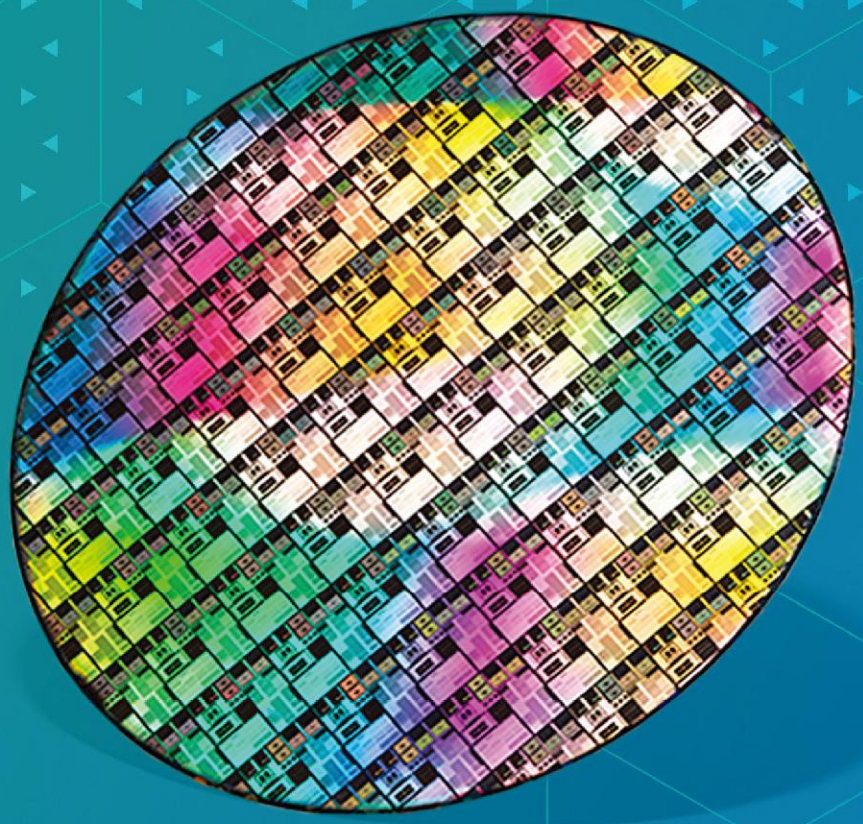
info@empyrean.com.cn

www.empyrean.com.cn

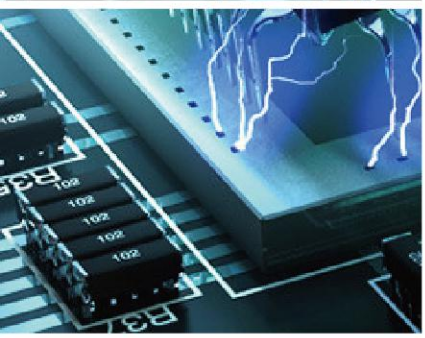
cadence®

# Advanced-Node Solutions

Complete, integrated, and silicon-proven design flows at 7nm and below for custom/analog, digital, and mixed-signal SoCs



www.cadence.com



**关于《IP与SoC设计》**

《IP与SoC设计》专注于IP和SoC设计技术，基于当前集成电路产业发展的趋势，依托无锡“芯火”平台，全面报道全球IP与SoC设计技术的发展和国内外应用经验，整合全球IP与SoC资源和技术资讯，扩展中国读者的全球视野，搭建一个IP与SoC的资讯交流、产业促进的平台，为中国IC设计行业和企业提供IP与SoC专业知识，以及相关信息支持和服务。

公司网址：www.ip-soc.com

# 目录 1
# DIRECTORY

## 编辑手记
EDITOR’S NOTE



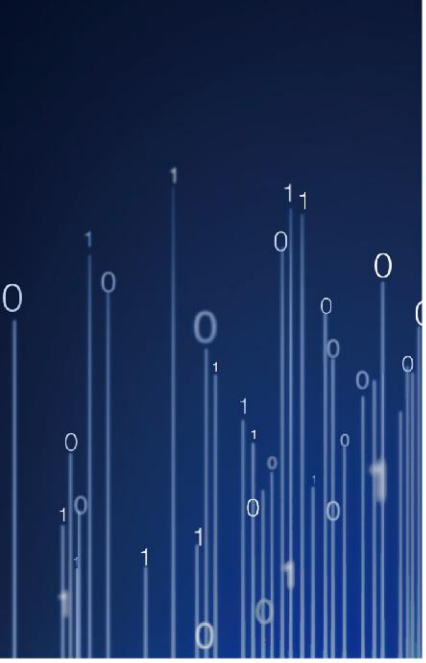
## 封面专题
COVER FEATURE



## 技术应用
TECHNICAL APPLICATION



## 产业观点
INDUSTRY VIEW



《IP与SoC设计》
—— IP Reuse and SoC Design ——

出　　版：无锡国家“芯火”双创基地（平台）
出 版 人：曹华锋
地　　址：无锡新吴区菱湖大道111号无锡软件园天鹅座C座
技术编辑：房龙涛
执行编辑：朱慧
美术编辑：何宇
发 行 部：（0510）85386687-8035
杂志网站：www.ip-soc.com
联系邮箱：zhuh@jsic-tech.com
Service@jsic-tech.com

# 目录 2
# DIRECTORY

## 需求与解决方案
DEMAND & SOLUTION



## 新品发布
NEW PRODUCTS



## 产品特写
PRODUCT FEATURES



## 广告索引 ADVERTISEMENT INDEX

## 《IP与SoC设计》索阅卡

INNOSILICON
芯 动 科 技

芯动，您的芯片定制专家

# 高端云芯片 · IP设计
# 一站式领军

- 支持芯片自主可控国产化
- 高效赋能高端国产生态链

## 先进IP及定制服务

全国产自主可控 | 高集成度低成本 | IP种类繁多全覆盖 | 中国市场份额领先

## 智能芯片定制服务

从需求到定制ASIC | 从FPGA到定制ASIC | IP+后端设计服务打包 | 各形式的联合设计

| 7nm | 50亿+ | 100% | 200+ |
| --- | --- | --- | --- |
| 量产最高工艺节点 | 高端SoC芯片量产 | 量产成功率 | 合作企业 |


**芯动科技有限公司**

珠海 · 武汉 · 苏州 · 西安 · 宁波 · 北京 · 上海 · 深圳 · 硅谷 · 多伦多

邮箱：Sales@innosilicon.com.cn　　官网：http://www.innosilicon.com.cn/


微信公众号


# 中国半导体IP龙头登陆科创板

8 月 18 日，国内自主半导体 IP 龙头芯原股份正式登陆科创板，开盘竞价大涨 289.31%，报 150 元 / 股。

招股书显示，芯原股份是一家依托自主半导体 IP，为客户提供平台化、全方位、一站式芯片定制服务和半导体 IP 授权服务的企业。主要经营模式为芯片设计平台即服务（Silicon Platform as a Service，SiPaaS）模式（以下简称“SiPaaS 模式”）。根据 IPnest 统计，芯原是 2019 年中国大陆排名第一、全球排名第七的半导体 IP 授权服务提供商。此外，在先进工艺节点方面，芯原已拥有 14nm/10nm/7nmFinFET 和 28nm/22nmFD-SOI 制程芯片的成功设计流片经验，并已开始进行新一代 5nm FinFET 和 FD-SOI 制程芯片的设计研发。

芯原股份在全球半导体 IP 市场的份额占比尚不足 2%，同时其所积累的 IP 多是依靠并购而来（主流 IP 大公司的通用方法），虽然芯原股份暂时无法提供包括 CPU IP 等在内的关键 IP 单元，但多年积累下，目前已能提供包括 GPU IP、NPU IP、VPU IP、DSP IP 和 ISP IP 的 5 大处理器 IP 及 1400 多个数模混合 IP 和射频 IP，GPU IP（含 ISP）和 DSP IP 市场占有率均排名全球前三，客户包括全球众多顶级厂商如博通、NXP、亚马逊等。

从市场情况来看，目前半导体 IP 市场是个赢家通吃的赛道，呈现出高度集中趋势，美国和英国企业处于主导地位。2019 年全球其中前十大供应商合计占比 78.1%，7 家为美国和英国企业。实际上国内之前对 IP 的讨论一直不多，讨论最多的就是芯片国产化的宽泛概念，然而在去年 ARM 断供华为的消息爆出后，IP 才受到更大关注，加剧了 IP 国产化的急迫性。在中兴、华为事件之后，半导体国产化声浪高涌，IP 的重要性也愈发凸显。

目前我们绝大部分的芯片都建立在国外公司的 IP 授权或架构授权基础上。一方面国外企业具有的优势地位使得授权费用较高，增加了我国芯片设计企业的设计成本；另一方面半导体核心技术和知识产权如果受制于人对于我国的国产芯片的自主和安全而言是一个潜在的风险，因此推进 IP 和芯片底层架构国产化是市场的选择也是国家战略的需求。

半导体 IP 因技术密集度高、知识产权集中、商业价值昂贵，处于产业链顶端，因此研发投入巨大，周期较长。从前几大 IP 公司已有的经验来看，技术研发本身是决定实力的关键因素之一，在国产 IP 的发展中，同时还要着重建立生态和平台的能力。令人欣慰的是，目前国内的 IP 公司也在蓬勃发展，涉及门类广泛。主要包括处理器、接口、存储、模拟混合、输入输出等。代表企业平头哥、芯原微、芯动科技、灿芯半导体、成都纳能、华大九天、四川和芯微、锐成芯微、芯来科技等。部分企业除了提供 IP 以外，还提供一站式设计服务业务，通过配合自有 IP 资源，较大的增强了市场竞争力。

国内半导体 IP 目前整体还处于初级阶段，IP 公司整体规模较小，在高端领域缺乏话语权，且同质化比较严重，除了加大投入以外，各地政策也需要向国产 IP 公司倾斜。比如，对设计公司购买国产 IP 进行一些额外的优惠补贴政策。国内设计公司也需要给国产 IP 公司一定的机会和信任，因为 IP 生态的搭建需要时间，离不开客户的积累。另外国内代工厂也需要释放一部分资源给到初创 IP 公司，相互促进建设完善的国产 IP 生态圈。

“好风凭借力，送我上青云”，对于国内半导体 IP 公司来说，这是个好时代！

PerfectVIPs

# Accelerate your **Product Development Cycle**

## Industries we cater to...

- Storage + Data Centre
- Wireless + Mobile
- AI + Machine Learning
- Aerospace + Defence
- Networking
- Automotive
- Consumer
- IOT + Cloud

## Spec to Silicon to Embedded Software Services

6 DESIGN CENTRES WORLDWIDE

## IP / ASIC / SoC Services

- IP/ASIC/Subsystems/SoC Development
- Architecture & Digital Design
- Synthesis, Timing & STA
- Functional Verification & GLS
- Emulation & Post SI Validation
- Physical Design
- Physical Verification & Silicon Sign Off
- DFT
- Analog & Mixed Signal Design
- Circuit Design
- Analog Layout

## Embedded & Firmware Services

- Integrated Product Design and Maintenance
- Embedded Platform Software and Migration
- Systems Integration
- Embedded OS ,BSP, Device Drivers and Firmware Development
- ML, AI , IOT and IIOT
- RISC V and LLVM based Compiler Customization
- Applications, UI / UX Development, Cloud and DevOps
- Boot and Secure Boot Software
- Hardware Bring-Up , Validation and Certifications

www.perfectvips.com

# 一种针对高压双向ESD防护的栅控二极管触发SCR的设计

作者：梁海莲，许强，朱玲，顾晓峰等

## 摘要

本文提出了一种新型高压双向 ESD 防护设计方案，体现为一种具有电压小回滞特性的栅控二极管触发 SCR（GDTSCR）结构的 ESD 防护器件。与传统 MOS 触发 SCR（MTSCR）结构的 ESD 防护器件相比，在小至 1600um² 的芯片面积上，GDTSCR 可实现 15 V 的高维持电压与 17V 低触发电压，高达 6000 V 的 ESD 鲁棒性。这是因为 GDTSCR 器件内部采用了两个栅控二极管和一个寄生 NPN 型三极管的特殊设计。内嵌的栅控二极管和寄生的 NPN 型三极管有效地抑制了传统 SCR 内部的正反馈作用。GDTSCR 的卓越 ESD 防护性能特别适用于高压 IC 的 ESD 防护，GDTSCR 可为双向高压 ESD 防护需求提供有效抗闩锁技术解决方案。

关键词：静电放电（ESD），栅控二极管，可控硅（SCR），双向 ESD 防护。

## 引言

因为 SCR 具有强单位面积鲁棒性，它已成为当前 IC 应用领域 ESD 防护需求中广泛关注的 ESD 防护器件。针对低压与高压 IC 的不同 ESD 防护需求，各学术研究团队提出了各种改进型 SCR 结构。在低压 IC 的 ESD 防护中，传统二极管和堆叠二极管触发 SCR 因具有触发电压（Vt1）低，箝位能力好和寄生电容小等优势，被广泛应用于射频 IC 的 ESD 防护中。又因为二极管的串接或叉指结构可能具有不可控寄生效应，比如达林顿效应，寄生三极管等副效应，所以多个堆叠二极管触发的 SCR 不适用于快速开启的低压 IC 与高压触发开启的高压 IC 的 ESD 防护。

普通工作于反向击穿的高压 SCR 结构的 ESD 防护器件通常呈现大电压回滞现象，在 IC 上电工作模式中存在较大闩锁风险。通常借用 MOS 辅助触发 SCR（MTSCR）技术，有助减小 Vt1 和电压回滞幅度。但是，MTSCR 器件的维持电压（Vh）仍然较小，还不适用于高压 IC 的 ESD 防护。最近，一种基于 20nm FD-SOI 工艺的内嵌栅控二极管的 NMOS 器件，呈现了良好的箝位电压和 ESD 鲁棒性。然而，该器件较高的工艺制造成本和较低的 Vh，仍制约了其大规模应用。

近年来，虽然其他一些改进结构的 SCR 器件有效地提高了 Vh 和减小电压回滞幅度，但是，这些器件通过呈现较大的器件面积或复杂 SCR 结构设计，单位面积的 ESD 鲁棒性仍然不足，以及还具有潜在达林顿效应等不良因素。本文提出了一种针对高压双向 ESD 防护结构，设计的栅控二极管触发 SCR(GDTSCR)具有结构简单与新颖性特点，还具有强单位面积 ESD 鲁棒性。该器件基于传统 CMOS 工艺，无需额外的掩膜设计成本。本文提出的 GDTSCR 可满足 15-20V 高箝位电压需求，并拥有高达 6000V 的 HBM ESD 鲁棒性。

## GDTSCR 的设计和机制分析

基于相同硅基 0.18um CMOS 和特征尺寸掩膜版制备的 MTSCR 和 GDTSCR 结构剖面如图 1 所示。由于 MTSCR 和 GDTSCR 具有相似的内嵌 SCR 结构，选用单向 ESD 防护的 MTSCR 作为 GDTSCR 的对比器件，有助于研究优化 GDTSCR 的 Vh 和 ESD 鲁棒性的物理机制。MTSCR 的多晶硅栅与器件的电学阴极端相连，GDTSCR 的多晶硅栅与位于 P 阱中的 P+ 注入区相连，它既不连接器件的电学阳极端也不连接器件的电学阴极端，可有效避免器件在高压作用下发生栅氧击穿现象。

与 MTSCR 相比，GDTSCR 通过利用劈栅和增加阱方法，将多晶硅栅分割成左右两部分，并在 P 阱中 MOS 的漏极和源极之间插入一个高掺杂 P+ 注入区，使 GDTSCR 内部形成两个栅控二极管和一个额外的寄生 NPN 三极管。这不仅有助于减小 Vt1，还同时可增加 Vh 和失效电流（It2）。此外，在 P 阱右侧增设一 N 阱，其中设置与 P 阱左侧 N 阱相同尺寸的高掺杂 P+ 和 N+ 注入区，可实现双向高压 ESD 防护。与两个 MTSCR 反向串接相连的双向 ESD 防护相比，GDTSCR 的单位面积 ESD 防护效率更高。

得益于 GDTSCR 的结构对称特性，无论在 GDTSCR 的阴阳极之间施加正向或反向 ESD 脉冲，GDTSCR 内部的等效电路相同。如图 2 所示，随着 ESD 脉冲大小不同，器件内部电流路径不同。图中三种不同颜色：白、黄和紫色电路路径分别代表 ESD 应力不断增加下器件内部的有效电流路径。

当 ESD 脉冲较小时，GDTSCR 内部在电场作用下，产生的漂移电流流经反向栅控管 D1、D2、大电阻 RN 和 P 阱电阻 Rp。随着漂移电流 Idrift 的增加，栅电位 VG 不断提高，VG≈Rt×Idrift。增大的 VG 又有利于促进增强栅耦合效应，继续促进 Idrift 持续增大。当 VG 和 Idrift 增大至一定值时，栅控二极管 D2 开启。此时由白色标示电子元件 D1 和 D2 构成的第一条 ESD 触发电流路径形成。

当 ESD 脉冲应力继续增加时，晶体管 T3 工作在放大状态。在 SCR 的正反馈作用下，T1 的基极电流随 T3 集电极电流增加而增加。当左侧的 N 阱电阻 RN 的压降增大至 0.7V 时，晶体管将会导通。此时由黄色标示电子元件 T1 和 T3 构成的第二条 ESD 触发电流路径形成。

同时，当触发电流达到一定阈值时，晶体管 T2 将会导通。此时由晶体管 T1 和 T2 构建的 SCR 电流路径将会导通，如图中紫色电子元件标示，第三条 ESD 触发电流路径形成。因此，与传统 MTSCR 相比，GDTSCR 具有多条 ESD 触发电流路径，有助于提高 ESD 防

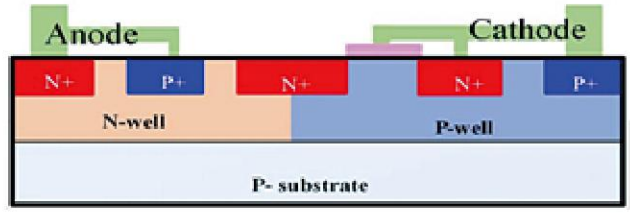



FIG.1 CROSS SECTIONS OF THE MTSCR

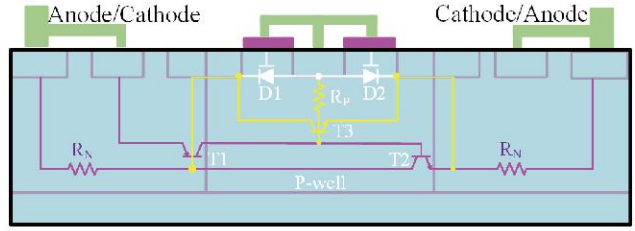



FIG.2. THE INTERNAL EQUIVALENT CIRCUIT OF THE GDTSCR

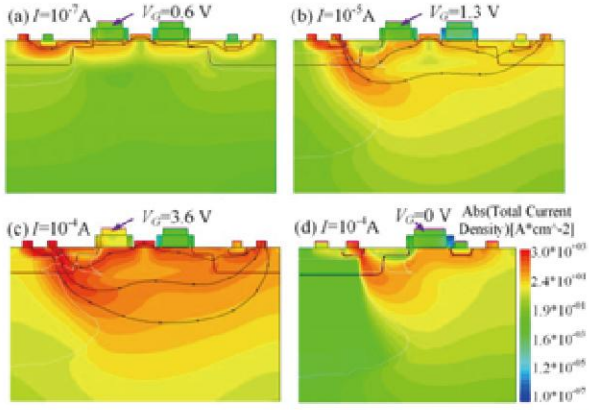



Fig. 3. The simulated internal current path of the GDTSCR under (a) $I = 10^{-7}$ A, (b) $I = 10^{-5}$ A, (c) $I = 10^{-4}$ A and the MTSCR under (d) $I = 10^{-4}$ A.

护性能。

上述 GDTSCR 器件内部的工作机制利用 TCAD 仿真工具进行验证与分析。GDTSCR 器件不同 ESD 应力作用下，内部开启状态在 Sentaurus 仿真结果如图 3 所示。图中黑色曲线为器件在 ESD 应力作用下自动生成的电流线，图 3（a）-（c）中的电流线与图 2 中展示的三条 ESD 触发电流路径一致。GDTSCR 器件内部电流仿真验证器件在不同 ESD 应力作用下存在多条电流导通路径，可增强器件的 ESD 鲁棒性。同时，晶体管 T1 是分别由 T1,T3 和 T1,T2 分别构建的两条 SCR 路径共用电子元件。因此，GDTSCR 内部的 SCR 正反馈受到抑制，可提高 GDTSCR 的 Vh。

同时，MTSCR 的 Sentaurus 仿真结果如图 3(d) 所示。与 GDTSCR 相比，MTSCR 内部因具有相同的位于 N+ 注入区和 P 阱表面的反偏 PN 结，MTSCR 触发特性相似。然而，MTSCR 在开启后的内部电流密度远小于相同 ESD 应力下的 GDTSCR，并且，MTSCR 内部只有一条较短的 SCR 电流路径泄放 ESD 电流。因此，上述器件的 TCAD 仿真结果进一步证实：设计的栅控二极管和 P 阱中嵌入的 P+ 注入区有助于提高 Vh 和 It2。此外，当 ESD 电流从 10-7 增加到 10-4A，GDTSCR 的 VG 从 0.6V 提高到 3.6V，此时 MTSCR 的多晶硅栅的 VG 仍然为 0。栅上电压 VG 的改变与上节提及的关于 VG 有助于开启 GDTSCR 的分析高度一致。

## 结果与讨论

### A.GDTSCR 的电学特性分析

器件宽度相同的 MTSCR 和 GDTSCR 在传输线脉冲（TLP）系统中测试并获得的电学特性如图 4 所示。

首先，GDTSCR 和 MTSCR 具有相近的最小 It2。尽管 GDTSCR 的开启电压（Von）被箝位在 12V 和 24V 之间，导通电阻 Ron 小于 3Ω。最小 It2 定义为 Ron 陡增时最小的 It2，且此时漏电流保持在 nA 级。GDTSCR 中的多条 ESD 电流泄放路径，促使 GDTSCR 足以通过 6000V HBM 测试，其 HBM 等级可由公式 It2×1500 V 估算。

第二，与 MTSCR 相比，GDTSCR 的 Vh 从 4.6V 提高到 13.6V，因为 GDTSCR 内部 SCR 的正反馈作用受到抑制，流经 SCR 导通路径的电流被晶体管 T2，T3 和栅控二极管 D1 和 D2 分流。

第三，GDTSCR 的 Vt1 略大于 MTSCR，如图 4 中的内嵌 I-V 插图所示，其对应黄色环圈出区域。GDTSCR 和 MTSCR 除具有位于反向栅控二极管 D1 处相同的触发机制外，GDTSCR 的 Vt1

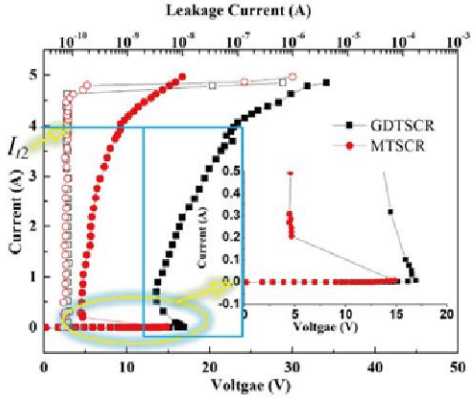



Fig. 4. TLP I-V characteristics of the experimental devices.

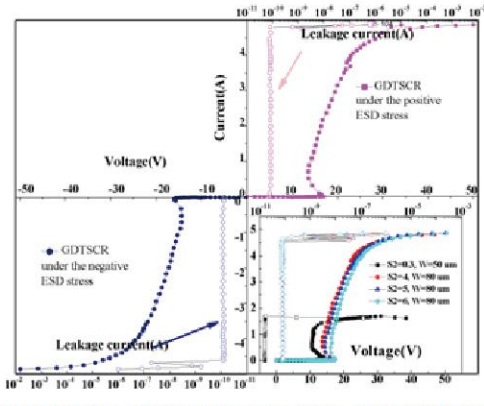



Fig. 5. Dual-direction electrical characteristics of the GDTSCR.

还由二极管的栅控场效应决定。在 GDTSCR 和 MTSCR 开启之前，以及相同 ESD 应力下，由于 Rp 的分压作用，导致 GDTSCR 中反向 D1 上的电势小于 MTSCR，如图 2 所示。从而促使 GDTSCR 的 Vt1 可能会远大于 MTSCR。反而言之，Rp 上的压降又有助于抬高 VG，增强栅耦合效应，促使 Idrift 增加，从而减小 Vt1。相比 MTSCR，GDTSCR 的 Vt1 从 14.9V 略微增加到 16.5V。

最后，GDTSCR 的 Von 箝位在 13.6V 到 23.4V 之间，如浅蓝色方框标示的工作区域。GDTSCR 的 Von 足以安全保护工作电压为 12V 的电路 I/O 口，并呈现出 6000V 的 HBM ESD 鲁棒性。此外，GDTSCR 还拥有良好对称的器件结构和电学特性，分别如图 1 和 5 所示。紫色菱形和深蓝圆形标记的 GDTSCR 的 TLP I-V 曲线如图 5 所示，GDTSCR 在正向和反向 ESD 应力下，呈现出几乎完全相同的电学特性。

最后，GDTSCR 的品质因数 FOM 在单向 ESD 防护中是 MTSCR 的两倍，若在双向 ESD 防护中，几乎是 MTSCR 的四倍。品质因数 FOM 可通过公式 FOM=(Vh×It2)/(Vt1×s) 计算，其中 s 为 ESD 保护器件的整体硅片面积。FOM 适合综合地评估器件的高压 ESD 防护性能。实验器件的 FOM 值以及最近提出的高维持电压 SCR（HVSCR）的 FOM 值如表 1 所示。

与 MTSCR 和最好的 HVSCR 相比，GDTSCR 的 FOM 最大，且非常接近工业硅片单位面积电流密度的理想值。

另外，还利用变温探针台系统与半导体参数仪测试了 GDTSCR 的击穿电压（BV）值，如表 2 所示。结果表明：GDTSCR 的 BV 随着温度的提高，没有明显的变化，展现出良好的温度稳定性。通常器件的 BV 和 Vt1 可分别由 DC 和 TLP I-V tracer 进行测试，它们均随温度变化呈正性相关变化。

TABLE I
ESD CHARACTERISTICS OF THE EXPERIMENTAL DEVICES

| Devices | $V_{t1}$ (V) | $V_h$ (V) | $I_{t2}$ (A) | $S$ ($\mu m^2$) | $FOM$ ($mA/\mu m^2$) |
|---|---|---|---|---|---|
| MTSCR | 14.9 | 4.6 | 3.9 | 1200 | 1.0 |
| The best HVSCR[11] | 34 | 16.9 | 8.84 | 9313 | 0.47 |
| GDTSCR | 16.5 | 13.6 | 3.8 | 1600 | 2.0 |

TABLE II
THE *BV* OF THE GDTSCR UNDER DIFFERENT TEMPERATURES

| Temperature (℃) | 25 | 50 | 75 | 100 | 125 |
|---|---|---|---|---|---|
| *BV* (V) | 15.8 | 15.2 | 15.2 | 15.2 | 15 |

### B.GDTSCR 的电学特性优化

GDTSCR 的电学特性还在两种不同的制造工艺上进行了多次验证。除了上文提及的 W=80um 的一批器件，还有一批 W=50um 的器件使用 0.25um BCD 硅基工艺进行了制备测试。通过选用不同工艺和关键尺寸的实验样品，确认并优化 GDTSCR 的电学特性。两批次的 GDTSCR 均表现为相似的小电压回滞特性，随着 W 的增加，ESD 鲁棒性得到了增强。随着器件长度的增加，导通电阻也增加。

同时，同一批次但关键尺寸不同的 GDTSCR，关键尺寸如图 1 中的 S1，S2 和 L，GDTSCR 的电学特性呈相似变化趋势。随着 S1，S2 和 L 的增加，GDTSCR 的 Vh 增加，It2 略微降低。当关键尺寸 S2 从 0.3 增加到 0.6um 并且 W 从 50 增加到 80um 时，两种工艺下制造的 GDTSCR 随着 W，S1，S2 和 L 的变化，其 I-V 曲线如图 5 右下角所示。

## 结论

本文提出了一种简单新型的 GDTSCR 器件，不仅具有完全对称的物理结构，还具有良好的双向 ESD 防护性能。栅控二极管和 P+ 注入区用于提高 ESD 特性，如 Vh 和 It2。通过 TCAD 仿真进一步验证了器件高 Vh 和强 ESD 鲁棒性的内部机制。实验结果证明：GDTSCR 具有电压回滞小的特性，在 Vt1 更低，Vh 更高的同时提高了品质因数 FOM。与传统的 MTSCR 以及一些其他使用硅基工艺制造的基于 SCR 的高 Vh 解决方案相比，本文提出的 GDTSCR 器件为高压 ESD 防护提供了更有吸引力、更有效的 ESD 防护方案，例如工作电压高且箝位电压范围小的汽车电子领域。

# IoT固件压缩-更低的能耗和更快的启动

Nikos Zervas，CAST，Inc

物联网“ IoT ”一词已经爆炸性地涵盖了各种不同的应用和不同要求的设备。然而大多数观察者会认同低能耗是物联网的关键因素，因为许多此类设备必须依靠电池运行或从环境中获取能量。

看看物联网设备实际上是如何使用能源的，显然大多数为：

1. 大部分时间处于闲置状态
2. 周期性地唤醒或响应事件，
3. 进行一些数据处理，
4. 传输结果
5. 返回继续休眠。

在第 2 步中，启动或唤醒可能会消耗大量能量，而在此处节省则可以减少总体能量预算。本文我们就来看看这个问题。

## 通过数据压缩节省能源

具体来说，在这里我们将展示 GZIP 数据压缩如何降低使用代码映射（物联网设备中使用的常见技术）的嵌入式系统中的能耗。

基本理念很简单：对先前压缩过的固件进行即时解压，可以减少数据加载，并在引导或唤醒过程中最大程度地减少对长期存储的访问次数，从而降低这一关键操作阶段的能耗（和延迟）。

可能节省的能量和开机时间与数据压缩级别成正比，而压缩级别又取决于压缩算法和代码本身。我们将在此探讨的实际案例表明，使用市售 IP 核进行硬件 Deflate/GUNZIP 解压、代码规模（以及因此产生的功耗和启动时间）可减少多达 50%。

此外，我们将看到，使用该方法所节省的成本远远超过了在系统中构建正确的解压内核所使用的额外资源。

## 代码映射与芯片内执行

低功耗嵌入式系统处于睡眠模式时，通常会将其应用程序代码（在某些情况下还存储应用程序数据）存储在非易失性内存（NVM）设备中，例如 Flash，EPROM 或 OTP。

当此类系统被唤醒执行其任务时，它们通过以下两种方法之一运行应用程序代码：

- 直接从 NVM 提取并执行代码，称为芯片内执行 XIP（eXecute In Place）
- 首先将代码复制到称为映射存储器的片上 SRAM 单元，然后从那里执行。

哪种方法最好取决于 NVM 内存的访问速度和访问能耗。通常，NVM 存储器要比片上 SRAM 慢得多，并且从 NVM 存储器读取数据的能耗成本要比从片上 SRAM 读取相同的数据高得多（尤其是当数据以随机顺序访问时）。

考虑到系统的活动模式，最好使用映射内存，但当我们回想起 IoT 设备通常在其整个生命周期中都处于睡眠状态时，情况就会发生变化。不幸的是，大型片上 SRAM 会遭受泄漏电流的影响，因

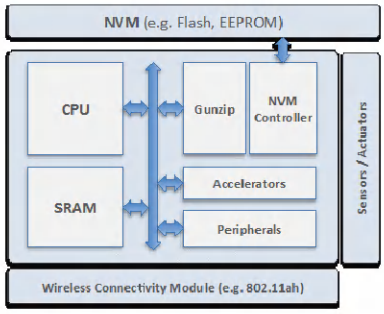



Figure 1: System architecture for Code Shadowing with Decompression.

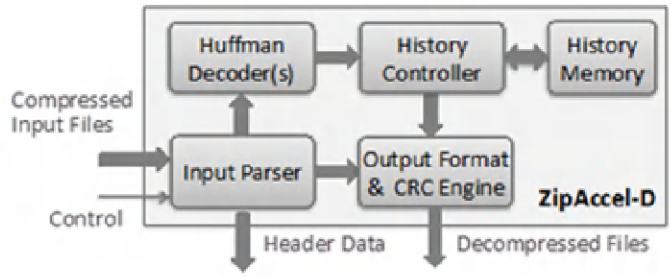



Figure 2: Hardware lossless data decompression engine; Huffman decoding type and History size are parameterized

此即使处于睡眠模式也要消耗功率，而大多数 NVM 则不会。

因此，在映射 SRAM 可以保持相对较小的情况下，或者严格的实时性要求使得 XIP 的缓慢访问时间无法接受的情况下，设计者往往选择代码映射。

## 通过快速数据压缩实现低功耗代码映射

我们可以通过减小存储在 NVM 中的应用代码的大小来解决这两个问题——并将设计决策引向节能的代码映射方法。

使用 GZIP 等无损算法压缩代码可以实现这一点，但意味着代码必须在执行前进行解压。图 1 展示了一个实现这一功能的物联网系统架构示例。在这里，NVM 控制器通过解压引擎连接到 SoC 总线（并从那里连接到片上 SRAM），比如 CAST 提供的 GUNZIP IP 核。

存储压缩代码意味着需要能耗更低的 NVM 访问来唤醒系统，但现在我们增加了解压的额外步骤，该步骤有有其自身的延迟和能耗。这是否是一个可行的方案取决于：

A. 我们能把程序代码的规模减少多少，也就是可实现的压缩率是多少

B. 当我们调整压缩算法以达到一个合理的压缩比时，对解压缩硬件的硅面积、功耗和延迟的要求是什么？

接下来让我们通过实例系统的数据来探究这些因素，看看使用压缩的代码映射是否真的能实现节能。

## 实例系统：真正节省了多少能量？

让我们考虑三个物联网相关的系统：

• 在我们的第一个示例中，R8051XC2 8051 [2] 微控制器运行 Cygnal FreeRTOS [3]。

• 在我们的第二个例子中，BA22-DE [4] 处理器运行一个由 FreeRTOS 管理的多线程的传感器控制应用。

• 在我们的第三个示例中，Cortex-M3 处理器 [5] 正在运行 InterNiche Technologies 的嵌入式 TCP/IP 和 HTTP 堆栈演示 [6]。

在所有案例中，当从低功耗串行 Flash NVM 存储器中读取固件时，我们都使用 ZipAccel-D GUNZIP IP 内核 [1] 进行解压缩固件。

节能效果取决于压缩水平，而压缩水平又取决于代码本身的可压缩性（指令集架构和应用程序的函数）和所选择的 GZIP 参数。对压缩影响最大的 GZIP 参数是 Huffman 引对于我们的应用程序，未压缩的代码大小在 8051 系统中为 25.5 Kbytes，在 BA2 系统中为 161 Kbytes，在 Cortex-M3 系统中为 985 Kbytes。图 3 显示了示例二进制文件的压缩率，表 1 显示了我们的解压核在不同的 GZIP 参数下的面积和延迟。

为了保持 GZIP 处理延迟和较低的芯片功耗，我们将使用静态 Huffman 和 2048 History。这使我们的压缩代码大约是未压缩代码大小的一半，并且同样减少了代码存储的 NVM 大小以及在启动或唤醒过程中读取代码所需的时间和功耗。表 2 和表 3 总结了这些降低的功耗（假设低功耗串行闪存 NVM 读取电流为 5mA、读取时钟为 50MHZ）。

资源节省平均约为 50%，显然是可观的，但是代价是什么呢？

## 分析压缩开销

以所述方式使用压缩会在两个方面引入开销：时间和能源。

我们在示例系统 [1] 中使用的

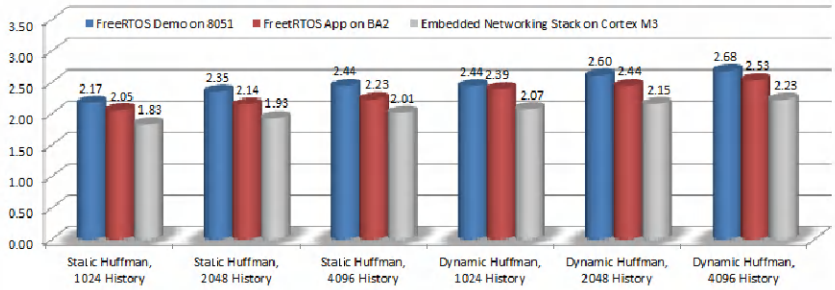



Figure 3: Compression Ratio for the image of InterNiche's demo of embTCP & embHTTP.

ZipAccel-D 解压核引入了 25 到 2000 个时钟周期的延迟（具体取决于使用静态还是动态 Huffman 表进行压缩）。

即使在 2000 个周期的延迟下，并且假设解压缩内核将以 NVM 的 50MHz 时钟运行，解压缩内核所增加的额外延迟仅为 0.04msec。因此，由于压缩而导致的额外延迟实际上可以忽略不计，因为从 NVM 读取代码的时间要高两个数量级。

在功耗方面，当系统处于响应状态时，解压内核的功耗可以忽略不计，但当系统处于空闲状态时，它也会消耗能源。这种空闲状态下功率消耗的意义取决于系统的占空比。

在我们的示例系统中，解压内核的空闲功耗相比系统所能节省的功耗低 3 到 6 个数量级。然而，由于能量是随时间变化的功率，较长的系统睡眠时间使得这种额外的功率消耗值得关注。

由于我们实现了巨大的功率节省，很明显，存储压缩代码并在需要的时候解压，对于大多数物联网系统来说，即使是那些占空比低至每天几毫秒的系统，也能产生净系统能量节省。

| Zip Accel-D配置 | 在k盖茨的区域 | 记忆在k字节 | 时钟周期的延迟 |
|---|---|---|---|
| 静态哈夫曼,1024历史 | 22 | 1.5 | 20 |
| 动态哈夫曼,1024历史 | 38 | 6.0 | ~1,500 |
| 静态哈夫曼,2048年历史 | 22 | 2.5 | 20 |
| 动态哈夫曼,2048年历史 | 38 | 7.0 | ~1,500 |
| 静态哈夫曼,4096历史 | 22 | 4.5 | 20 |
| 动态哈夫曼,4096历史 | 38 | 9.0 | ~1,500 |

表 1：ZipAccel-D 减压核心硅资源和延迟。

| | 代码大小为k字节 | | | 所需的NVM尺寸 | | |
|---|---|---|---|---|---|---|
| | 系统#1（8051） | 系统2（ba2） | 系统#3（手臂） | 系统#1（8051） | 系统2（ba2） | 系统#3（手臂） |
| 未压缩代码 | 25.5 | 161 | 985 | 256千比特 | 2米比特 | 8米比特 |
| 压缩代码 | 10.9 | 76 | 511 | 128千比特 | 1米比特 | 4米比 |
| 节余 | 57.25% | 52.80% | 48.12% | 50.00% | 50.00% | 50.00% |

表 2：使用代码压缩实现 NVM 大小节省。

| | 启动时间在毫秒 | | | 启动电源在mA秒 | | |
|---|---|---|---|---|---|---|
| | 系统#1（8051） | 系统2（ba2） | 系统#3（手臂） | 系统#1（8051） | 系统2（ba2） | 系统#3（手臂） |
| 未压缩代码 | 3.98 | 25 | 154 | 0.02 | 0.13 | 0.77 |
| 压缩代码 | 1.7 | 12 | 80 | 0.01 | 0.06 | 0.40 |
| 节余 | 57.29% | 52.00% | 48.05% | 57.25% | 52.80% | 48.12% |

表 3：使用代码压缩实现启动时间和节能。

## 结论

高效的硬件解压缩引擎（例如可从 CAST 获得的 IP 核）可以对代码进行行内解压缩（因为从 NVM 中读取了代码），而代价是几乎可以忽略不计的额外延迟或能耗。

采用代码映射的 IoT 设备可以通过使用代码压缩获得显著降低的能耗。

压缩后的应用代码需要一个较小的 NVM 设备进行长期存储，系统将压缩后的代码从 NVM 读入片上 SRAM 所消耗的时间和能量也大大减少。

一个高效的硬件解压引擎，如 CAST 提供的 IP 核，可以以极低的代价在线解压代码（当代码从 NVM 中读出时）。

ZipAccel-D GUNZIP/ZLIB/Inflate Data Decompression Core:
https://cast-inc.com/compression/gzip-lossless-data-compression/zipaccel-d/

R8051XC2 High-Performance, Configurable, 8051-Compatible, 8-bit Microcontroller:
https://cast-inc.com/processors/8051s/r8051xc2/

FreeRTOS Cygnal (Silicon Labs) 8051 Port:
http://www.freertos.org/portcygn.html

BA22-DE 32-bit Deeply Embedded Processor:
https://cast-inc.com/processors/32-bit/ba22-de/

ARM® Cortex ®-M3 Processor:
http://www.arm.com/products/processors/cortex-m/cortex-m3.php

InterNiche Technologies embedded TCP/IP stacks demo:
http://www.iniche.com/source-code/networking-stack/nichestack.php

FARADAY

# 智原高速接口IP方案

近三十年ASIC实战经验 | 联芯在地生产 | 系统验证IP

## 网通应用接口

- 28G/16G SerDes PHY
  - 支持xPON应用
  - 符合OIF-CEI、JESD、PCIe Gen1-4和Ethernet等多项主流接口规格
- Ethernet PHY
  - 支持10/100M或10/100/1000M
  - 单端口与多端口PHY，支持电流模式和电压模式

## 显示应用接口

- V-by-One
  - 每条信道速度高达4Gbps，最多支持8条信道
- MIPI D-PHY
  - 支持DSI/CSI-2、TX & RX，每条信道速度高达2.5Gbps
  - 可Combo其他IO：LVDS、sub-LVDS、HiSPi、GPIO
- LVDS
  - 每条信道速度达1.25Gbps
  - 支持扩频时钟与低通道偏移

## SoC接口

- DDR 2/3/4、LPDDR 2/3/4
- USB 3.2/2.0
  - 支持Type-C与PD、OTG与XTAL-Less
  - 业界最小40纳米USB 2.0 OTG PHY

微信

# 先进的电源管理平台-打破效能新记录

苏希尔·姆希拉；皮埃尔·加泽尔；Dolphin Design

## 背景介绍

连接到数据中心的数十亿电池供电的 IoT 设备推动了智能城市，智能家居和智能建筑的出现，将迫使 IC 设计团队追求苛刻的电源目标：在待机模式下的零功耗，在运行模式下以优化的能效实现最大性能。能源效率是一个关键指标，它展示了用最小的能量可以做到的最高性能。

不幸的是，摩尔定律提供了几十年的免费午餐现在已经结束了，缩减到下一个技术节点不再提供所需的能源效率收益。

设计团队现在必须通过部署越来越复杂的电源管理技术来追求收益，以满足新的物联网市场的需求。在先进的物联网中，这一点尤其棘手，因为在先进的物联网中，近端传感器处理必须与射频连接有效结合，同时还要进行先进的电源管理。

半导体公司正在不断创新，通过采用新的工艺节点、先进的 SoC 架构和智能电源管理技术，为其物联网客户提供最先进的解决方案。

微控制器由存储器、处理器和输入 / 输出外围设备组成的单片集成电路。它被安装在自动控制产品和电子设备中，如遥控器、办公机器、家用电器、电动工具、玩具等。在电子设备中使用微控制器可以使其正常工作，并确保平稳的工作状态。

在庞大的微控制器市场中，超低功耗（ULP）微控制器市场目前备受关注。

ULP 微控制器市场预计将从 2019 年的 44 亿美元的估计值增长到 2024 年的 129 亿美元，2019-2024 年期间的年复合增长率为 24.1%（marketsandmarkets 分析）。

ULP 微控制器市场的主要驱动力是：

•越来越多的低功耗设备被采用

•消费电子行业对低功耗微控制器的需求不断增加；楼宇和家庭自动化系统的使用越来越多。

•物联网生态系统的需求激增。

事实上，32 位 ULP 微控制器领域预计将在 2019 年至 2024 年期间引领市场。这些微控制器的增长可以归功于一个特点，即功耗和高性能之间的平衡。这满足了受功率限制或低功耗应用的需求，为物联网（IoT）和联网设备寻求节省能量的功能。

具有超低功耗微控制器的模拟设备市场很高，

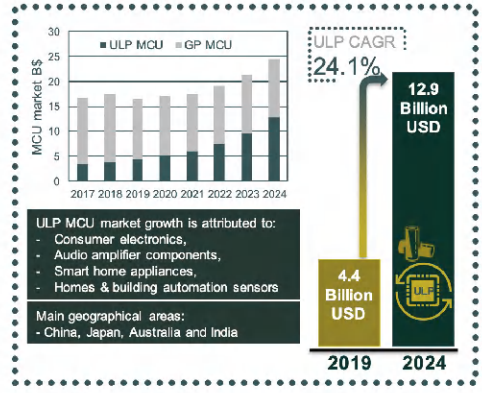



Fig. 1: Ultra-Low Power microcontroller market evolution 2019-2024

因为低功耗器件主要用于获取现实世界的信号，如温度、压力、加速度和速度，这些信号被测量并转换为数字信号。

模拟外设的优点包括高可靠性、降低噪声、低延迟和降低成本。集成模拟外设的应用包括工业仪表解决方案、工业控制器、联网家庭控制台、恒温器、温度传感器、智能仪表、智能电网、血糖仪、心率监测器、植入式设备和物联网设备。

对于所有这些情况，必须积极管理微控制器的功率，以实现超低功耗和合理的高峰值性能。

2018 年组织的一项对 RTL 设计人员的调查显示，虽然多年来已经确定了各种电源管理技术，但对许多人来说，管理这些技术仍然被认为是一个障碍。

从这个角度来看，Dolphin Design 提供一套全面的经过硅验证的 IP 和 SW 解决方案，以透明而高效的方式使用所有这些技术。

## 电源管理技术简短回顾

从设备级别到 SoC 级别都可以考虑电源管理和低功耗技术。都可以通过以下公式来平衡漏电功率、动态功率和面积：

- 动态功率 ~$W.V_{dd}^2.F$
- 漏电功率 ~$(V_{dd}/L).e^{-V_{th}/S}$
- 速度 ~$W/L\ (V_{dd}-V_{th})^2$

### 标准单元库：低功耗 SoC 实现的基础

多驱动（多个 W），多 Vth（低 Vth，常规 Vth，高 Vth）和多长度（标准栅长，较大栅长）标准单元库的设计使 SoC 设计人员能够找到合适的器件。在物理实现和签核 ECO 期间在速度和功率之间进行权衡。

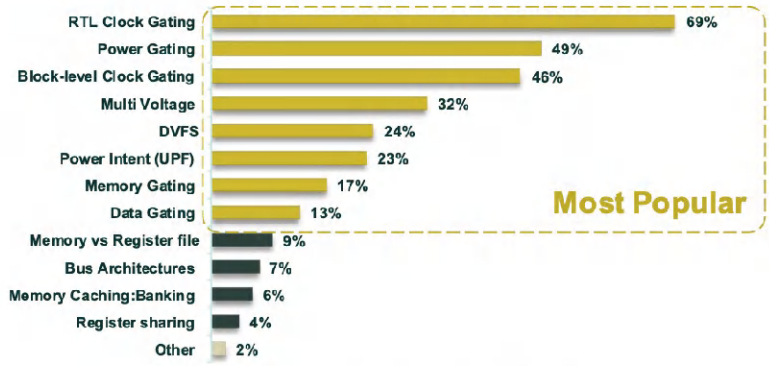



Fig. 2: Usage percentages of known power management techniques (as per Mentor's 2018 survey)

当要在休眠和深度休眠模式下实现最佳功耗时，需要特别注意实现 Always-On 域的逻辑功能的标准单元库，这是 SoC 中唯一在其余部分休眠时保持活跃的部分。使用高 Vth 单元是获得较好结果的方法之一，然而使用厚氧化物晶体管可能是最有力的方法，可以将 AON 逻辑的漏电数字降低几十个，然而，使用厚氧化层晶体管可能是将 AON 逻辑的泄漏电流减少几十倍的最有力的方法。

### 时钟门控：让我们停止时钟

在模块级，时钟门控可能是 IC 设计人员采用的首选降低功耗的技术之一。在时钟树上添加一些逻辑门控，可以通过在不需要时停止时钟（实际上将“ F”设置为 0）来降低动态功耗。

### 电源门控：关闭你不需要的东西

接下来是电源门控，当应用不需要时，允许关闭未使用的电源域，以节省漏电(我们实际上将 ″Vdd ″ 设置为 0)。电源门控一般采用标准的 Power Management Kit (PMK) 来实现，它实现了电网式或环形结构的电源开关。电源开关可以显著降低漏电，然而由此产生的 IR-Drop 约束和涌浪电流约束往往会导致过大的电源开关配置，从而打破睡眠模式的漏电预算。

### DVFS, AVS, Body-Biasing

在 SoC 级别，对超低功耗数字的需求促使设计界定义越来越复杂的功耗状态，每个模块都有自己的电压、频率和功耗目标。第一步是多电压策略，其中包括近阈值电压 (Near Threshold Voltage-NTV)，随后是更复杂的方案，例如动态电压频率调整 (Dynamic voltage and frequency scaling -DVFS) 和自适应电压调节 (Adaptive voltage scaling-AVS)，通过持续调整电源电压，可以对 SoC 性能进行精细控

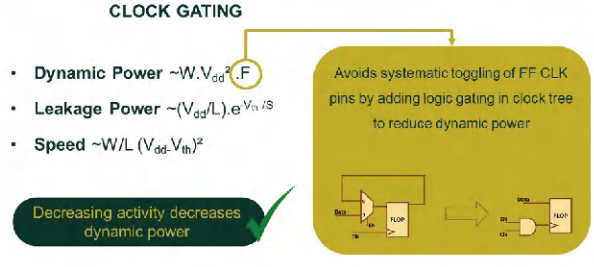



Fig. 3: Clock gating technique

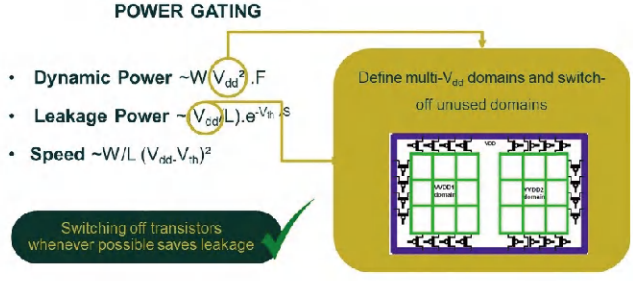



Fig. 4: Power gating technique

制，同时降低设计裕度。

FD-SOI 技术随后引入了一种新方法，通过增加或减少施加在阱上的电压来虚拟地调节晶体管的阈值电压。

自适应体偏压等技术表现出前所未有的功率效率数，特别是在低压下工作时，依靠一个完全自主的子系统，可以动态调整偏压来达到预期的性能。

## PMU：SoC 电源管理的基石

由 DVFS 等技术开发的 SoC 电源模式越来越多，需要一种智能的方法将电源电压和时钟设置为正确的值并使其在芯片中可用，并控制 SoC 的启动和从一种模式过渡到另一种模式。

**这就是电源管理单元（PMU）的作用。**

对于 PMU 能够实现的功能并没有一个标准的定义：一些应用依靠外部电源管理芯片（PMIC）来处理电压调节、电池充电、电源选择和基本的上电顺序，但是需要降低系统成本并采用复杂的电源策略已促使 ASIC 设计团队考虑将电源管理单元（PMU）集成为内置功能。晶圆厂现在依靠先进工艺节点，在单块 SoC 上实现数字、射频和电源管理的集成。

PMU 绝对是电源管理策略的关键。它驱动开机顺序，配置电压调节器以获得给定电源模式下的正确输出电压，并确保上电顺序的正确执行。目前，PMU 有两种实现方式：全定制设计或软件 PMU。

完全定制的 PMU 可以实现超低功耗，尤其是在 Always-On 域采用低漏电逻辑单元实现的情况下，然而它存在着可配置性不足的问题，如果 SoC 架构发生变化或用于产品的衍生品，需要完全重新设计。

基于软件的 PMU 依靠一个嵌入式内核（通常是一个小的 MCU 模块）来控制电源模式的顺序和管理中断。可以使用常规固件更新的方法轻松地现场重新配置它，然而由于需要有一个始终处于运行状态的 MCU（以控制 SoC 运行），因此它与休眠模式下需要超低功耗的休眠应

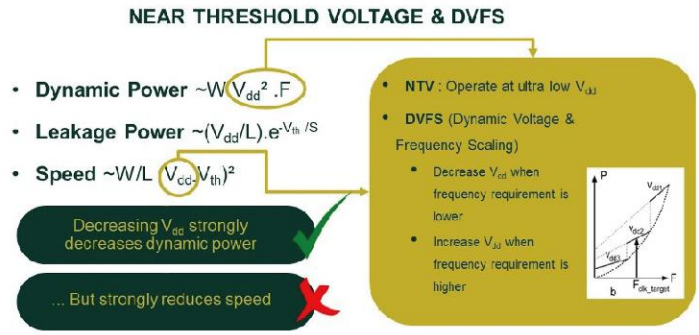



Fig. 5: NTV and DVFS, multi-voltage techniques

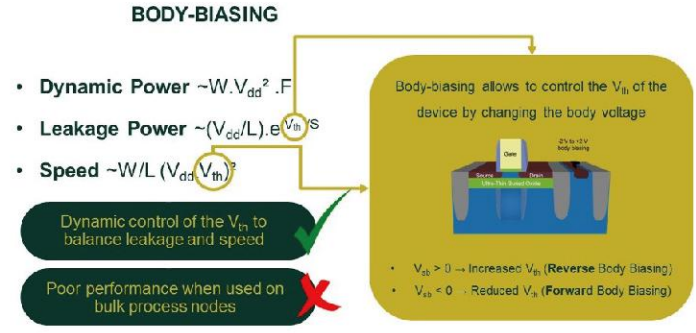



Fig. 6: Body-biasing technique

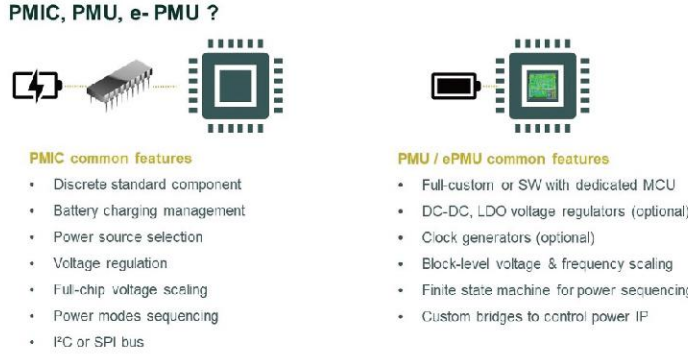



图 7：PMIC 和 PMU / ePMU 的定义

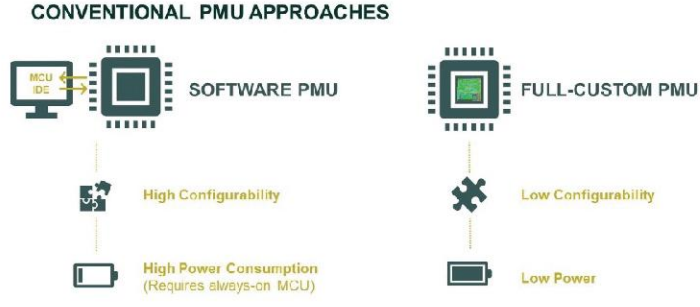



图 8：传统 PMU 方法的优缺点

Easy-Logic

# 奇捷科技Functional ECO

## 更精准、更效率地解决IC设计全流程的逻辑问题

技术团队连续三年荣获ICCAD CAD冠军，产品经过数年打磨，已获全球顶尖IC设计公司采用

## 领先的国产自主研发技术

### 01 功能强大

支持先进工艺设计；支持多时钟、多电压、多模块、多位寄存器，电压隔离单元等；覆盖IC设计全流程。

### 02 迅速便捷

相比手工ECO，EasyECO可能节省数日甚至数周工作时间；
相比其他ECO工具，EasyECO速度更快，可比其他工具运行时间缩短数倍

### 03 结果优异

仅仅增加最少数量的逻辑补丁（备用资源），变更数量极少更小的逻辑补丁可以让时序收敛更容易通过

## 为您节省

**$10 million**

**重新流片费用**

整个电路设计周期较长，在已经完成电路功能设计进入到后期设计流程后，电路的功能会由于性能改善、新功能增加或错误修复等原因，需要再一次进行设计变更。奇捷科技的自动Functional ECO工具可以协助您轻松完成IC设计后期的逻辑修正，以节省上千万美金的重新流片费用。

## 只需原有

**30%**

**时间和人力**

当电路已经完成布局、布线时，工程师不希望重新合成网表以增加新的逻辑功能，因为那相当于又要从头开始重新设计，重新完成一遍完整的设计流程会耗费大量的时间。因此通过增加一个APR网表补丁来变更网表逻辑功能或增加新逻辑功能会为整个项目节省大量时间。

## 处理时间和效率

**10X**

**优于市场现有产品**

奇捷科技的明星产品EasyECO对于流片前或流片后均可进行ECO操作。EasyECO采用了革新的算法，其运行速度和所需备用资源数量均有巨大改进。测试结果显示，EasyECO的运行时间可比传统工具快数倍，所需要的备用资源数量平均减少30%。有些case甚至所需资源数量可减少10倍以上。

用不兼容。

### 稳压器：从分立到集成

降低 BOM 成本的需求意味着，为了在 SoC 中同时拥有不同的电源，高效的稳压器越来越多地被嵌入到 SoC 中，以避免 PCB 上昂贵的分立器件。

稳压器基本上分为两类：线性稳压器（LDO）和开关稳压器（DC-DC 转换器）。选择取决于应用场景，通常是在效率、面积和 BoM 成本之间进行权衡。

如今的物联网 SoC 通常会嵌入多个线性和开关稳压器，为其主要领域（逻辑、RF、IO、Always-On 和模拟电源）供电。

漏电流绝对是必须满足 IoT 系统严格功率约束的关键模拟特性之一，但无论输出电流如何，DC-DC 转换器展现出高效率的能力对于希望采用这种方法的模拟设计人员来说都是一个真正的挑战。

当要在休眠和运行模式下实现超低功耗指标时，问题会从高效率变为低静态电流，这通常可以通过使用低静态 LDO 来提供 Always-On 域来实现。

### 关键配置

前面的章节表明，一个 ULP MCU 可以用许多不同的 IP 配置来构建，但可以确定四大类，下面将总结这四大类。

第一类包括所有依靠外部 PMIC 单元（通常在 PCB 上）来管理 MCU 电源电压的产品。

第二类与 MCU 有关，这些采用了一些电源管理解决方案（例如时钟门控和 / 或稳压器），但依靠 MCU 上不断运行的软件来管理不同的资源。这种配置具有完全灵活的优势，同时无需为虚拟的电源管理单元（PMU）增加硬件开发成本。

第三类代表了主流的 ULP MCU，适用于那些试图嵌入一切（包括作为 FSM 的 PMU）的公司，以便从芯片中榨取每一个微瓦特。

第四类展示了 Dolphin Design 公司的 SPIDER 平台可以实现的目标。该平台不同于其他方案，因为它采用了特定的功率门控解决方案、独特的 AON 标准单元、超低漏电稳压器和独特的 FD-SOI 自适应体偏压解决方案。

| Power Management Techniques | IP solutions | Configurations | | | |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 SPIDER |
| Power Management Unit (PMU) | External PMIC | Yes | | | |
| | SW PMU | | Yes | | |
| | Full Custom PMU | | | Yes | |
| | MAESTRO | | | | Yes |
| Integrated Regulators | Standard Regulators | | Yes | Yes | |
| | Low Leakage Regulators | | | | Yes |
| Power Gating | Standard PMK Digital Domain | | Yes | Yes | |
| | CLICK Digital Domain | | | | Yes |
| | NEVA IO Gating | | | | Yes |
| Always-On Domain | Foundation IPs Standard Cells | Yes | Yes | Yes | |
| | Dedicated Standard Cells | | | | Yes |
| Adaptive Body Bias | ABB IP | | | | Yes |

Fig. 9: ULP microcontroller configurations

## ULPMark Benchmark

超低功耗（ULP）为当今的 MCU 设计人员带来了主要的设计挑战，其产品期望范围从使用单个电池运行 10 年到从环境中采集皮焦耳的能量到减少全球总体能源需求。

多年来，EEMBC 提出了评估性能 / 功率的基准，以实现微控制器和节能策略的公平比较。

有两个针对 ULP 微控制器的基准，ULPMark-CP 和 ULPMark-PP。

第二项侧重于外设数据传输的架构改进，而第一项（内核相当时）其实是关于技术与主动电源管理的权衡。这也是为什么使用 ULPMark-CP 来评估本文所描述的配置的原因。

ULPMark-CP 专注于 MCU 内核，特别是在睡眠和运行模式以及这两种模式转换期间的能源成本。该基准使用了一套通用的 8 位、16 位和 32 位微控制器上的便携式工作负载。该基准测试以 1 秒的周期运行，并将这些工作负载与较长时间的不运行状态结合在一起（使用微控制器的低功耗模式时）。换句话说，基准测试在长时间的睡眠模式下运行，然后在运行模式下短暂唤醒以执行最少的处理，从而模仿了一个节能边缘节点。

图 10 显示了一个理论例子，其中运行周期长度持续 1 毫秒（取决于为基准选择的 MCU PLL 频率和运行基准所需的周期数，具体取决于 MCU 架构）。在这段 1 ms 的时间内，CPU 消耗 2 毫安（2 mA）的电流，在基准测试的 1 秒钟内实际上是 2 微安（2 μA）的消耗。MCU 在休眠模式下又消

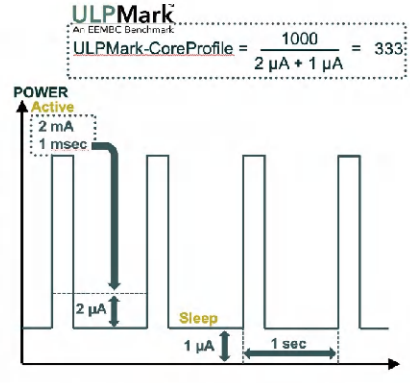



Fig. 10: ULPMark-CP operation

耗1微安。ULPMark-CP得分计算为1000/(运行+休眠消耗)。在图10的具体案例中，分数是333，是一个特别好的分数。

Ⅰ）配置1。

在第一种配置中，电源管理能力降至最低。芯片使用外部PMIC以Go-No-Go方式产生电源电压。不使用休眠模式，芯片只是处于运行或断电状态（参见图11）。

从SoC设计的角度来看，这种配置是最简单的，结果是PCB上较高的BOM成本，而且没有权利管理电源。

因此，这种配置被认为是功耗方面最差的情况，被视为是ULPMark-CP的参考分数，如图17所述。

Ⅱ）配置2：

在第二种配置中，大多数与电源管理相关的解决方案都已在芯片中实现，但设计时间较长。这种方法需要专业的工程师来管理所有不同的技术和IP以及UPF(Unified Power Format)。

这种方法的主要目的是使休眠模式与电源和时钟门控技术结合起来，最大限度地减少功耗，特别是对于ULP MCU执行的低占空比操作。

数字域的电源门控实现了深度休眠模式。在这种模式下，只有一部分芯片保持运行，以保留一些数据或启用唤醒，即所谓的Always-On域。该域通常由高Vt或厚氧化物标准单元组成，因为其低漏电值通常为0.8 V或0.9 V，具体取决于工艺技术。与配置1相比，这种策略可使ULPMark-CP得分提高62倍（参见图17）。

为了实现这一改进，必须永久运行一些软件，作为MCU的PMU。即使它可以在非常低的功率模式下运行（例如在1 MHz下），甚至在睡眠模式下也仍然会消耗功率，从而将增益降低了4倍（参见图17）。

最后，在集成稳压器上运行可带来额外的能效提升，转化为10%的提高。

总体而言，ULPMark-CP得分提高了16倍，这是一个巨大的进步，这说明了为什么越来越多的公司现集成了稳压器和电源管理模块。

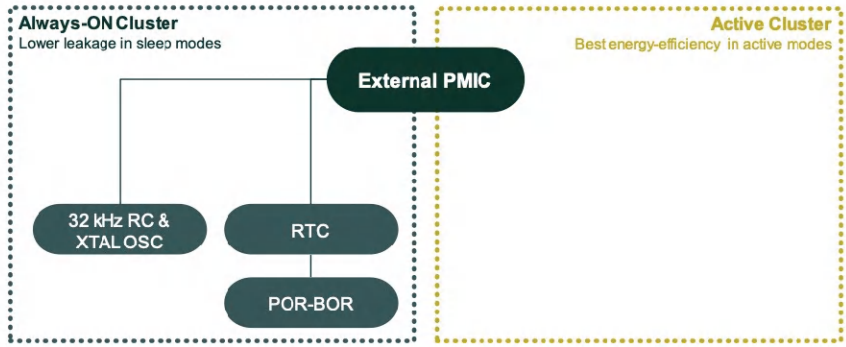



图11：配置1

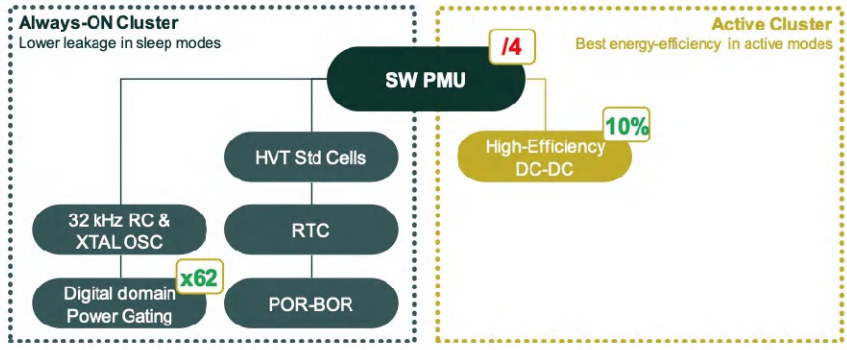



图12：配置2

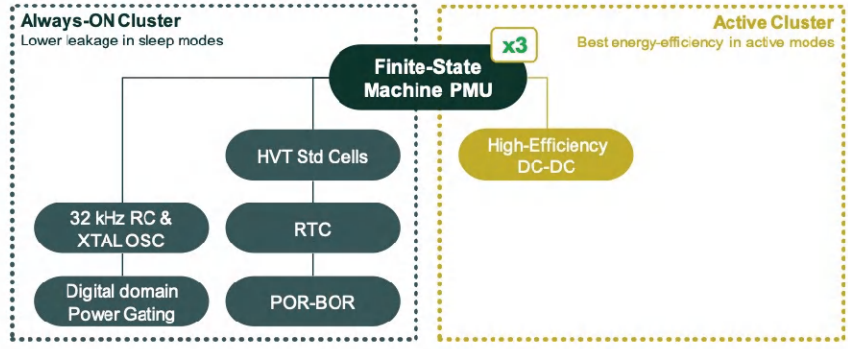



图13：配置3

Ⅲ）配置3。

虽然前一种方法有很大的收益，但它会因软件模拟单片机的PMU而产生功耗。

为此，最先进的公司已经用轻量级的有限状态机(FSM)PMU取代了SW PMU。这种方法大大降低了功率损失，在ULPMark-CP得分提高了3倍（参见图13）。

然而，由于这些MCU将在大量的应用场景下使用，FSM的缺乏或有限的可重构性可能是一个问题。

Ⅳ）配置4：

在FSM上的超低功耗PMU操作与SW PMU的高可重构性之间存在一种折衷的解决方案。

Dolphin Design的嵌入式电源控制器MAESTRO是一种完全可配置的软件IP，可控制SoC电源管理，从启动到最先进的DVFS方案以及时钟和电源门控方案。该IP不仅具有与有限状态机相关的优势（超低功耗和预编程模式），

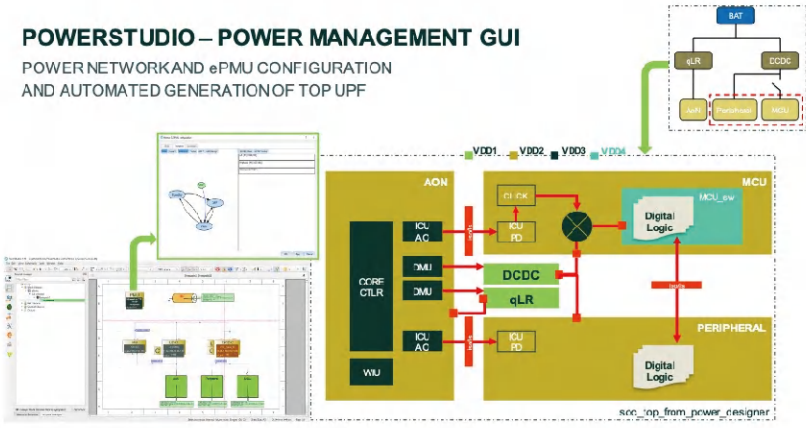



Fig. 14: Dolphin Design PowerStudio GUI

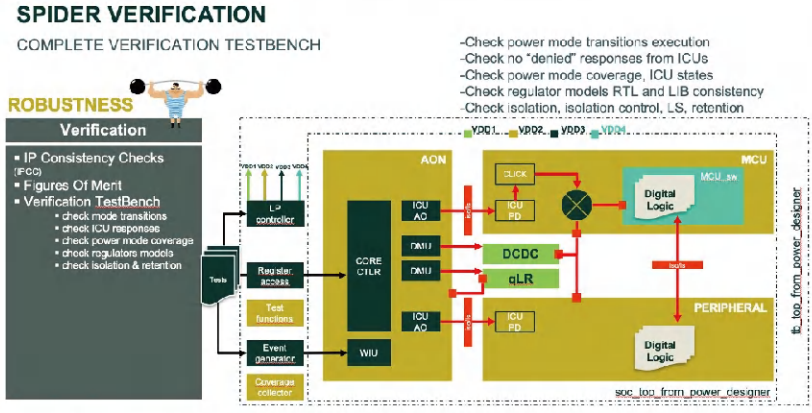



Fig. 15 : Dolphin Design PowerStudio verification and IP consistency checks

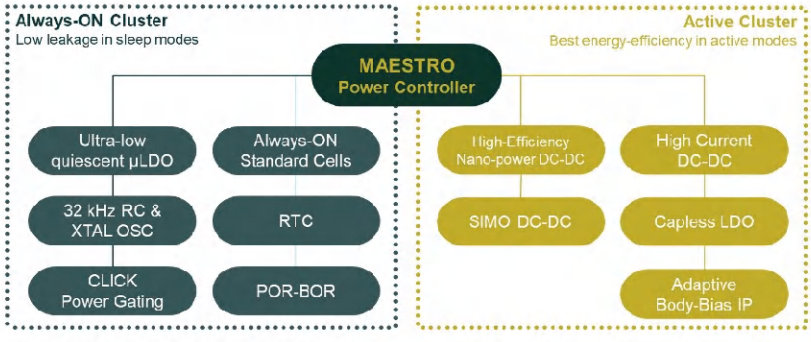



Fig. 16: Dolphin Design IP offering to enable active power management

还可以通过其驱动程序在现场进行重新编程，并提供与 MCU 上 PMU 软件相同的可配置性。

MAESTRO 拥有一套全面的稳压器，在运行模式下，它能有效地转换输入的电池电压。所有这些 IP 都是可配置的，以满足确切的需求并建立一个最佳的电源网络，同时控制 BOM 和集成成本。这些 IP 可以优化运行模式下的功耗。

深度休眠模式下的漏电是 ULP MCU 的主要耗电因素，因此我们开发了一套独特的 Always-On 解决方案，以实现超低漏电。这套 IP 不仅包括超低静态 LDO，还包括专用振荡器和电源门控解决方案。

这种基于 FSM 的可配置方法避免了唤醒 MCU。

软件 IP 可以很容易地用 PowerStudio 进行配置，PowerStudio 是一个专门的配置平台（参见图 14），它在配置 PMU 的同时可以构建优化的电源网络（参见图 14）。第二步，配置好的 RTL 会自动生成相关的验证测试平台和相关的 IP 一致性检查，以实现稳健的集成（参见图 15）。

除了 PowerStudio，Dolphin Design 的 SPIDER 还提供了一系列的超低漏电 IP，通过降低休眠模式下的漏电来进一步提升性能。

Dolphin Design 名为 CLICK 的解决方案取代了标准的 PMK，这是一个可调的电源门控解决方案，提供了 2.2 倍的性能提升。这种提升主要来自于以下事实，即由于 Ron/Roff 比率可在线调整，因此必须集成较少数量的开关，从而限制了睡眠模式下的额外漏电。

另一个改进来自于用 Dolphin Design 独特的 AON 标准单元取代传统的 HVT 标准单元，这种单元虽然在相同的电压下工作，但漏电率更低。这提供了 1.5 倍的额外性能提升。

最后，使用超低漏电线性稳压器为 Always-On 域供电，由于静态电流的增益，带来了 1.1 倍的性能提升（参见图 16）。

总体而言，与配置 3 相比，SPIDER 的 ULPMark-CP 得分提高了 3.6 倍，这是最有效的电源管理策略。与被动管理电源的情况相比，增加到 135 倍的巨大提升（参见图 17）。

## 成果总结与标杆

在本文中，我们探讨了各种通用配置如何逐步提高 MCU 的功率指标。探讨的两个主要参数是休眠模式下的漏电流（单位：µA）和运行模式下的能效（单位：µA/MHz）。这些参数是 ULPMark-CoreProfile（CP）分数的核心，该分数被广泛用于微控制器的基准测试。与 MCU 微架构密切相关的 ULPMark-Peripheral Profile（PP）相比，ULPMark-CP 几乎完全与电源管理策

平头哥
www.t-head.cn

# 平头哥玄铁910

扩展RISC-V架构的性能边界

平均提升20%性能

+13%
桌面级CPU测试基准

+16%
嵌入式CPU测试基准

+26%
通用测试基准

+21%
加解密测试基准

为5G、自动驾驶、网络通信等
AIoT场景提供更强算力



# 平头哥无剑SoC平台

承担AIoT芯片约80%的通用设计工作量

让芯片研发企业专注于剩余20%的专用设计工作

无剑由SoC架构、处理器、各类IP
操作系统、软件驱动和开发工具等模块构成

芯片设计的“平头哥模式”

以无剑平台为核心，面向应用领域全栈开放集成

实现处理器、算法、操作系统等软硬件核心技术的深度融合

扫码申请玄铁910
全球免费开放仿真代码

中国·上海市·浦东新区川和路55弄张江人工智能岛A2栋阿里研发中心

中国·杭州市·余杭区向往街1122号欧美金融城(EFC)英国中心西楼T6-阿里巴巴

技术咨询邮箱：marketing_thead@service.alibaba.com

| Power Management Techniques | IP solutions | Configurations' ULPMark Scores | | | |
|---|---|---|---|---|---|
| | | 1 (ref)<br>1 (ref) | 13x<br>13x | 2.9x<br>37x | 3.6x<br>135x |
| Power Management Unit (PMU) | External PMIC | Yes | | | |
| | SW PMU | | Yes | | |
| | Full Custom PMU | | | Yes | |
| | MAESTRO | | | | Yes |
| Integrated Regulators | Standard Regulators | | Yes | Yes | |
| | Low Leakage Regulators | | | | Yes |
| Power Gating | Standard PMK<br>Digital Domain | | Yes | Yes | |
| | CLICK<br>Digital Domain | | | | Yes |
| | NEVA<br>IO Gating | | | | Yes |
| Always-On Domain | Foundation IPs Standard Cells | Yes | Yes | Yes | |
| | Dedicated Standard Cells | | | | Yes |
| Adaptive Body Bias | ABB IP | | | | Yes |

Fig. 17: ULP MCU configurations ULPMark scores comparison

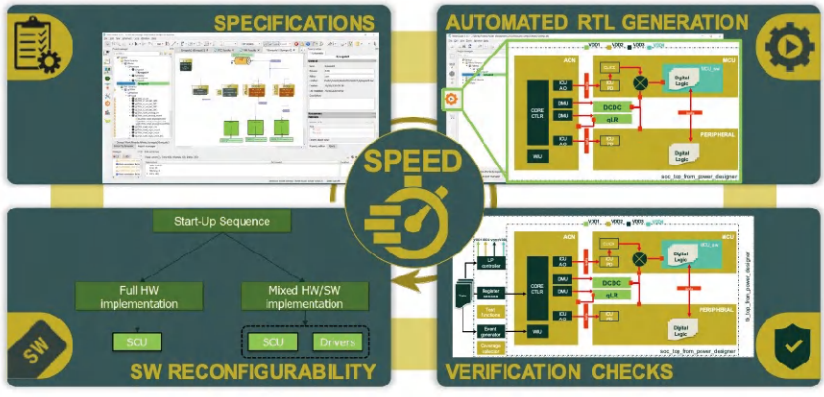



图 18：SPIDER 平台一瞥

略相关，因为现在大多数 MCU 使用相同的 CPU（通常是 Cortex-M4 或 Cortex-M7）。

a) 结果总结

ULPMark-CP 得分的改进（相对于配置 1）总结如下。第一条分数线是指从配置 N-1 到配置 N 的相对改进（例如，在配置 3 和 4 之间观察到 3.6 倍的改进）。第二条分数线指的是自配置 1 开始的绝对改进（例如，在配置 1 和 4 之间观察到 135 倍的改进）。

使用 Dolphin Design 的 SPIDER 所获得的最高分数来自该平台中同类最佳的 IP。该平台还提供其他好处：它的建立是为了在 IP 之间提供强大的一致性，并实现简单而强大的实现，从而通过经过优化和经过硅验证的 IP 集来实现最高效的电源网络。

b) SPIDER 平台概述

图 18 对这种方法进行了全局解释。为了方便电源架构工程师，SPIDER 平台嵌入了一个名为 PowerStudio 的 GUI，它有助于在规范阶段定义、架构和构建任何类型的电源网络。自动计算出功绩值（FOM），并可使用 FOM Podium 功能进行比较，以确保产品的最佳选择。在此阶段，不仅要根据应用目标选择稳压器和电源门控解决方案并确定其大小，而且还要对 MAESTRO 电源控制器进行全面配置（包括启动序列和所有预编程的过渡序列）。

一旦选择完成，由于在第一阶段执行的配置计划是一个更大的域的一部分，因此该 PMU RTL 会自动生成，而 IP 已得到充分验证。

在第三阶段，适当的 IP 兼容性检查与自动生成的验证测试台一起运行，以检查 RTL 中的 PMU 集成。

最后，在运行时，MAESTRO 可以通过软件（提供驱动程序）按需重新配置。如果不需要它，它就像标准的 FSM 一样在预编程的启动序列和过渡序列上运行。

c）行业标杆

由于与最先进的产品配置相比，其 3.6 倍的得分看起来过于乐观，因此我们已经在硅片上运行了一些 MCU（采用 40 nm LP 和 22FDX 技术），以测量休眠模式下的泄漏电流和运行模式下的能效。实验结果如图 19 所示。40LP 试验着重于芯片布局的公开，因为当今大多数商用 MCU 使用的技术范围从 90 nm 到 40 nm。

大多数知名的 MCU 公司都在其网站或应用说明中提供了其商用芯片的类似测量结果。图 19 总结了大范围的 MCU 的一些值，包括 ULP MCU（最大频率为 100MHz）和高性能 MCU（最大频率等于或大于 200MHz）。

从这个基准来看，很明显，即使我们正在比较相同的技术节点（40 nm）和等效的内核（Cortex-M4 或 M7 或等效的内核），Dolphin Design 的 SPIDER 仍可以实现超过 3 倍的得分，如图 17 所示。

## 结论

利用其 SPIDER 平台，Dolphin Design 提供了一个交钥匙的解决方案，以加快先进电源管理解决方案的设计，从架构到实施，并在几周内而不是几个月内达到最终的能效数字。

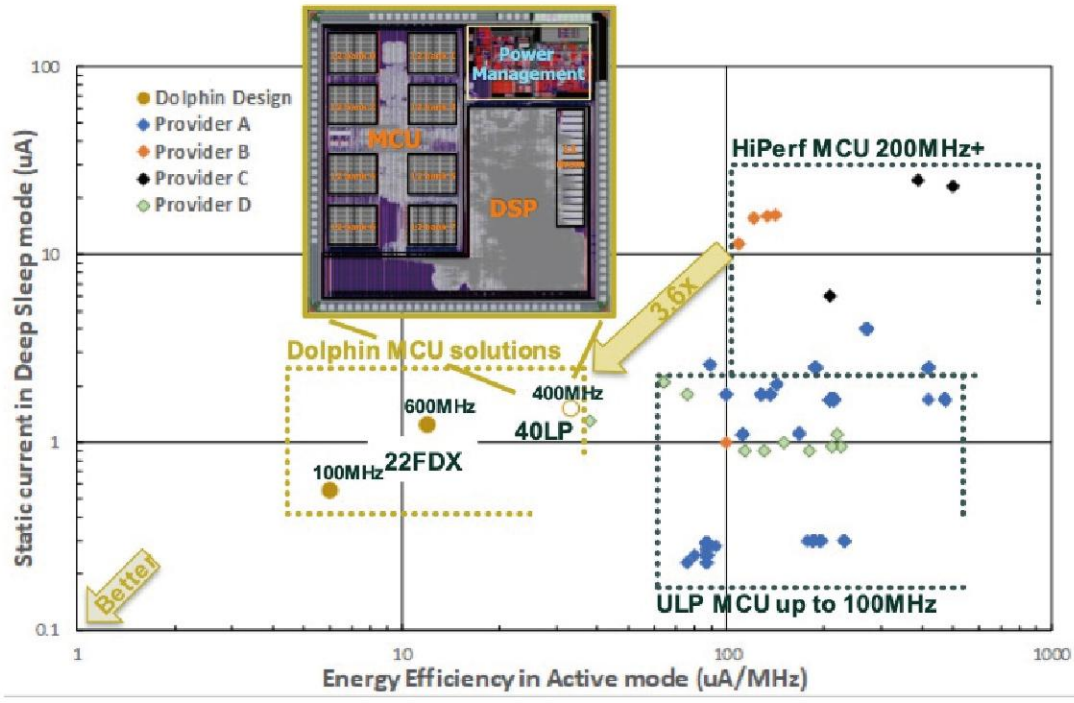



Fig. 19: SPIDER ower Management Platform gains

Dolphin Design 带来了最先进的解决方案，其结合了最先进的电源管理 IP 组合（低漏电 LDO、微功率高效 DC-DC）、可扩展至任何 SoC 复杂度的全配置低功耗电源控制器 IP，以及独特的 PowerStudio 系统工具，加快了电源架构探索和 PMU 无缝集成的速度，从而保证了芯片的安全性，并使上市时间处于可控状态。

专注于您的核心竞争力，用更少的能源做更多的事。

## 关于作者

2018 年，苏希尔•姆希拉获得了艾克斯 - 马赛大学的电气工程博士学位，她致力于先进的现场监控，为汽车和任务关键型应用提供超低功耗集成电路和高度可靠的微控制器。她的工作涵盖了从设计规格到产品工程的所有方面。之后，她加入了曼托图形公司，担任应用工程师

皮埃尔•加泽尔于 2006 年毕业于巴黎高等电子技术学院，获得电子工程硕士学位。2015 年，他获得格勒诺布尔管理学院技术与创新管理行政硕士学位。皮埃尔负责海豚设计公司蜘蛛平台的业务开发和产品营销。在加入海豚之前，他在意法半导体工作了 12 年，先后在数字设计流程和方法领域担任 R&D 工程师、高级工程师和高级技术主管。在此期间，皮埃尔致力于为成熟和先进的硅技术节点开发数字设计平台，并参与了针对物联网、汽车、图像传感器和微控制器市场的关键片上系统和专用集成电路项目。

## 关于海豚设计

海豚设计公司（Dolphin Design）总部位于法国，前身为海豚集成公司（Dolphin Integration），是一家半导体公司，拥有 160 名员工，包括 140 名高素质工程师。

它们提供基于最先进的入侵防御系统和体系结构的差异化平台解决方案，由独特的系统级实用程序定制，以提供由客户或为客户设计的快速、安全的专用集成电路。这些平台可用于各种工艺流程，并针对高能效片上系统设计进行了优化。

他们的客户现在已经超过 500 家，他们专注于人类、创新和长期合作，使他们能够将产品和设备带到数十亿人的手中，这些产品和设备由创新和可访问的集成电路驱动，将环境影响降至最低。在包括物联网、人工智能和 5G 在内的消费市场，以及高可靠性市场，它们释放了 SoC 设计师的创造力，带来了差异化。

告诉他们你最大的梦想。挑战不可能。他们启动了它。

## 参考

https://www.eembc.org/ulpmark/

https://blogs.mentor.com/verificationhorizons/blog/2019/03/05/part-11-the-2018-wilson-research-group-functional-verification-study/

# 安全的硅指纹

郭正伟， IntrinsicID大中华区

## 总述

多年来，基于硅的物理不可克隆功能（PUF）被视为一个充满希望和创新的正在稳步发展的安全技术。同时，低成本和强大的密钥存储技术，对于实现负担得起的、有效的安全系统也至关重要。如今，Intrinsic ID 的基于静态随机访问存储器（SRAM）的 PUF 提供一个成熟和可行的安全部件，正在广泛被用于商业产品中。它们被运用于从微型传感器和 MCU 到高性能现场可编程门阵列（FPGA）以及保护金融交易、用户隐私和军事机密的安全元件等各种设备中。

IntrinsicID 是一家 2008 年从飞利浦电子分拆出来而成立的、总部和研发都位于荷兰埃因霍温的高科技公司，一直专注于研究基于 SRAM 的 PUF 技术，并将其产品化，在过去的 10 多年里得到了广泛的应用。

## 基于 SRAM 的 PUF

由于深度亚微米制造工艺的变化，集成电路（IC）中每个晶体管的物理性能略有不同。这将导致电子特性（如晶体管的阈值电压和增益系数）方面的微小而可衡量的差异。由于这些工艺变化在制造过程中不能完全控制，因此无法复制或克隆这些物理设备属性。

阈值电压易受温度和电压等环境条件的影响，因此其值不能直接用作唯一的密钥或标识符。

另一方面，SRAM 单元的行为取决于其晶体管的阈值电压的差异。即使是最小的差异也会被放大，并将 SRAM 单元推入两种稳定状态之一。因此，其 PUF 行为比基础阈值电压稳定得多，这使它成为使用阈值电压构建标识符最直接和最稳定的方法。

## 基于 SRAM 的 PUF 的行为

SRAM 存储器由许多 SRAM 单元组成。每个 SRAM 单元由两个交叉耦合反向器组成，每个反向器都由 PMOS 和 NMOS 晶体管构建。当电压施加于 SRAM 单元时，其逻辑状态由反向器中 PMOS 晶体管的阈值电压之间的关系决定。首先开始导通的晶体管决定结果，即逻辑的 "0" 或 "1"。

事实证明，每次 SRAM 上电时，由于阈值电压的随机差异，每个 SRAM 单元都有其自己的偏向的状态（“0”或者“1”）。这种偏向性与相邻单元的偏向性无关，也与单元在芯片或者晶圆上的位置无关。

因此，一片 SRAM 区域生成 0 和 1 的独特随机分布。此分布可以称为 SRAM 指纹，因为它对每片 SRAM 是唯一的，因此对每颗芯片芯片也是唯一的。于是，它可以被用作 PUF。

从 SRAM PUF 派生的密钥不会 " 在芯片上存储 "，而是 " 从芯片 " 中提取，当需要时，就实时从芯片中提取出来。这样，它们只在很短的时间内出现在芯片中。当 SRAM 未通电时，芯片上不存在密钥，使解决方案非常安全。

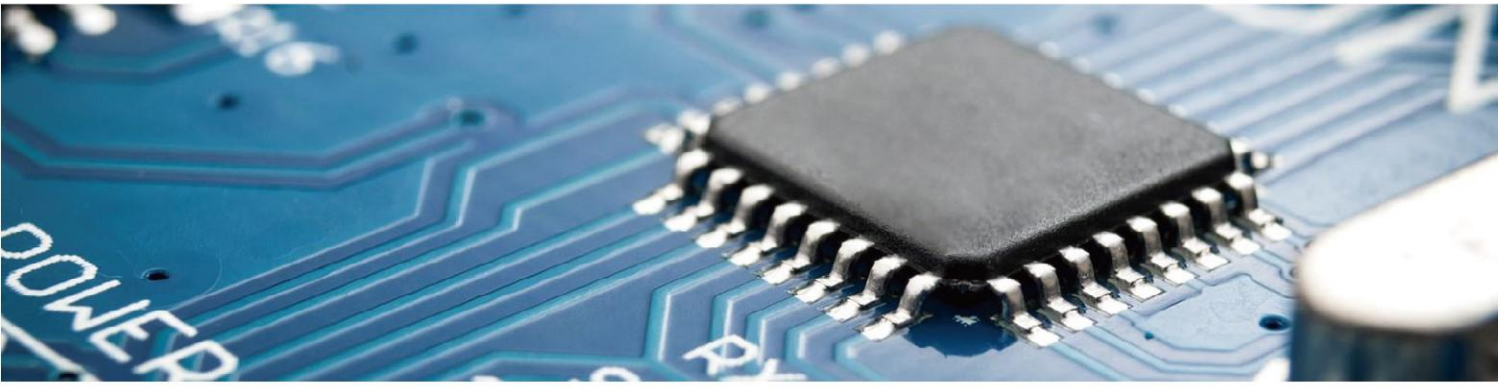
图 1 大致展示了其行为。

## 基于 SRAM 的 PUF 的可靠性

决定 PUF 行为的深亚微米工艺变化在制造过程中被固定下来，之后不会更改。因此，SRAM 单元的上电初始值的偏向性是长期的，并且是稳定的。

然而，仍然有一定程度的噪音。有少数单元的阈值电压是接近平衡的，因此其上电初始值是不稳

ALTRAN
Part of Capgemini



# #1 Ranked in Semiconductor *

End-to-end ER&D services for
Semiconductor and Electronics industries

## Silicon Engineering

End-to-end chip design services for leading-edge ASICs, SoCs and FPGAs
Boards & software to prepare chips for embedded/product development

## Embedded Systems Engineering

Design, development and integration services to tailor embedded systems for vertical markets

## Product Engineering

Design, engineering, test, maintenance and support for end products

| End-to-End | 4500+ Engineers | 15 + Years |
|---|---|---|
| Design services from spec to silicon | Worlds largest VLSI engineering services workforce (2500+) & 2000+ embedded & product engineers | Experience in silicon & platform design and implementation |

| 7nm FinFET | Global Leader | Deep Vertical Expertise |
|---|---|---|
| Expertise in complex SoC geometries down to 7nm | #1 ranked in Semiconductor for the last 3 years * | Expedites both engineering and business outcomes in customers' end markets |

* Zinnov Zones (2016,2017,2018)

Address: Room 1708, Tower 2 of Raffles City No.1191 Changning Road Shanghai China
www.altran.com

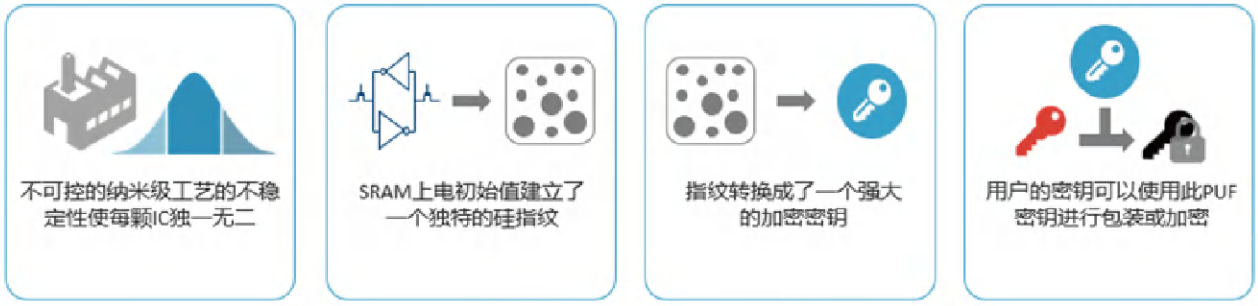



图 1. 从 SRAM 的行为中提取出一个强大的密钥

定的，看起来是随机的，不带偏向性。因此，对于一片 SRAM，每次上电启动时，会出现一个略有不同的初始值，我们将这不同的部分称作噪声。此噪声取决于温度、电压斜坡和工作条件。

基于 SRAM 的 PUF 响应的噪声已经在各种环境和制造工艺中进行了详尽的特征描述和测试：

- 温度范围从 -55℃至 +150℃(-67° F 至 300° F)
- 电压变化 +/-20%
- 湿度高达 80%
- EMC 测试 3V/m（EN55020 0.15~150 MHz 和 IEC 61000-4-3 80-1000MHz）

特别值得一提的是，基于 SRAM 的 PUF 已经通过与客户和合作伙伴的合作，获得了汽车、工业和军事用途的资质，在这些领域已经被广泛使用。

我们已经对其进行了数百万次的测量。在所有这些情况下，基于 SRAM 的 PUF 响应的平均噪声水平被发现低于 15%。尽管有这么多的噪声，但每次为 SRAM 供电时，它都有可能重建一个高熵的、设备唯一的、可靠的密钥。这可以通过应用纠错技术（如“辅助数据算法”(参考文献一)）或“模糊提取器”(参考文献二)）来实现。这些算法执行两个主要功能，即纠错和隐私放大，这将在下面进行解释。

## 纠错

加密密钥重建的纠错技术需要两个阶段：注册阶段和重建阶段。在注册阶段（一次性过程），PUF 响应映射到纠错代码的码字。有关映射的信息存储在激活码（AC）或辅助数据中。AC 的构造使它不会泄漏任何有关密钥的信息。它应该存储在 PUF 算法可以访问的存储器中，但它可以存储在芯片外，因为它不敏感、不用保密。任何对 AC 的更改，无论恶意与否，都将阻止密钥重构。每一个 AC 只对创建它的芯片有效。

每次设备运行身份验证协议并需要 PUF 密钥时，都将重新进行包含有噪声的 PUF 测量，并从 AC 和这个新的 PUF 响应中提取 PUF 密钥（无噪声）。这被称为重建阶段。注册阶段和重构阶段如图 2 所示。

纠错算法的设计使密钥重构的平均错误率小于 -12。即使在极端情况下，例如极端温度下，即使噪声水平上升至 25%，重构的错误率仍然低于 -9。

## 隐私放大和安全

密钥是完全随机的，因此是不可预测的，基于这一事实，密钥提供了安全性。物理测量（如 PUF 响应）具有高度的随机性，但通常不是完全均匀随机的。隐私放大用于生成均匀随机密钥。

通过结合纠错和隐私放大，一个 1kByte 的 SRAM PUF 响应可以转换成为 256 位均匀随机密钥，而对于转换一个具有完全随机的 128 位密钥只需要大约 0.5 kByte。

一个典型的 SRAM PUF 包含如此多的熵，仅需要几十个字节就可以提供一个不重复的全局唯一标识符，该标识符可用作唯一（但有噪声的）电子芯片 ID（ECID）或序列号。

客户的专门的安全实验室和安全团队分析了 Intrinsic ID 的 SRAM PUF 针对各种侵入性和非侵入性物理攻击的安全性，而没有暴露任何弱点。用扫描电子显微镜、激光、FIB（聚焦离子束）和探针攻击都没有成功。侧信道攻击没有导致任何敏感信息的泄漏。

## 老化

在基于 SRAM 的 PUF 上进行了加速老化试验，以研究随着时间推移的噪声水平的情况。通过使用抗老化专利技术，基于 SRAM 的 PUF 技术可以保证 25 年的使用寿命（参考文献三）。

## 实现——软件版本 BK 与硬件版本 QuiddiKey

Intrinsic ID 将上述纠错、随机性提取、安全对策和抗老化技术捆绑在其产品中。它们以非常安全的方式从 SRAM PUF 中提取加密密钥，既有称为

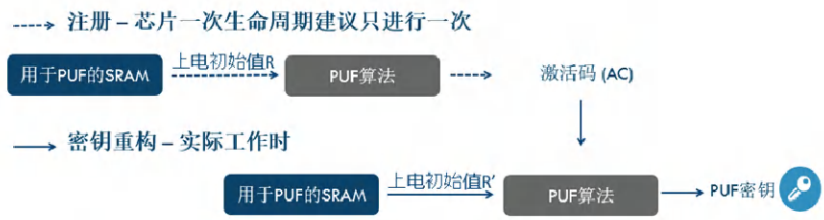
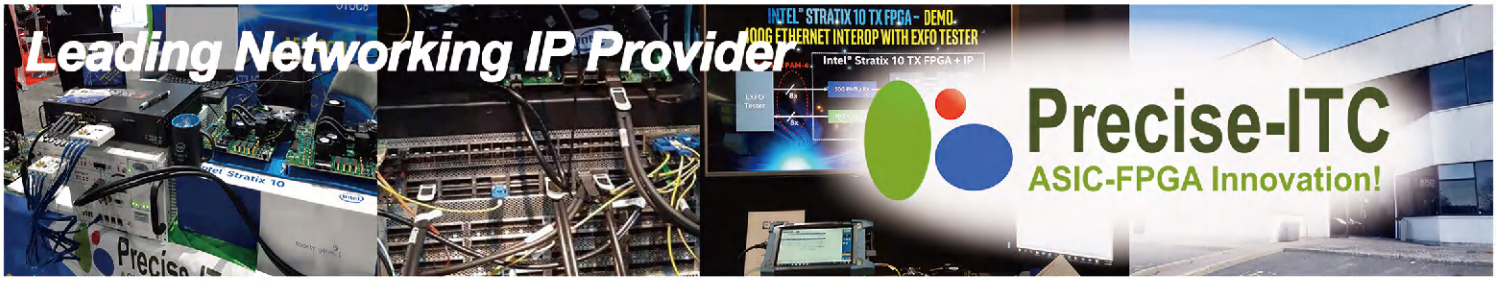



图 2. PUF 密钥生成的注册和重构阶段(注意，R 是注册时的初始 PUF 响应，而 R’是带有噪声的重构时的 PUF 响应)




## ABOUT US:

- Founded in 2003
- Headquarter: Ottawa, Canada
- 3 Lines of Business
  - IP Cores
  - Network SOCs
  - ASIC/FPGA design service; custom development
- Customer Sectors
  - Semiconductor/ ASIC Design Companies
  - Telecom Systems/ Data Centers/ 5G
  - Test Equipment Vendors

## MAIN PRODUCTS:

- Ethernet Package SOC : E-pak 1.6T/800/400/200/100G
- 800/400/200/100/50/40/25/10 GE PCS+FEC+MAC
- FlexE 2.1/2.0/1.1/1.0
- FlexO 1/2/4 - SR framer with FEC
- 1GE/SGMII/QSGMII/USXGMII
- OTUC 16/12/8/6/4 Framer
- 400/200/100/50/40/25/10G CBR Mappers
- OTU4/3/2/1/0 Framer
- CPRI/eCPRI/RoE

***The Largest Supplier of Ethernet and OTN IPs in the World***

## OUR COMPETENCES:

### Top Brand

- 50% Ethernet, 75% OTN 3rd Party IP market shares
- Proven track records
- 100+ successful projects
- 18+ years in business

### 1st Class R&D

- Extensive ASIC, FPGA and system knowledge
- UVM design and verification
- 100% coverage
- FPGA emulation

### Off-the-Shelf IPs

- Reduce time-to-market
- Proven in silicon (FPGA & ASIC)

### Cutting Edge Technology

- Smallest footprint, Ultra-low latency, Low power
- Experienced designs in high end 5nm & 7nm process nodes

### Standard Compliant

- Fully compliant, guaranteed interoperability
- Strong VIP and Test equipment partnership
- Active participation in OIF and IEEE

QuiddiKey® 的硬件 IP 版本（RTL 源代码），也有称为 BK™的软件 IP 版本（二进制库文件），还有软件、硬件相结合的混合版本。当已经集成的硬件加速器（如对称加密算法、非对称加密算法）与 SRAM PUF 技术结合使用时，这些结合硬件和软件的混合解决方案可以极大的提高效率。

硬件 IP 面积小且速度快，大约为 2.5 万门、5 万个时钟周期，可连接到公共互连总线上，如 AMBA@AHB、APB 以及专有接口。逻辑中包含内置的自测试（BIST）、诊断和运行状况检查。并且提供了驱动程序以方便与软件的集成。由于它是纯数字的，单时钟域逻辑电路，它很容易被综合到任何目标工艺库上。

软件参考实现最小、最基础的功能版本可以小到只有 4KBytes，可用于任何主流的平台，如 ARM ®、ARC ®、英特尔 ®、MIPS 和 RISC-V。软件实现可用于通过固件升级的方式将 PUF 技术部署到现有产品中。IntrinsicID 还提供与 Arm@TrustZone 预先集成的 BK 版本。

QuiddiKey 硬件和 BK 软件解决方案都可以根据应用进行优化，以实现低内存占用、低延迟或低存储空间使用。重用或与现有的密码内核和随机数发生器集成可以进一步提高性能并减少占用空间。Intrinsic ID 解决方案附带了全面的产品规范和集成指南，包括说明了提供给应用程序程序员的 API 使用方法的参考代码。

## 使用条件与要求

这些 Intrinsic ID 的产品使用未初始化的 SRAM。这可以是一个单独的 SRAM 块，也可以是一个较大的现有 SRAM 的一部分。标准的 SRAM 就足够了。要存储激活码（AC），需要访问存储介质，它可以是嵌入非易失性内存（NVM），也可以是电路板上的独立存储器，例如闪存或云存储。对于软件版本 BK，需要知道处理器的具体型号以及其具体所使用的 C 语言编译器。PUF 算法可以存储在任何 NVM 中，例如 flash、ROM。

另外，还需要说明的是，SRAM 在几乎所有的 MCU 和 SoC 中都有集成、在芯片制造工艺的每个工艺节点都存在、并且是标准制造流程的一部分。使用基于 SRAM 的 PUF 技术也无需进行耗时的评估和芯片测试，因为 Intrinsic ID 及其合作伙伴的广泛测试已经表明，该技术能够可靠地扩展到当前可用的最小工艺节点。

## 实际使用情况

基于 SRAM 的 PUF 已经被很多半导体公司采用、并且产生已经在市场上大量销售多年。它们已经广泛应用于微控制器、FPGA 和智能卡控制器中（参考文献四）。在其他市场，软件版本（BK）的实现使该技术能够快速部署，甚至可以作为一种在现有硬件基础上进行安全功能改进的解决方案。Intrinsic ID 与领先的半导体公司合作，开发了用于保护嵌入式系统、传感器和控制器的解决方案。有关我们的 SRAM PUF 部署的详细信息，请访问我们的网站：https://www.intrinsic-id.com。

## 结论

基于 SRAM 的物理不可克隆函数已成功在商业产品中实现。SRAMPUF 结合了高安全性和可靠性与低成本、低空间占用、并且易于实现的特点。它们已经被广泛部署在从 MCU 和传感器到高性能 FPGA 和安全芯片等等许多设备中。

许多实现一致地证明了该技术的可靠性和安全性。SRAM PUF 是一项成熟而强大的技术，专为安全性而设计，并基于坚实的理论基础。SRAM PUF 已经在高安全市场中赢得了信誉，现在正在从低成本 IoT 应用到政府、国防和支付行业的高端安全解决方案等市场中越来越多地受到关注和使用。

## 参考文献一：

J.-P. Linnartz and P. Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric templates,” in International Conference on Audio and Video-based Biometric Person Authentication (AVBPA’ 03), ser. LNCS, J. Kittler and M. S. Nixon, Eds., vol. 2688. Heidelberg: Springer-Verlag, 2003, pp. 393 - 402.

## 参考文献二：

X. Boyen, “Reusable cryptographic fuzzy extractors,” in ACM Conference on Computer and Communications Security (CCS’ 04). New York, NY, USA: ACM, 2004, pp. 82 - 91. AND Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in EUROCRYPT’ 04, ser. LNCS, C. Cachin and J. Camenisch, Eds., vol. 3027. Heidelberg: Springer-Verlag, 2004, pp. 523 - 540.

## 参考文献三：

R. Maes and V. van der Leest, ″Countering the effects of silicon aging on SRAM PUFs″, Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST), pp. 148-153 available at http://www.Intrinsic.id.com/wp-content/uploads/2014/09/PUF_aging.pdf

## 参考文献四：

H.Hodson - New Scientist, “Silicon fingerprint on chips could make any gadget unhackable” June 6, 2016 https://www.newscientist.com/article/mg23030771-400-physical-quirks-in-silicon-chips-are-key-to-unhackable-devices/ or “Chip design quirks make our lives more secure” in the June 11 printed issue page 24.

# SweRV Support Package

## 为您部署 SweRV 所需的一切


SweRV EH1 是由 Western Digital 开发的第一代 RISC-V 内核。SweRV 将嵌入在数以百万计的 WD 设备中。而且 SweRV 是开放的，所以您可以自由地使用它来构建自己的 SOC 片上系统。只是，从单纯的 RTL 到硅实现的过程长路漫漫，您需要我们帮忙吗？

我们所推出强大的 SweRV 内核支援方案 (SweRV Support Package，简称 SSP)，提供了完善的包含晶片设计，实现，至测试和软体编程等各阶段所需之文档，脚本，验证环境和用例等各方面支援，并且支持第三方开发工具。使客户能以竞争力最高的技术和最低的开发成本应用 SweRV 核心进行系统单进晶 (SoC) 之整合。

Codasip 已被 Western Digital 选定为 SweRV 的独家官方支持服务提供商。

**“开放内核和专业的技术支持 双剑合璧!”**

codasip®

www.codasip.com

# 使用自定义 RISC-V ISA 指令创建特定域的处理器

Codasip

## 介绍

当系统芯片（SoC）开发人员在设计中包括处理器时，他们在解决计算难题时面临着多种选择 . 复杂的 SoC 通常具有各种处理器内核，这些处理器内核负责各种功能，如运行主应用程序、通信、信号处理、安全性和管理存储。迄今为止，传统上，这些内核可分为不同的类别，如：微控制器（MCU）、数字信号处理器（DSP）、图形处理器（GPU）和应用程序处理器。此外，还为非常专业的应用程序开发了一些独特的体系结构和指令集。然而，独特指令集的缺点是缺乏软件生态系统。

今天，经典内核类别之间的区别日渐模糊。这是因为，如果内核设计的方式正确，该处理器可能涵盖多个用法。此外，通过创建适应 SoC 需求的处理器，可以提高面积和功率方面的硅效率。

创建特定域处理器的最新催化剂是 RISC-V ISA（指令系统体系结构）。由于 ISA 的使用是开放的，免版税，因此它作为实现处理器设计的基础，很有吸引力。此外，每个字长的基本指令集的存在意味着可将使用基本指令集的软件移植到具有该字长的所有 RISC-V 处理器。

RISC-V ISA 采用模块化方式设计，这意味着 ISA 具有几组可根据需要启用或禁用的指令（ISA 扩展）。这可以精确实现此域所需的指令组，而不必为未使用的面积或电源付费。

其中一组很特殊 ；它没有标准的预定义指令。设计人员可以对需加速的应用程序添加所需的任何指令。这是一个强大的功能，因为它不会破坏任何软件兼容性，并同时为发明和差异化留下了空间。本白皮书介绍了如何添加特定域的指令（自定义 ISA 扩展）、如何在 SDK 中构建所有所需的工具，以及如何在 HDL（例如 Verilog）中实现自定义 ISA 扩展。最终结果是一个经优化的特定域处理器。

## RISC-V 指令系统体系结构

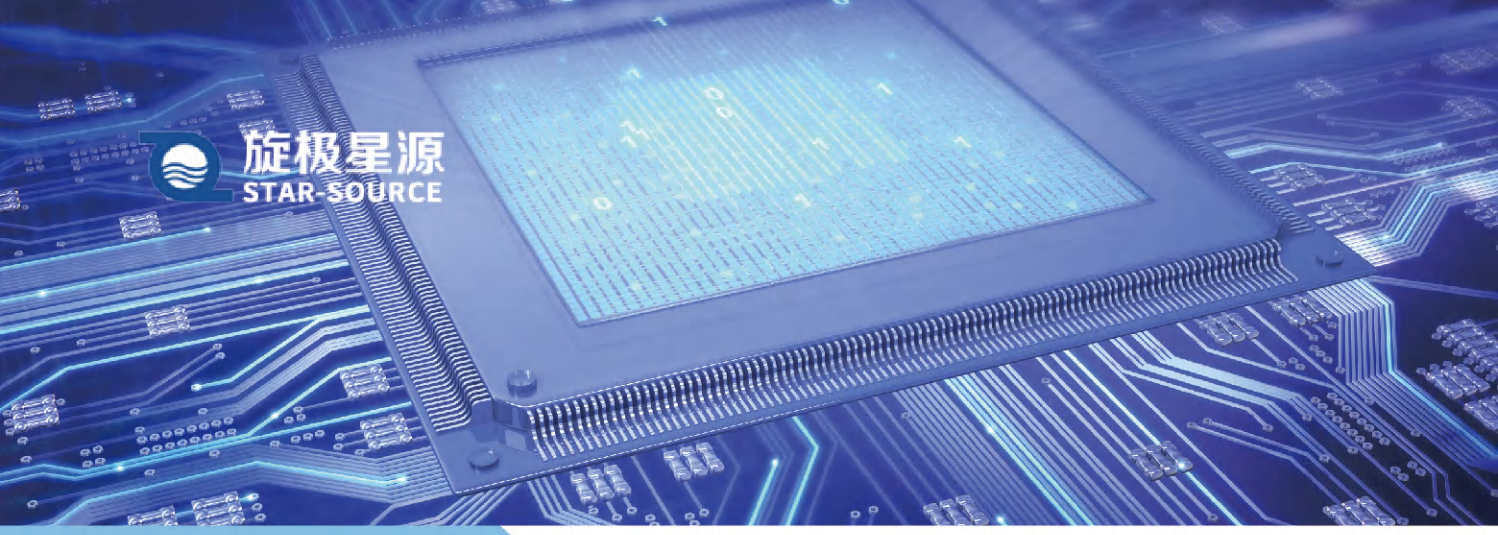
RISC-V ISA 被组织成指令组（基本 ISA 和扩展）。您可以将其随意混合和匹配。例如，您可能具有实现绝对最小值的 RISC-V 处理器，或者具有实现所有 ISA 扩展的 RISC-V 处理器，具体取决于设计需求。

下表列出了 RISC-V 基金会已批准的主要 ISA 扩展和目前正在开发的主 ISA 扩展。

| ISA 扩展 | 获得批准 | 备注 |
|---|---|---|
| /I/E | 是 | 基本整数运算的指令。这是唯一强制性指令组。I 需要 32 个寄存器，E 只需要 16 个寄存器。 |
| M | 是 | 乘法和除法指令 |
| C | 是 | 只有 16 位编码的紧凑指令。此扩展对于需要内存占用低的应用程序非常重要。 |
| F | 是 | 单精度浮点指令 |
| D | 是 | 双精度浮点指令 |
| A | 是 | 原子记忆指令 |
| B | 否 | 位操作指令。该扩展包含用于位操作的指令，例如旋转或位组/清除指令。 |
| V | 否 | 可用于 HPC 的矢量指令。 |
| P | 否 | 嵌入式 DSP 处理器所需的 DSP 和封装的单指令多数据（Packed-SIMD）指令。 |

随着新增更多 ISA 扩展，上表将进行扩展。

尽管该表已经很广泛，但当没有符合设计需求且现成合适的 ISA 扩展时，可能会出现这种情况。在这种情况下，RISC-V 规范允许添加自定义 ISA 扩展。这可能是该公司的 " 秘密武器 " 和关键不同点。




# 射频芯片设计服务　射频 IP 授权服务

## Sub_G RF Transceiver

AGP2141 RF Transceiver IP 采用40nm CMOS工艺，应用于Sub_G射频信号无线收发，支持TDD半双工。IP采用零中频接收机和IQ直接上变频调制发射机结构,实现低功耗设计，支持2V～3.6V供电电压，接收工作电流18mA，发射23dBm功率时工作电流200mA。IP内部集成sigma_delta小数分频锁相环、射频收发开关、零中频接收机、自动增益控制、sigma_delta ADC/DAC、低通滤波器、发射IQ调制器、发射功率放大器和SPI接口，支持输出功率-40dBm～23dBm调节。该IP已和国内多家企业合作，应用于泛在电力物联网及各类自组网领域。

## NB-IoT

2019年成功开发基于55nm工艺的NB-IoT RF Transceiver IP AGP2121，设计兼容3GPP R14 NB-IoT标准，支持R14全部标准频段，是国内唯一单片集成23dBm CMOS PA的超低功耗NB-IoT RF IP，采用了独特的设计架构和特有的低功耗技术，IP达到了业界面积最小和功耗最低，同时性能指标达到国际先进水平，已与多家知名行业客户合作。2020年，旋极星源为能更加顺应市场的发展趋势和3GPP标准的更新，成功开发AGP2122 NB-IoT/GNSS Transceiver RF IP，IP采用更加先进的40nm ulp工艺，可同时应用于NB-IoT射频信号收发和GNSS信号接收，兼容3GPP R15 NB-IoT FDD标准，支持R15标准FDD频段，支持GNSS导航频率(L1，B1，E1)。

**成都旋极星源信息技术有限公司**

Chengdu Watertek Star-source Information Technology Co., Ltd.

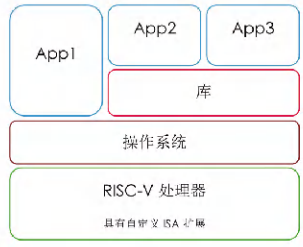
## ABUOT US

***旋极星源，用芯连接你我！用芯改变世界！***

成都旋极星源信息技术有限公司是国内领先的射频及混合信号集成电路设计及应用解决方案提供商，是北京旋极科技集团（股票代码：300324）旗下重要分子公司。旋极星源一直专注于低功耗窄带物联网和卫星导航等领域，定位于180nm至28nm高端射频混合信号芯片设计服务与射频IP Turn-Key服务。

旋极星源也一直致力于同合作伙伴一起打造NB-IoT及低功耗物联网领域的SOC平台方案，我们目前已与多家国内外知名IP设计企业建立了战略合作关系。


schema_ 图 1




schema_ 图 2

由于 RISC-V 生态系统的性质，自定义 ISA 扩展不会违反主要参数——即使使用其他指令，您的处理器仍完全符合 RISC-V 标准，并且可以运行从该生态系统中取得的通用软件堆栈。

图 1 显示了自定义 ISA 扩展如何适合软件堆栈。在最低级别上，有一个具有自定义 ISA 扩展且符合 RISC-V 规格的处理器。它运行一个操作系统，无论是实时操作系统（RTOS）还是传统操作系统。它可利用兼容标准 RISC-V 处理器的任何编译器编译（无特殊的 ISA 扩展）。除了操作系统，还有三个应用程序。App1 是一个不需要任何加速的通用应用程序。您可以使用公开可用的现成编译器（例如 GCC）来编译它，或者甚至可以使用预编译的应用程序；无论哪种方式，RISC-V 处理器都能运行它。App2 和 App3 是需要尽可能快速运行的重要应用程序。这些应用程序必须使用专门了解自定义 ISA 扩展的编译器进行编译。该编译器可以利用可加速 App2 和 App3 的新指令。

图 2 显示了一个具有自定义 ISA 扩展且符合 RISC-V 规格的处理器示例。App1 不使用自定义 ISA 扩展。App2 和 App3 使用通用 API。该 API 由了解自定义 ISA 扩展的库执行，App2 和 App3 可以因此再次获得加速。App2 和 App3 都可以在现成的 RISC-V 处理器中重复使用。接下来只需执行所需 API 的库。在此系统中，使用自定义 ISA 扩展从 RISC-V 将 App2 和 App3 移到没有扩展的 RISC-V 非常简单，并且不需要任何应用程序移植。

在以下各部分，我们将更详细地介绍自定义 ISA 扩展以及 Codasip 如何在设计和验证方面提供帮助。

## 自定义指令集扩展

自定义指令集体系结构或自定义 ISA 扩展屡见不鲜，已得到广泛应用。然而，他们通常需要付出很多努力。首先，您需要确定改进处理器设计的指令。然后，您需要将它们添加到 C 编译器、模拟器、调试器和其他工具中，并验证这些更改是否将相同的内容添加到所有这些不同的工具中。添加自定义指令通常需要一些手动操作。通常，为了便于编程工具可以传递和编译这些指令，您需要一个团队将新指令添加到 SDK 中。您还需要向指令集模拟器添加新代码。最后，必须扩展 RTL，并且必须验证对 RTL 的任何更改。根据手动工作量的不同，ISA 扩展在时间和资源方面可能相当昂贵。

为了降低 ISA 扩展的成本，需要尽可能多地自动化工作，从确定合适的指令到 RTL 验证。这正是 Codasip 的功能优势所在。Codasip 提供了一个名为 Studio 的 EDA 工具，使您能够自定义 Codasip 提供的现成处理器。您可以通过 Codasip 的现成 RISC-V 兼容处理器开始工作，只需根据需要添加自定义 ISA 扩展，也可以从头开始编写自己的 RISC-V 处理器。

自定义指令可以很简单，例如乘加单元（multiple-and-accumulate）的变体，也可以是自定义控制指令，如零开销循环（硬件循环）。您还可以拥有具有后增量或前增量的特殊加载/存储指令。这说明自定义指令因复杂性而不同，会影响 C 编译器的功能和由此产生的处理器的性能。C 编译器可以使用简单的指令，而无需更改原始 C 代码。换句话说，我们可以有一个应用程序，可以将其编译成 x86 或 RISC-V。如果指令过于复杂，则使用它的唯一方法就是内联汇编或 C 内嵌函数。限制约为 ~25 次操作和 ~3 次输出。另一方面，更复杂的指令通常会提高性能，因此结果值得付出此类努力。

有一种将内联汇编或内嵌集成到库中的简单方法。该库也采用一种通用实现方式。这种库的好处是，我们可以实现最终应用，并且可以为多个目标对其进行编译。每个目标可能使用不同的实现方式。该应用不需要了解最终实现。

下面的示例显示了此类库的一个代码段。它表示一个简单的字节交换函数。如果存在指定的宏，C 编译器具有执行交换的特殊指令。否则，将采用标准方法。

```
// universal byteswap() function
inline uint32_t byteswap(const uint32_t word) {
#ifdef ISA_BYTE_SWAP
    // C compiler intrinsic
return __byteswap(word);
#else
return ((word >> 24) & 0x000000ff) |
       ((word <<  8) & 0x00ff0000) |
       ((word >>  8) & 0x0000ff00) |
       ((word << 24) & 0xff000000);

#endif
}
```

为第一部分生成的代码非常简单明确；只有一个指令。

```
byteswap:
byteswap x10, x10
c.jr ra // return from function
```

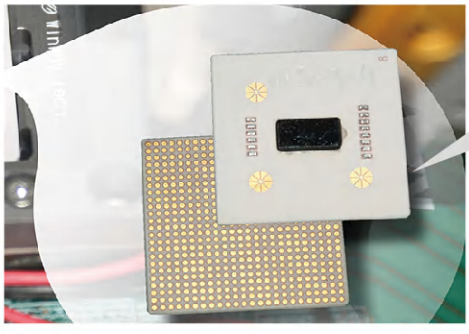
第二部分在 RV32IMC 上的十二个指令中完成。X10s 保留一个词的值，并且它最后也保留返回值。

```
byteswap:
  srl x15, x10, 8
  lui x14, %hi( 65280 )
add x14, x14, 65280 & 0xfff
c.and x15, x14
srl x14, x10, 24
c.or x15, x14
sll x14, x10, 8
lui x13, 16711680>>12 &0xfffff
c.and x14, x13
sll x13, x10, 24
c.or x14, x13
  or x10, x14, x15
c.jr ra // return from function.
```


# General Video Interface: GVI
# SOC/ASIC 芯片的多协议通用视频接口 PHY IP

## One-PHY-Fits-All

GVI PHY IP 是专门为智能电视、投影设备、监控芯片、显示器及其他各类高清视频显示芯片而设计的多通道多协议视频传输 PHY IP 核，可以满足 eDP、 MIPI、VByOne 等主流视频接口协议的电气特性要求和传输数据率要求，同时向后兼容传统 LVDS 视频传输技术。GVI 接口的兼容性，低功耗小面积及通道数可随意配置的特点，为视频类 SOC 客户在选择接口 IP 核上提供了极大的便利与灵活性。



Small Area
Silicon Proven
Ultra Lower Power
General Interface
One channel 24 lanes
Node:22nm,28nm,40nm

成都纳能微电子有限公司
NANENG MICROELECTRONICS
www.nanengmicro.com

四川省成都市高新区益州大道 1858 号天府软件园 G5 栋 708A

Made in CHINA

纳能微主要产品包括：

- GVI 通用视频接口收发器 PHY IP
- USB3.0 PHY IP 核
- USB3.1 Type-C PHY IP 核
- PCIE Gen1/Gen2/Gen3/Gen4 PHY IP 核
- SATA 1/2/3 PHY IP 核
- JESD204B 物理层收发器 IP
- RapidIO/XAUI/SGMII SERDES IP
- 1.25G - 12.5G 通用 SERDES IP 核
- 多路 LVDS 收发器 IP
- 5000V ESD 模拟 IO 库 IP
- LDO/PLL/RC oscillator 等 IP
- USB2.0/USB1.1 PHY 接口 IP

这不仅提高了该应用程序的性能，还显著减小了代码大小。您可以有一些类似的指令，包括种群计数（pop-count）、各种位操作类指令、控制指令等。

下一部分将介绍 Studio 如何处理自定义 ISA 扩展。

## Codasip Studio

Studio 是一款用于处理器设计的 EDA 工具，被多家领先公司用于创建特殊处理器，被 Codasip 用于设计 Bk RISC-V 内核。它可以生成 SDK 中的所有必备工具，以及处理器在 Verilog、SystemVerilog 或 VHDL 和基于 UVM 的验证环境中的实现。所有这些输出都从 CodAL 和 CodAL™中的处理器描述生成。CodAL 是一种基于 C 语言的混合体系结构描述语言。CodAL 不仅捕获 ISA 本身，还捕获处理器的资源和处理器微体系结构的其他细节。

每个处理器描述由两部分组成：处理器的一个功能模型和一个实现模型。这两个模型共用共同的部分，如操作代码或指令编码。更重要的是，这些模型同样使 Studio 能够生成基于 UVM 的验证环境。

当涉及到 ISA 扩展时，设计人员通常从 CodAL 中编写的成熟 RISC-V 兼容处理器开始，该处理器由 Codasip 提供。他们需要做的只是添加自定义 ISA 扩展。请注意，我们在内部也使用 Studio 来构建我们自己的 RISC-V 合规处理器。

该过程首先确定合适的自定义指令。有许多方法可以做到这一点；一种便捷方式是使用 Studio 中的探查器。设计器在现成的处理器上运行关键应用程序，探查器提供表示计算热点的特定指令序列以及需要大量计算时间的函数列表。此信息可帮助设计人员添加新指令。

第一步是更改处理器的功能模型。设计器需要定义指令的汇编和二进制形式。然后，至关重要的是，指令的语义。其语义也可用 CodAL 编写。

在字节交换示例中，假设 32 位 RISC-V，该代码将显示如下：

```
element i_comp_2reg {
  // use of two registers
usexregs as dst, src;
  // textual form of the instruction
assembly { "byteswap" dst "," src };
  // encoding of the instruction
binary { PADDING src  OPC_BYTESWAP[OPC_FRAG1] dst
OPC_BYTESWAP[OPC_FRAG0]};
  // behavior of the instruction
semantics {
// input from register
    uint32 val;
codasip_compiler_builtin();
codasip_preprocessor_define("ISA_BYTE_SWAP");
// read the input from registers
val = rf_gpr_read(src);
// do the computation and store the result to the
register
rf_gpr_write(dst, val[ 7.. 0] :: val[15.. 8] ::
val[23..16] :: val[31..24]);
    };
};
```

下一步是定义实现。让我们考虑在一个时钟周期内执行整个指令简单直接地实现。这里唯一的任务是更新 ALU。

```
...
  case ALU_BYTESWAP:
ex_result = alu_op1[ 7.. 0] :: alu_op1[15.. 8] ::
          alu_op1[23..16] :: alu_op1[31..24];
break;
  ...
```

一旦我们提供了 CodAL 描述，Studio 就可以生成基于 UVM 的验证环境、SDK 和实现中所有工具。

SDK 中最重要的工具之一是 C 编译器。Codasip 使用 LLVM 和 GCC；通常，为 LLVM 编译器生成新指令。在这种情况下，我们可以看到 LLVM 识别字节交换的模式，并在指令语义的中间代码中使用 bswap 函数。生成的代码将表示如下：

```
def i_comp_2reg__regs__regs__:
CodasipMicroClass_<(outs regs:$op0),
(ins regs:$op1)>
{
letAsmString = "byteswap $op0, $op1";
let Pattern = [(set regs:$op0, (i32
      (bswap (i32 CheckFI_i32_regs:$op1))))];
let Size = 4;
letisReMaterializable = 1;
letmayLoad = 0;
letmayStore = 0;
letAddedComplexity = 1;
 }
```

所有其他工具都知道该新指令，因此汇编器和反汇编器、调试器和探查器也可以识别字节交换指令。

关于在 HDL 中的实现，Studio 支持三种主要的 HDL 语言：Verilog、SystemVerilog 和 VHDL。字节交换示例生成的 Verilog 代码如下所示：

```
always @(*) begin
    case ( alu_opcode )
...
// <file>.codal:<line>:<column>
   4'h9: mux_ex_result_D = {alu_op1_Q[ 7: 0],
alu_op1_Q[15: 8],
                                alu_op1_Q[23:16],
alu_op1_Q[31:24]};
    ...
endcase
end
```

如图所示，Studio 基于 CodAL 代码生成所有必要的 CodAL 输出。生成 SDK 和 RTL 完全自动完成。

最后一步是验证。Studio 包括功能视图和实现视图。功能视图用于参考模型，实现视图用作 DUT，这表示生成的实现将针对参考模型进行检查。Studio 生成基于 UVM 的环境，这需要一些刺激因素。Studio 附带了一组广泛的预定义测试，它还支持生成随机指令流，包括自定义指令流。设计人员也可以添加自己的直接测试。三个源（预定义测试、生成测试和直接测试））确保全覆盖，包括非典型极端情况。

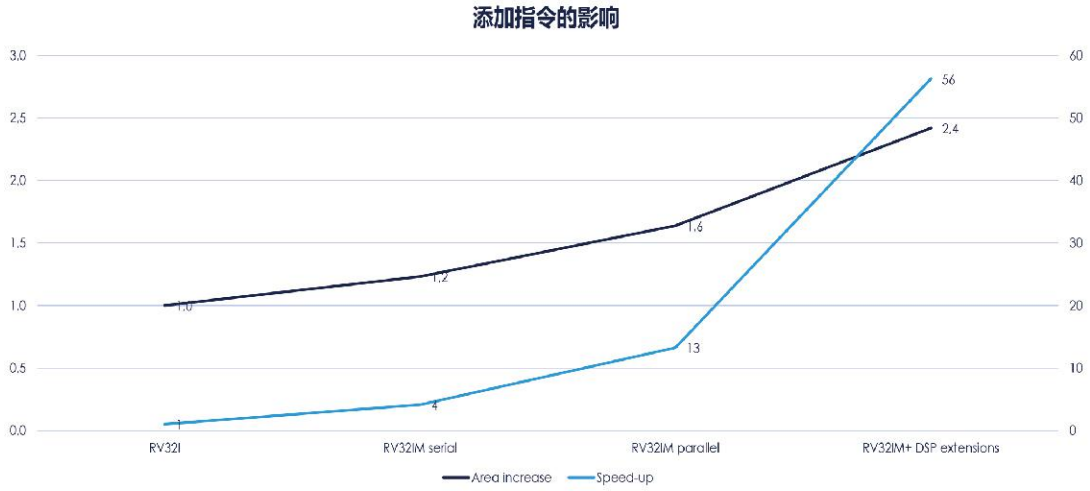
## 用例：针对音频处理优化的处理器

许多常用的算法在通用内核上性能不是很好。典型的示例是用于信号处理、加密和机器学习的示例。一个实例是，Microsemi 有兴趣使用 RISC-V 来取代其音频处理产品系列中著名的商用微控制器内核。

在新一代产品中，他们面临着多种业务挑战：

- 物联网（IoT）应用需要低功耗。
- 希望最大限度地降低处理器 IP 成本，特别是消除版税。
- 旨在最大限度地降低制版和衍生设计成本。
- 旨在提高上市时间。
- 希望提高计算性能和代码密度。

由于缺少 ISA 版税，RISC-V 因成本而成为有吸引力的选择，评估了用于音频处理的各种核心选项。这些测试以最小的 Codasip Bk3 RISC-V 内核为起点，并使用 Codasip Studio 添加一些标准扩展以及自定义指令。




graph_ 添加指令的影响

起点是最少的 RV32I 指令集。相应的基本配置 RISC-V 内核具有 16k 门(Gate)。由于基本指令集没有乘法指令，这些算法包含许多乘法，指令，计算性能太慢也就不足为奇了。

添加乘法扩展 RV32IM 并使用顺序乘法器可提高性能 4 倍，同时将核面积增加 20%。使用并行乘法器产生的结果为具有 60% 禁区的原始 RV32I 内核之性能的 13 倍。

使用乘法扩展和硬件乘法直观合理。然而，真正的改进是在分析软件和设计一组自定义 DSP 扩展之后推出。这两类任务均可在 Studio 完成。

分析生成特定域的处理器后，最终性能比原始处理器增强 56 倍，而只需要 2.4 倍的门数。这种性能改进在门数方面成本不高，非常经济高效。不仅如此，而且代码大小减少到基本配置的 26%。

通过最小化组合内核和指令内存区域，客户能够管理其硅成本和功耗。事实上，他们能够避免迁移到更昂贵的过程节点。

## 用例：加速加密算法

为了进一步说明仅用一条指令扩展一个 RISC-V 内核可以提供可量性改进，让我们考虑为 Veridify（原为 SecureRF）的 Walnut 数字签名算法（WalnutDSA）扩展一个 Codasip Bk3 内核进行身份验证的情况。与其他加密算法一样，RISC-V 上的 Walnut DSA 性能比预期要长。共同调查发现了伽罗瓦域（32）中乘法运算存在瓶颈，即，它需要 24 个周期，其中有一个周期是可取的。

在 CodAL 中定义了一个单周期指令（quad_gmul32），并且由 Studio 以组合逻辑实现。为新指令创建了一个包装器，并且该算法也像以前一样使用。

改进后的 Bk3 RISC-V 处理器比原始版本大 ~2%，但它的速度提升了 3 倍。代码大小也减少了 30%，这将改善指令内存的面积和功耗。

## 结论

特定域的处理器正在成为一种可提供额外处理性能的硅高效方式。RISC-V ISA 由于其模块化和内置的自定义指令支持，所以成为创建此类处理器的理想之选。RISC-V ISA 提供广泛的 ISA 组可供选择，只有基本组（I/E）是必需的，其余的均为可选。这个概念允许设计师精确选择他们需要的内容。如果这仍然不足以达到预期的结果，RISC-V 规范允许添加额外的指令，同时保持 RISC-V 合规。这是一个显著优势，使您能够重用社区软件堆栈，并仅加速关键部分。

添加自定义指令可以手动完成，但这是一项耗时且容易出错的任务，还需要大量资源。Codasip 用它的 EDA 工具 Codasip Studio 来解决这个问题。RISC-V 处理器和任何添加的自定义指令在高级体系结构描述语言 CodAL 中描述，然后 Studio 使用该语言生成 SDK 和实现处理器。高度自动化允许在数小时、数天或几周内添加新指令。

与现成的处理器内核相比，使用 RISC-V 自定义指令创建的特定域处理器效率非常高。在音频处理示例中，门数增加 2.4 倍，性能提高 56 倍。添加一个单指令，数字签名算法的速度会加快 3 倍 。在其他应用领域也取得了类似的进展。为了产生可测的独特改进结果，跨域使用 Codasip Studio 没有限制。

# 成都锐成芯微科技股份有限公司

Chengdu Analog Circuit Technology Inc.

## ●超低功耗 IoT/MCU 方案

全套 nA 级模拟 IP，量产验证品质
涵盖 PMU, AD/DA, USB, I/O, PLL, RC, OSC
特别针对 IoT/MCU 的功能和性能优化
极具成本优势的设计架构
平台化方案加速产品设计，缩短开发周期

## ●高可靠性 MTP 供应商

高可靠性>10Yrs/150℃
擦写次数高达 20K　100K
高达 20nS 读取速度
极具成本优势的设计架构

## ●低功耗蓝牙解决方案

超低功耗
超小面积
射频性能优异
具有良好的兼容性

## ●高性能高速接口 IP 供应商

大批量量产检验
高兼容性
完整的解决方案

Tel: 028-61682666　　Email：sales@analogcircuit.cn
成都、上海、新竹、南京

# 简化视觉SLAM应用程序的开发

CEVA

即时定位与地图构建（SLAM）是指设备（如机器人）利用传感器数据构建周围环境的图像，并同时确定自身在环境中的位置的过程。在实施 SLAM 时，可使用多种不同的软件算法和传感器，包括相机、声呐、雷达、激光雷达与惯性测量单元（IMU）所获得的基础位置数据。

便宜的小型相机的使用使单目视觉 SLAM 系统流行起来，该系统利用单一个标准相机执行定位与地图构建功能。这种视觉 SLAM 系统在一系列机器人中均有应用，包括火星漫游车和着陆器、农场机器人、无人机以及可能在以后出现的无人驾驶车辆。SLAM 系统在 GPS 不可用时也具有优势，例如在室内或 GPS 准确性受建筑影响的大城市。

本文描述基础视觉 SLAM 过程，涵盖目标识别和跟踪以及错误更正涉及的模块与算法。

本文还讨论了利用专用 DSP 执行 SLAM 计算和功能的好处，并以 CEVA-SLAM SDK 开发工具包为例说明了采用该开发方式的优点。

## 直接 SLAM 与基于特征的 SLAM

可使用多种方法实施视觉 SLAM，但所有方法整体相同，即通过连续相机帧跟踪设置点，使 3D 位置形成三角形，同时利用该信息粗略估计相机位姿。此外，SLAM 系统将不断利用复杂算法最大化缩小投影点与实际点之间的差异 - 重投影误差。

根据对接收图像中获得信息的不同使用方式，可将视觉 SLAM 系统划分为直接或基于功能的 SLAM 系统。直接 SLAM 系统对比整张图像，提供丰富的环境信息，使构建的地图更加详细，但处理量大，而且速度慢。本文着重讨论基于特征的 SLAM 法，该方法搜索所设特征（如角点和“斑点”）的图像，仅基于这些特征估计位置与周围环境。尽管基于特征的 SLAM 法未使用图像提供的大量有用信息，但这促进了过程的简化，使计算更易实施。

## 视觉 SLAM 过程

基于特征的 SLAM 的主要步骤是从输入图像中提取一组稀疏特征、将通过不同相机位姿获得的特征进行匹配，以及通过最小化特征重投影误差（指在估计的相机位姿下，某一点的跟踪位置与预期位置的差异）解决 SLAM 问题。

这些步骤通过实施基于特征的 SLAM 的一系列常用构件（如下所述）完成。视觉 SLAM 不断发展，促成了大量研究，为各模块提出和开发了多种算法。每种算法均有各自的优缺点，取决于 SLAM 实施的确切性质。以下描述了部分当前最常用的算法。

特征提取（如图 2 所示）指以紧凑特征向量形式高效表示图像中的有用信息，如角点、边缘、斑点和更加复杂的对象（门窗）。常用的特征提取算法包括高斯差（DoG）和加速分割测试获得特征（FAST9）（因计算效率高而适用于实时视频处理的角点检测方法）。

特征描述将提取的每个特征周围的区域转化为可匹配其它描述子的紧凑描述子。特征可通过（例如）外观或特征点周围区域内的像素强度加以描述。ORB 和 FREAK 是常用的两种特征描述子算法。

特征匹配指将提取的特征（描述子）在多个帧上进行匹配。将第一张图中的所有特征与第二张图中的特征进行对比，以匹配两张图中的特征。由于可在硬件中高效实施对数据位组（如向量）的异或和数据位计数，汉明（Hamming）间距功能常用于特征匹配。汉明距离指示两向量中不同数位的数量，汉明距离越小，匹配度越高。

环路闭合是 SLAM 过程的最后一步，确保 SLAM 解决方案的一致性，尤其是在定位和地图构建操作长期执行时。环路闭合检测非相邻帧提供的相同画面，在帧之间添加约束，从而减小位姿估计的累计漂移。与其它视觉 SLAM 模块相同，现已为环路闭合开发了多种算法，最常用的算法包括光束法平差、卡尔曼滤波与粒子滤波。

## SLAM 实施面临的挑战

视觉 SLAM 处理过程包含的计算量极大，对传统基于 CPU 的实施造成了较大负载，导致了高耗电量与低帧频，进而影响了准确性与电池寿命。新兴 SLAM 应用程序的开发商需要能够实现高度集成与低耗电量的解决方案，在设计中越来越多地使用专用

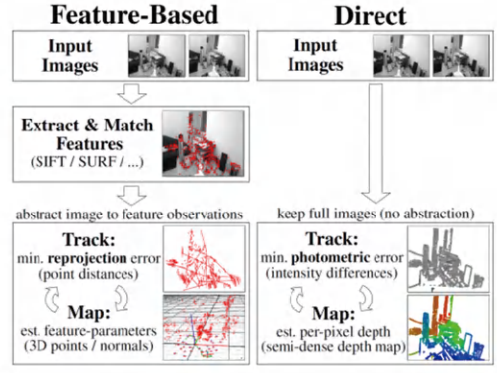



图 1：直接 SLAM 与基于特征的 SLAM 的对比
（来源：https://vision.in.tum.de/research/vslam/lsdslam）

视觉处理单元（VPU）。VPU 是一种专门设计用于加速机器视觉任务（如 SLAM）的微处理器，可用于分担主应用程序 CPU 的视觉处理量。VPU（如图 3 所示的 CEVAs CEVA-XM6）包括耗电低、功能强大的算术逻辑单元、强大的 MAC 能力、高吞吐内存存取与专用视觉指令等特点，还支持图像处理应用需要的强大浮点能力。

即使使用了 VPU，视觉 SLAM 开发商仍须克服若干其它挑战，包括为不同 SLAM 模块创建高效代码和将 VPU 与主处理器连接。

对于嵌入式应用程序，执行速度与耗电量必须得到优化，因此创建高效代码至关重要。视觉 SLAM 模块的编码任务十分复杂，可能需要获取、存储与处理大量数据。以特征匹配为例，描述子以 128 位向量的形式保存在存储器中。为将特征在连续帧上进行匹配，一般必须将 200 个特征与 2000 个候选逐一对比，也就是必须实施 400,000 次匹配操作。匹配操作明显需要大量存储空间，但即使样本数据量较小，高昂的数据获取与格式化费用也会超过编码算法的高效性带来的利益。

Bundle adjustment 是涉及复杂线性代数的另一算法，需要处理大矩阵。现有多种技术可优化上述以及其它 VSLAM 模块的编码过程，但实施这些技术需要掌握较专业的视觉类专业编码知识。

内存管理是图像处理面临的另一挑战。从图像采集的数据一般保存在连续存储位置，而随机从图像中选取区块意味着处理的不是保存在连续存储位置的数据。执行特征匹配的软件程序必须从非连续存储位置检索描述子，这进一步增大了设置费用。

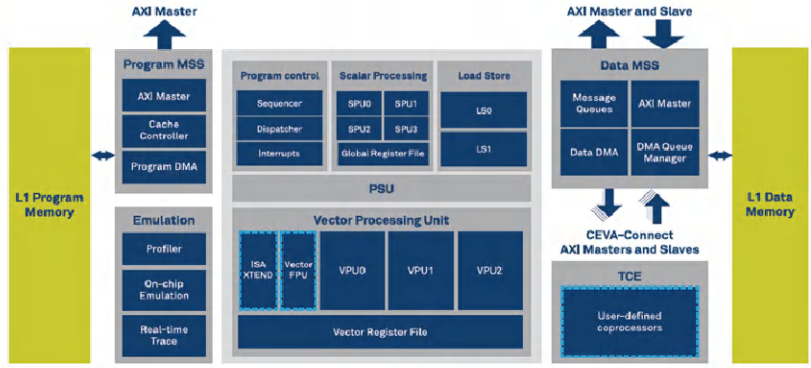



图 3：CEVA XM6 视觉处理单元（来源：CEVA）

## VSLAM 开发工具

上市速度在当今环境下至关重要，但开发商不一定有时间掌握实施高效视觉处理代码需要的技能和知识。幸运的是，现有多种工具可用于加快高性价比 SLAM 应用程序的上市过程，而且有提供视觉软件库、优化硬件和集成工具的应用程序开发工具包，使开发商能够轻松将视觉任务从 CPU 转移到 VPU。

CEVA SLAM SDK（如图 4 所示）是著名的应用程序开发工具包。

CEVA SLAM SDK 基于 CEVA XM6 DSP 和 CEVA NeuPro AI 处理软件，使 SLAM 实施能够被高效地集成到低功耗嵌入式系统中。SDK 包含一系列构件，包括提供特征检测和匹配的高效代码以及 Bundle adjustment 的图像处理库，还支持线性代数、线性方程求解、快速稀疏方程求解与矩阵操作。

CEVA XM6 是优化的图像处理硬件，包括多种创新功能，例如解决非连续存储访问问题的平行加载指令和用于执行汉明距离计算的独特专用指令。SDK 还包括 CPU 接口，使开发商能够轻松将视觉处理功能集成到主应用程序 CPU 中。

SDK 作为开发工具的性能可以得到如下展示，一个以每秒 60 帧的帧速运行的完整 SLAM 跟踪模块的参考实现，测得的耗电量仅 86mW。

## 结论

视觉 SLAM 系统在诸如农场机器人和无人机等一系列应用中越来越受欢迎。有许多替代方法可用于实施视觉 SLAM，但随着嵌入式应用程序的广泛应用，高效编码与低耗电量成为了重要考虑因素。

尽管开发商常使用 VPU 从 CPU 分担计算密集的视觉处理任务，但生产高效代码与管理 VPU 和 CPU 间的接口仍面临重大挑战。

鉴于上市时间是一大驱动因素，开发商可通过集成到 SLAM 专用开发工具包（例如 CEVA SLAM SDK）中的能力加快产品开发。

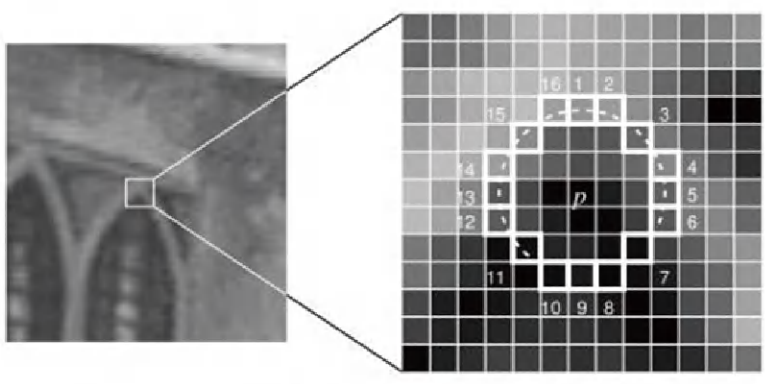



图 2：SLAM 特征提取
（来源：https://medium.com/towards-artificial-intelligence/oriented-fast-and-rotated-brief-orb-1da5b2840768）

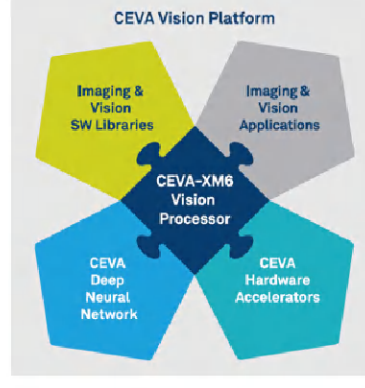


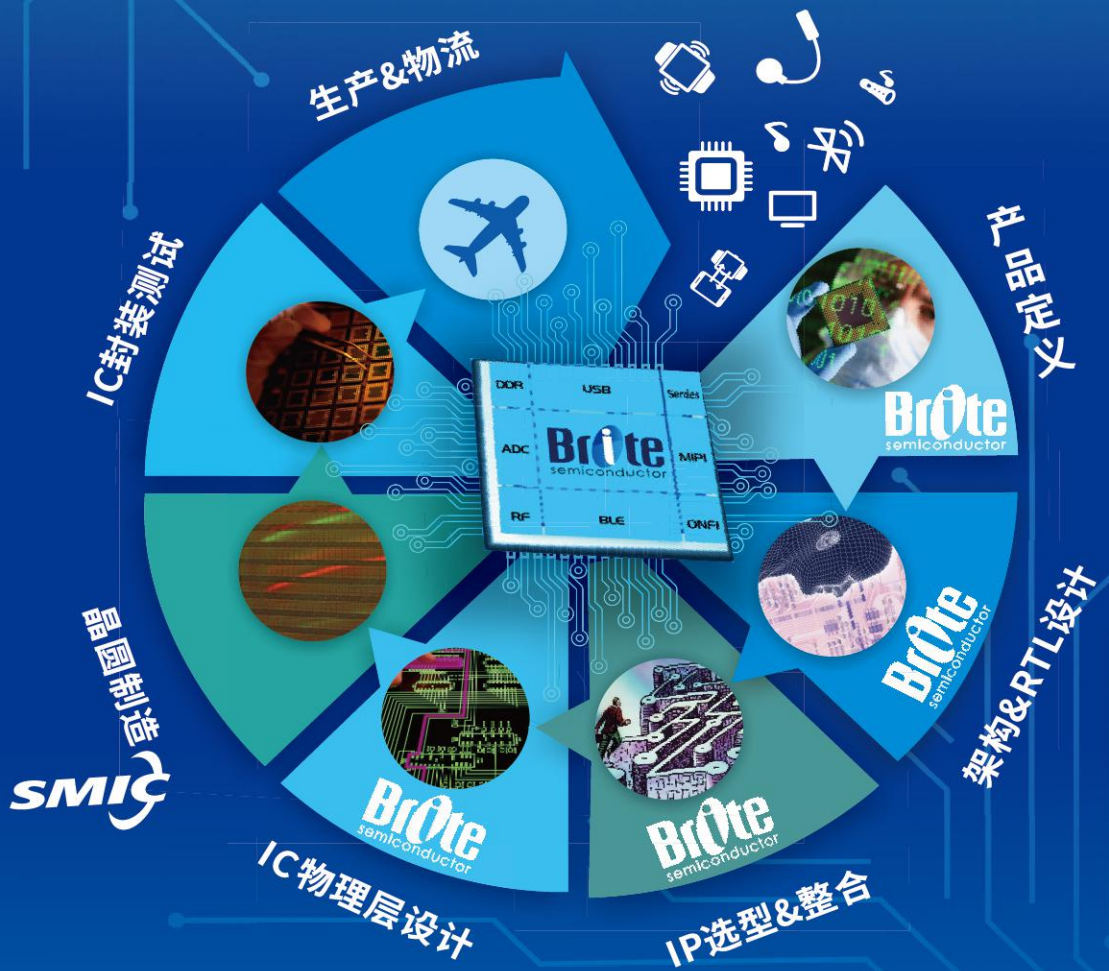

图 4：CEVA SLAM SDK（来源：CEVA）

Brite semiconductor

您值得信赖的

# ASIC一站式设计服务供应商

Brite SMIC




2008年成立
2010年与中芯国际达成战略合作

灿芯半导体 www.britesemi.com
上海 |合肥| 苏州 | 新竹 | 圣何塞
E: sales_bs@britesemi.com

# 如何利用高级DFT最大程度提高企业在半导体行业中的竞争力

Mentor, A Siemens Business

## 简介

通过改进和优化设计与制造的各个方面，半导体行业已经能够实现 IC 能力的巨大进步。可测试性设计（DFT）包括从将测试逻辑插入 RTL 中到现场退货失效分析的一切内容，是半导体业务成功的重要组成部分。如果没有有效的 DFT 策略，公司将难以满足市场对 DFT 集成、缺陷检测以及制造工艺 / 良率改进的巨大需求。这些需求中的任何一项都会干扰产品在市场上的生存能力。此外，DFT 在产品生命周期管理中的作用越来越大，而且对于某些产品，DFT 是系统功能需求的一部分。为了在半导体行业中保持竞争力，公司需要与低风险、值得信赖、有可靠业绩记录（即与合作伙伴共同开发适用于各种设计流程的可扩展技术）的 DFT 解决方案提供商合作。通过与合作伙伴一起全力应对此类挑战，Tessent 成为了遥遥领先的市场领导者和“安全之选”的 DFT 解决方案提供商。我们在整个半导体生态系统中的牢固合作伙伴关系也使 Mentor 处于有利位置，来继续发展 DFT 技术以满足未来需求。

在当今市场上，公司需要利用一些基本 DFT 能力来保持竞争力。基本的 DFT 需求包括：

- 采用最有效的技术来检测制造缺陷
- 实施能够有效集成到各种通用设计流程和系统功能需求中的解决方案
- 利用 DFT 和生产测试结果提高良率，这会直接影响量产时间和盈利能力。

好的工程师基于坚实的数据做出决策。本文介绍了研究与开发的最重要领域，正是它们使得半导体公司能够生产出具有竞争力的产品。文章将展示如何将这些解决方案应用于当今一些最具挑战性的设计，例如：需要层次化即插即用方法的超大型人工智能（AI）处理器，以及需要极高制造测试质量和系统内测试能力的汽车应用。

## 检测缺陷

DFT 的核心功能是捕获所制造硅片中的缺陷，确保零件置于系统内后会按设计运行。缺陷覆盖率是制造测试可以检测到的所有可能缺陷的百分比，可以用一个众所周知的公式表示（Williams,1981），以根据

工艺良率来预测缺陷等级：

缺陷等级 =1- 良率 (1- 缺陷覆盖率 )

缺陷等级通常用每百万件产品的不合格数 (DPPM) 来表示。如果您未能检测出有缺陷的产品，并且交付了过多不合格零件，您的整个业务都会受到影响。表 1 显示，即使达到 99% 的缺陷覆盖率，不同的制造工艺良率也会极大地影响 DPPM 率。达到 99% 的缺陷覆盖率听起来可能不错。但从表 1 可以看出，即使对于 90% 良率的成熟工艺，99% 的缺陷覆盖率也会导致 DPPM 超过 1000。对于当今的许多汽车和功能安全产品，如此高的 DPPM 率是无

法接受的。在相同的 90% 工艺良率下，缺陷覆盖率需分别达到 99.9% 和 99.99%，DPPM 才能分别达到 100 和 10。

表 2 显示了当工艺良率为 80% 时，不同的缺陷覆盖率如何影响 DPPM。

尽管 Williams 公式使得预测 DPPM 率看起来非常简单，但实际上，由于很难确切知道这些变量，应用该公式是很困难的。缺陷覆盖率涉及全部的潜在缺陷类型，它包括固定、转换延迟、路径延迟、IDDQ、桥接、单元感知等已知的故障模型。单元感知故障模型已经开发了 15 年以上，可以有效执行基于缺陷的故障建模，以检测技术单元内的潜在缺陷。关于该技术对实际产品的价值，以及对 DPPM 的巨大影响，行业领先企业已经发表了许多文献，包括 AMD（Hapke，2014）。

最近，“汽车级”ATPG 的进步被继续开发，用于增强单元感知测试，并提供新型桥接、开路、单元感知时序感知（图 1）和相邻单元测试。Intel（Howell，2018）和 ON Semiconductor（Maxwell，2017）已发表硅片结果，表明单元感知测试和新型汽车级 ATPG 具有重要价值。一些读者可能会认为，这些新型测试向量针对的是特殊情况或汽车级 DPPM 要求。然而，凭借 1000+ DPPM 范围内的独特硅片检测结果，许多公司已经对单元感知测试进行了标准化，不再应用固定或转换测试向量。

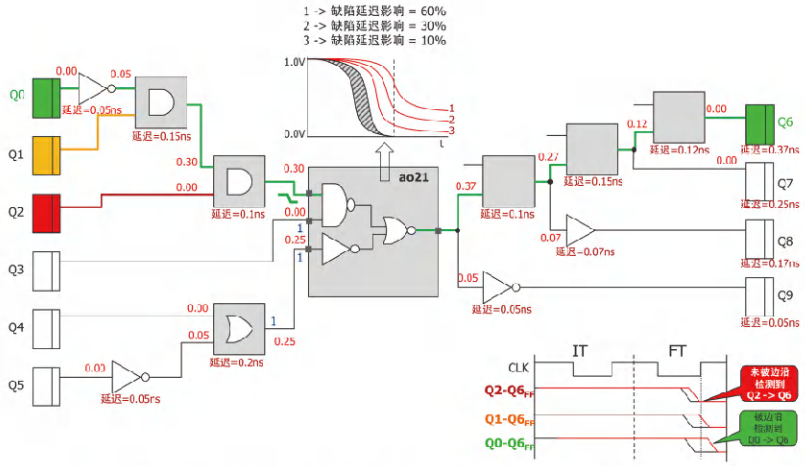



图 1：时序感知 ATPG 与单元感知测试相结合以找到较小延迟（考虑单元内的最长路径和延迟）。

存储器内建自测试（BIST）用于检测嵌入式存储器及其接口逻辑中的故障。存储器 BIST 的最大挑战不是新技术或新型存储器，而是业界倾向获得更多片上存储能力的趋势——如今远远超过嵌入式 SRAM 的 Gbit 范围，涵盖远超过 10,000 个存储器实例。对于具有大量存储器实例的设计，为了管理存储器 BIST DFT，最好用层次化 DFT 方法来实现。针对这种规模的设计，层次化 DFT 需要完全自动化的解决方案，所有参数（测试时间、面积消耗、功耗等）都应该能接受一般用户指令。此外，对每个存储器 BIST 控制器的（移位）访问时间，尤其是访问失效数据以对存储器测试失败进行批量诊断，已成为存储器 BIST DFT 规划的重要组成部分。

Tessent 与 IC 设计人员和存储器供应商紧密合作，不断在最新技术和存储器设计上验证 Mentor 的存储器 BIST 解决方案。因此，我们的标准库算法持续提供最高级别的缺陷检测。存储器 BIST 功能内置了相当大的灵活性，支持对不同样式的存储器设计使用定制算法。几乎每个设计都包含可修复存储器，因此内建修复分析（BIRA）和内建自修复（BISR）在设计中被广泛采用，甚至在系统内被采用。

| 工艺良率 | 缺陷覆盖率 | 缺陷等级 | 每百万件产品的不合格数 |
|---|---|---|---|
| 0.9 | 0.99 | 0.00105305 | 1053 |
| 0.8 | 0.99 | 0.002228948 | 2229 |
| 0.7 | 0.99 | 0.003560396 | 3560 |
| 0.6 | 0.99 | 0.005095231 | 5095 |

表 1：工艺良率会极大地影响 DPPM 率。

| 工艺良率 | 缺陷覆盖率 | 缺陷等级 | 每百万件产品的不合格数 |
|---|---|---|---|
| 0.8 | 0.98 | 0.004452927 | 4453 |
| 0.8 | 0.97 | 0.00667195 | 6672 |
| 0.8 | 0.96 | 0.008886026 | 8886 |
| 0.8 | 0.95 | 0.011095167 | 11095 |

表 2：80% 良率时的缺陷覆盖率和 DPPM。

## 赋能技术

为达到可接受的缺陷率，需要针对各类缺陷使用不同的故障模型，但这要付出实际成本。以 2001-2002 年开发的 130nm 工艺对 DFT 的影响为例。它引入了一种新工艺和新材料（铜），导致缺陷只有在高速运行时才能看到。在那之前，固定故障的高覆盖率被认为是充分的测试。但随着出现这些新的高速缺陷，突然间必须使用转换延迟故障模型来执行高速测试，有时还要使用路径延迟来执行。结果，测试向量数目激增，导致测试成本大增，因为需要更多制造测试设备来满足需求。

正是在这个时候，Tessent Test-

Kompress首次引入了嵌入式压缩技术（Rajski，2004），支持以更少的测试机存储器测试更多的测试向量。由于摩尔定律使设计规模不断扩大，而且新技术产生了新的缺陷类型而需要更多测试向量，因此 TestKompress 压缩水平的提高一直是开发的重点。根据Broadcom发表的文章（Konuk，2015），引入特殊测试点通常将测试向量规模显著缩小5倍，这有助于控制不断增长的测试向量数。纳入LBIST 用于系统内测试，以及MBIST用于高质量存储器测试，对于需要这些的设计至关重要。

## 利用 DFT 提高良率

减少失效芯片的数量并提高制造工艺的可靠性会给业务带来直接影响。但是，要实现目标并不容易。挑战包括不断扩大的设计规模、不断缩短的上市时间以及新工艺节点带来的新缺陷类型和行为。

将芯片交付给客户之前，会使用结构化测试向量来检测失效芯片，失效测试得到的数据可提供关于芯片失效机制的有价值信息，利用这些信息可以更快速地提高良率。拥有制造设施的公司、纯晶圆代工厂和无晶圆厂半导体公司通常会对失效扫描测试数据进行彻底分析，称为扫描诊断。

扫描诊断会产生一组缺陷怀疑点和高度局部化的缺陷位置，它们是该芯片扫描测试失败的原因所在。此详细信息可提高用于验证缺陷机制的物理失效分析（PFA）的成功率。Tessent Diagnosis 已被成功用于指导 PFA 过程以找到根本原因机制。GLOBALFOUNDRIES 报告称，采用这种方法使分辨率提高了 10 倍以上（Benware，2012）。

要分析和解决一个良率问题，意味着不仅要了解单个芯片的失效 / 缺陷机制，还要了解整个芯片群体的失效机制。这群失效芯片可能涉及多个晶圆或批次。通过扫描诊断了解限制良率的因素会带来竞争优势，从而提高盈利能力。

许多公司积极使用批量扫描诊断来实现良率爬升，并提高成熟工艺技术的良率。对于大批量产品，即使很小的良率提升也很有价值。现在，许多公司使用先进的统计分析工具来分析整个批次群体和 / 或晶圆群体的批量扫描诊断结果。经过多年研究，并通过与无晶圆厂半导体制造商、晶圆代工厂和集成器件制造商合作，Mentor 开发出根本原因反卷积（RCD）技术——这是一种非监督的机器学习算法，可在有噪声的情况下根据批量诊断结果估算缺陷帕累托图。

在较新的工艺节点中，前道工序（FEOL）中的缺陷通常是缺陷分布的主要部分。实施新制造工艺的公司必须迅速确定良率限制因素，尤其是当其与特定单元的版图或几何形状相关时。利用针对单元感知测试创建的数据，Tessent Diagnosis 可以指出标准单元内部的缺陷位置和类型。当使用单元感知诊断时，Tessent YieldInsight 生成的缺陷帕累托图可以有前道工序（FEOL）或后道工序（BEOL）的根本原因（Tang，2019）。

减少良率异常周期也可能影响盈利能力。拥有设计的无晶圆厂客户可以持续生成批量诊断结果，分析这些结果，并将其与 PFA 结果相关联。这些批量扫描诊断结果可用来跟踪随时间变化的缺陷帕累托图。晶圆代工厂还可以利用从批量扫描诊断得到的缺陷帕累托图结果，将其与其他数据源相关联，以了解异常的来源。这种协作方法可以加快异常问题的解决，缩短周转时间。

## DFT 方法的进展

随着设计规模的增加，设计流程变得更加层次化，所创建的设计内核在整个物理设计中都具有完整的功能。然后，完成的模块实例化到芯片的顶层中。尝试利用人工步骤，继续进行完整扁平 ATPG 或分区做法的公司，遭遇了产品上市时间的严重延迟。将设计分成更小的部分，使得物理实现更容易被设计人员和自动化工具加以管理。

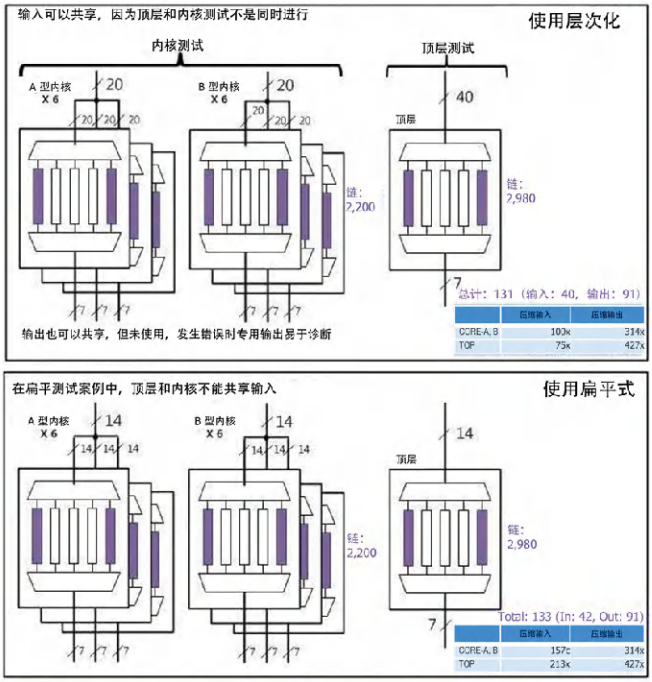
层次化 DFT 还允许您利用具有许多相同实例化的内核，这在许多 AI 设计中都可以看到。所有设计工作都进入到一个实例中，然后可以根据需要进行多次实例化。DFT 还受益于类似分而治之的方法，该方法与其余设计流程一致，可解决大型设计中的相同问题。Tessent 层次化 DFT 的引入，使得物理设计模块不仅可以在功能上是完整的，而且 DFT 也是完整的。这种方法需要一些关键技术，例如：用于分离内核的内核隔离，用于减少机器存储器消耗的灰盒模型生成，以及用于复用内核级别生成的测试向量的测试向量重定向。

改用层次化 DFT 后，DFT 的各个方面都显示大幅改善。Amazon 解释了层次化 DFT 如何将其 DFT 工作从流片的关键路径中剥离出来（Trock，2016）。Samsung 在运行时间、测试向量数和计算资源方面的改善总结在图 2 中（Shin，2019）。采用这种层次化 DFT 方法实现了一个数量级的改善。对于大型 SoC 设计，层次化 DFT 已成为标准做法。

## 统一的 DFT 环境

设计实践不断发展，一个日趋明显的趋势是将尽可能多的设计推到 RTL 阶段，因为当物理综合工具可以看到全部设计时，所产生的时序收敛结果会更好。DFT 一直被视为是偏后端任务，但向来都有必要在设计中添加更多 DFT 逻辑，例如 Tessent TestKompress，以应对测试挑战。随着 DFT 必然地进一步向上游迁移到 RTL 阶段，如下工作变得越来越重要：与前端设计流程合并，以可重复的流程管理这些任务，以及保持设计意识以促进下游集成。

当更多的内核、DFT 功能和复杂性已被集成到设计中，设计人员试图




| 案例（针对固定型） | 测试覆盖率 | 测试向量数 | 运行时间（秒） | 内存使用（MB） |
|---|---|---|---|---|
| 扁平 ATPG | **99.00%** | **169,426** | **982,104** | **191,648** |
| 层次化（重定向：内核 A） | 99.00% | 7,424 | 12,116 | 30,220 |
| 层次化（重定向：内核 B） | 99.01% | 7,168 | 12,317 | 30,277 |
| 层次化（顶层） | 97.93% | 19,396 | 23,563 | 51,690 |
| 层次化（总计） | **99.13%** | **26,820** | **47,996** | **22,378** |

| 案例（针对转换延迟） | 测试覆盖率 | 测试向量数 | 运行时间（秒） | 内存使用（MB） |
|---|---|---|---|---|
| 扁平 ATPG | **90.01%** | **224,468** | **877,018** | **196,887** |
| 层次化（重定向：内核 A） | 90.00% | 19,328 | 32,530 | 49,904 |
| 层次化（重定向：内核 B） | 90.01% | 19,200 | 31,736 | 49,705 |
| 层次化（顶层） | 89.29% | 51,790 | 51,790 | 67,464 |
| 层次化（总计） | **90.01%** | **71,118** | **116,056** | **28,296** |

## 层次化 DFT 实现的结果

- 测试向量数：SA 为 6.3 倍，TD 为 3.2 倍
- 运行时间：SA 为 20.5 倍，TD 为 7.6 倍
- 存储器使用量：SA 为 8.7 倍，TD 为 6.96 倍

图 2：层次化 DFT 为 GPU 设计带来的好处(B. Shin,ETS 2019)。

以简单、低风险且可重复的方式集成所有内容所要遭受的痛苦显而易见。使用 EDA 工具的用户可能认为 DFT 产品都是单独构建的，必须在单个产品之外进行集成。过去确实如此，但现在不是。

为了帮助管理庞大而复杂的设计，Tessent 建立了一个平台，通过一个工具来控制所有内容。Tessent Connect 是近十年开发工作的成果，提供一个集成的 Tessent 平台。这个工具可以执行所有 DFT 操作，而每个 DFT 功能可以共享同一数据库并知晓其他 DFT 功能。因此，Tessent Connect 作为一个“意图驱动”的环境运作，可减少许多步骤并加快产品上市时间。用户可以


图 3：Tessent Connect 提供当前复杂度和集成度所需的平台类型。

在更高的抽象级别下工作。插入 DFT、创建测试向量以及在顶层集成 DFT 功能的挑战，全都在一个即插即用的环境中加以管理。如果没有这样的集成平台，公司将难以在 ATPG 期间管理 DFT 功能（例如 BIST），而且要经过许多步骤才能在顶层集成内核级别 DFT 和测试向量。

eSilicon 讨论了在复杂的下一代 ASIC 上实施 DFT 时 Tessent Connect 为他们带来的价值（Mentor，2019）。Broadcom 为了将 AI 设备等高级设计快速推向市场，采用了层次化 DFT 和 Tessent Connect，结果将实现时间缩短了 50%（Mentor，2020）。他们在美国华盛顿特区举办的 2019 年国际测试会议上介绍了这一重大优势。

## 高级 DFT 对半导体行业的必要性

某些技术领域不断突破工具和技术的界限。如今，AI 处理器设计规模通常非常大，由数以百计或千计的重复处理器阵列组成，并且需要很高的测试覆盖率。没有层次化 DFT 方法将任务细分，便无法进行管理。覆盖率要求包括许多故障模型，这意味着嵌入式压缩也必须很激进。Graphcore 报告说，对于一个含 236 亿个晶体管的 AI 芯片，由于使用层次化 DFT，他们得以在不到三天的时间里便构建并运行逻辑 BIST、ATPG 和存储器 BIST（Mentor 和 Graphcore，2019）。

由于必须满足功能安全应用要求和 ISO 26262 标准，汽车设计对质量的要求最为苛刻。对于设计汽车产品的公司而言，拥有强大的系统内测试能力至关重要。需要管理所有内建自测试（BIST）功能的测试，并非常快速地完成测试。Arm 与 Tessent 合作提供一个安全生态系统（Bush,2019），该系统建立在 Tessent MissionMode 控制器和新型 LBIST Observation Scan 技术基础之上，可将逻辑 BIST 测试时间减少到原来的 1/5（Tyszer，2019）。

DFT 能力和实现不仅取决于 DFT 工具，还取决于与之相关的生态系统。Tessent 与合作伙伴紧密合作以开发基础性和可扩展的技术，Tessent 产品可在任何设计流程中工作。我们同

时知道为客户提供一个坚实生态系统的重要性。因此，Tessent 与合作伙伴密切合作以提供如下生态系统：

• Arm 单元感知库模型，用于单元感知测试和单元感知诊断(Gahdhi,2019)

• Arm/Tessent 层次化参考流程，用于包含 Arm 内核的子系统 (Press,2019)

• Samsung 晶圆代工厂 SAFE 汽车和层次化参考流程

• Teradyne 和 Advantest ATE-Connect 云端测试机访问

• Teradyne 和 Advantest 1149.10 高速 IO (HSIO) 扫描测试

• Tessent 还有很多其他参考流程；其中很多提供开源测试用例

## 结语

我们与业界领导者密切合作，精心开发出 Tessent 解决方案，提供可扩展的技术。尤其是提供了创建汽车级 ATPG 的能力和真正的层次化即插即用 DFT 平台，对许多公司来说是很重要的解决方案。旧的 DFT 方法对于当今存在的大量设计并不奏效。Tessent 平台旨在将所有 DFT 功能集成在一个工具和一个数据库下，并搭配通用的即插即用基础架构来集成模块和 DFT 功能。

作为市场领导者，Tessent 拥有比其他所有 EDA DFT 供应商加起来还要多的资源，这使得 Tessent 能和合作伙伴一起打造出具有前瞻性的功能。Tessent 小组与半导体设计和生产相关的所有领域的大多数领先企业展开合作。

## 参考文献

T. W. Williams, N. C. Brown. (1981). Defect Level as a Function of Fault Coverage. IEEE Transactions on Computers.

F. Hapke et al. (2014). Cell-Aware Test. Trans on CAD, vol 33, no 9, 1396-1409.

W. Howell et al. (2018). DPPM Reduction Methods and New Defect Oriented Test Methods Applied to Advanced FinFET Technologies. International Test Conference. IEEE.

P. Maxwell et al. (2017). Bridge Over Troubled Waters: Critical Area Based Pattern Generation. European Test Symposium (ETS). IEEE.

J. Rajski et al. (2004). Embedded Deterministic Test. IEEE Transactions on CAD, 23, 776-792.

H. Konuk et al. (2015). Design for low test pattern counts. IEEE Design Automation Conference (DAC). IEEE.

B. Benware et al. (2012). Determining a Failure Root Cause Distribution From a Population of Layout-Aware Scan Diagnosis Results. IEEE Design & Test of Computers.

H. Tang et al. (2019). Yield Learning for Complex FinFET Defect Mechanisms Based on Volume Scan Diagnosis Results. 2019 30th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC) (pp. 1-7). Saratoga Springs, NY, USA: IEEE.

D. Trock et al. (2016). Recursive hierarchical DFT methodology with multi-level clock control and scan pattern retargeting. Design, Automation& Test in Europe Conference&Exhibition (DATE). IEEE.

B. Shinet al. (2019). Novel Clock and Reset DFT Methods to Improve Hierarchical ATPG pattern Reuse Shown on a GPU Design. European Test Symposium (p. Embedded Workshop). IEEE.

Mentor. (2019). Mentor' s Tessent Connect automation reduces IC test implementation costs and accelerates time to market. https://www.mentor.com/company/news/siemens-mentors-tessent-connect-automation-reduces-ic-test-implementation-costs-and-accelerates-time to-market.

Mentor. (2020). Broadcom case study using Tessent Connect to build DFT flow for AI chips. https://www.mentor.com/products/silicon-yield/blog/post/broadcom-case-study-using-tessent-connect-577682b3-95b5-4d70-9998-3f5deef0f153.

Mentor. (2019). Graphcore leverages Mentor DFT solutions to speed time to market for innovative AI acceleration chip. https://www.mentor.com/company/news/siemens-mentors-graphcore-leverages-mentor-dft-solutions-to-speed-time-to-market-for-innovative-ai acceleration-chip.

S. Bush. (2019). Mentor aims at automotive functional safety with tool ecosystem. Electronics Weekly.

B. Lu et al. (2018). The test cost reduction benefits of combining a hierarchical DFT methodology with EDT channel sharing-A case study. International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS). IEEE

R. Gahdhi et al. (2019). Beyond traditional ATPG:A test methodology targeting in-cell defects. Arm community web site site - https://community.arm.com/developer.

R. Press (2019, August 15). Achieving more efficient hierarchical DFT for Arm subsystems. Tech Design Forum.

C. Acero tt al. (2016). On New Test Points for Compact Cell-Aware Tests. IEEE Design & Test, 7-14.

J. Tyszer et al. (2019). Test Time and Area Optimized BIST Scheme for Automotive ICs. International Test Conference (ITC). IEEE.

R. Singhal. (2019). How To Manage DFT For AI Chips. Semiconductor Engineering.

扫一扫，获取白皮书电子版，
随时阅读！

IP Reuse SoC Design
IP与SoC设计

您愿意收到（可多选）
☐ 数字版《IP与SoC设计》
☐ 印刷《IP与SoC设计》
☐ 相关电子快讯/厂商信息

# APPLICATION N FORM
# 索阅表

## 您是否希望收到/继续收到免费的《IP与SoC设计》杂志？

☐ 是　　☐ 否

## 请填写您的姓名及联系方式

时间：_____ 月 _____ 日 _____ 年

姓名：_____ 职务：_____

电话：_____ 邮箱：_____

公司：_____

地址：_____

邮编：_____

**您的主要工作范围**
(单选项)

☐ 芯片架构
☐ 数字前端
☐ 数字后端
☐ 数字验证
☐ 可测试性设计（DFT）
☐ 射频芯片设计
☐ 模拟芯片设计
☐ 模拟版图设计
☐ 单元库
☐ MEMS/分立器件
☐ 其他

**主要终端产品或服务**
(单选项)

☐ 汽车电子
☐ 消费电子
☐ 工业控制
☐ 医疗电子
☐ 网络通信
☐ 物联网
☐ 云计算
☐ 人工智能AI
☐ 其他

**您推荐,支持或者决定购买的产品**
(可多选)

☐ Analog & Mixed Signal
☐ Storage Controller & PHY
☐ Graphic & Peripheral
☐ Interface Controller & PHY
☐Processors & Microcontrollers
☐ Memory & Logic Library
☐ Security
☐ Multimedia
☐ Wireline Communication
☐ Wireless Communication

**请回答所有问题，我们将根据您的回答确定是否寄送免费的《IP与SoC设计》杂志。**
详情请联系：朱慧　电话：0510-85386687　电邮：zhuh@jsic-tech.com

# ATTENTION PLEASE
# 请注意

## 请完成下面三个简单步骤

**Be sure you have followed these 3 easy steps:**

1 . 回答所有的问题 Completed all the questions

2 . 签名并注明日期 Signed and dated the form

3 . 网上填卡 Online subscription

## 在我们的单位内及朋友中，我推荐以下人士阅读《IP与SoC设计》

请寄《IP与SoC设计》杂志免费索阅卡到以下地址：

Please send Free 《IP Reuse and SoC Design》China Subscription Card to The following individuals at my location:

公司/Company _____

地址/Address _____

| | 姓名/Name | 工作性质/Job Function | 电邮/E-mail |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |

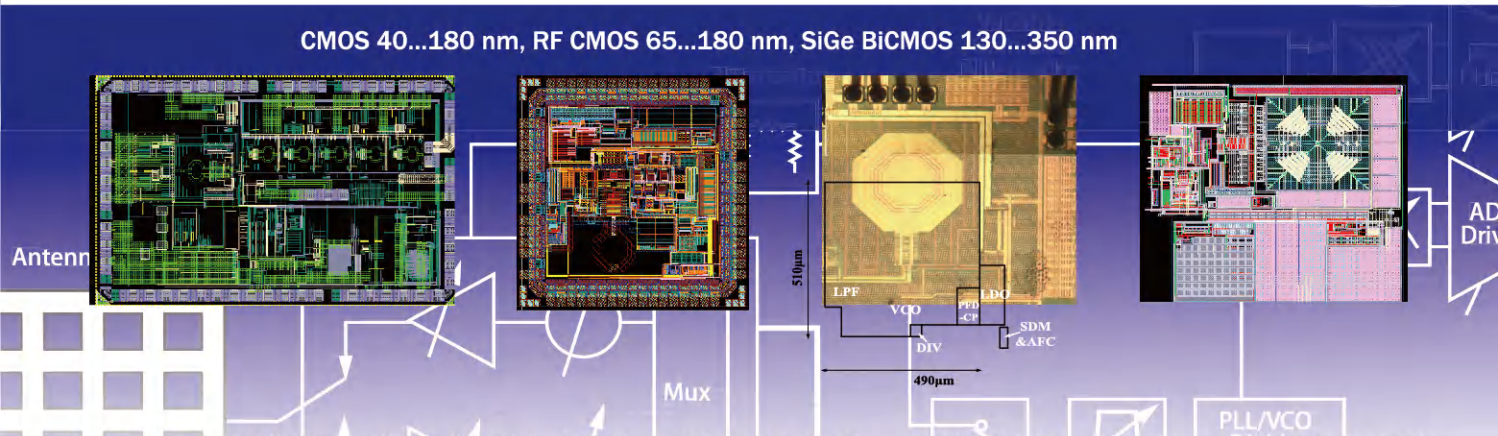
请将表格工整书写填妥后，用以下任何一种形式交回，复印有效：
Please fill in the form completely in print and return by one of the below methods, copy is acceptable

邮件至（E-mail to）：zhuh@jsic-tech.com

或邮寄至（Mail to）：

江苏无锡市新吴区菱湖大道111号无锡软件园天鹅座C座19楼 邮编：214000
19th floor, block C, Cygnus, wuxi software park, 111 linghu avenue, xinwu district, wuxi city, jiangsu province, China

# 国内领先的模拟和射频芯片设计服务及 IP 提供商




**尔芯电子能够提供广泛的射频集成电路设计服务，拥有 350nm 到 40nm 的 RFCMOS 和 SiGe 的经验，频率高达 40Ghz。可以支持您的定制规格或利用我们广泛的 IP 来支持您的需求。设计范围从单个的模块，如 LNA、VCO、PLL 或 MIXER 到完整的无线电子系统。我们与一流的晶圆厂、封装、测试的战略关系，加上我们丰富的设计专业知识，确保射频和微波设计满足客户的预期。**

## Design service ： Sub-6GHz Transceiver

支持 Sub-6G 工作频段，采用零中频结构，射频带宽最高可支持 200MHz，可配置小数频率综合器，提供窄带和宽带两种模式选择，快速带宽 / 直流消除 / 镜像抑制 / 载波馈通等校正技术，fast SPI 配置，为系统集成提供便捷灵活的接口。WIFI/BLE/SDR 等项目和产品经验涵盖 ADC/DAC。
工艺：CMOS 和 SiGe
制程：180nm/130nm/90nm/65nm/55nm/40nm
※根据客户需求定制高性能和低功耗版本

## Silicon IP ： PLL

Frequency band：
550MHz
Phase noise：
<-117dBc/Hz@100kHz
<-140dBc/Hz@1MHz
RMS Jitter：217fs (10k-25MHz)
Spur：<-65dBc
工艺：CMOS 和 SiGe
制程 ：180nm/130nm/90nm/65nm/55nm/40nm
※可以根据客户需求定制

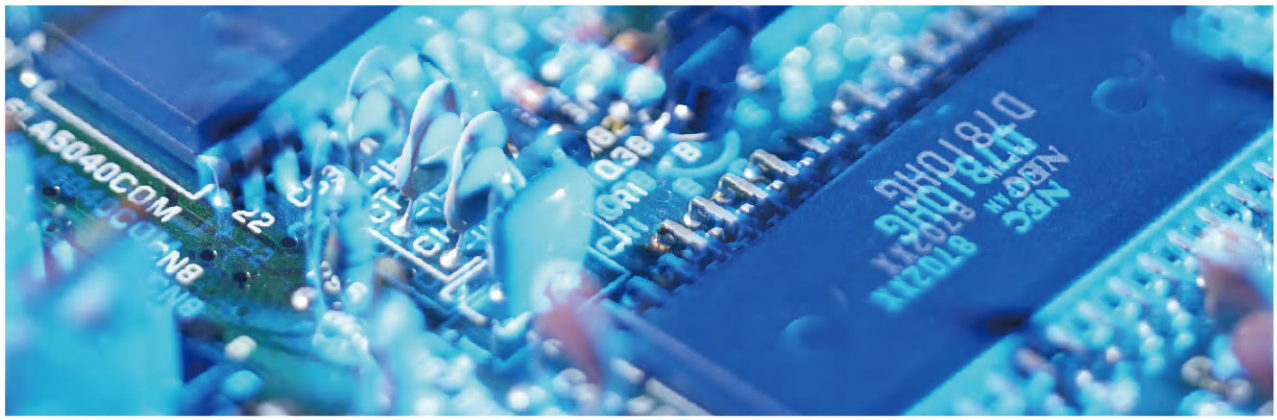
Frequency band：
2.8-3.8 GHz
Phase noise：
<-120dBc/Hz@1MHz
<-98dBc/Hz@100kHz
RMS Jitter: 0.86ps (10kHz~10MHz)
Spur：<-65dBc
工艺：CMOS 和 SiGe
制程 ：180nm/130nm/90nm/65nm/55nm/40nm
※可以根据客户需求定制

Frequency band：
20-26GHz
Phase noise：
<-110dBc/Hz@10MHz
RMS Jitter：低于 80fs (10k-40MHz)
Spur：<-70dBc
工艺：CMOS 和 SiGe
制程 ：180nm/130nm/90nm/65nm/55nm/40nm
※可以根据客户需求定制

## Silicon IP ： LDO/Buck/POR/RTC

低纹波和低噪声线性低压差 LDO 和 Buck
极低功耗，亚阈值工作区间
制程：CMOS 和 SiGe，180nm/130nm/90nm/65nm/55nm/40nm
※根据客户需求定制高性能和低功耗版本

EXCHIP
南京尔芯电子有限公司



# 基于Cadence CHI和IVD VIP的多核SOC系统数据一致性验证

范君健，晁张虎，杨庆娜，刘 琪，朱 红，单建旗
天津飞腾信息技术有限公司， Cadence

## 摘要

在多核的 SOC 系统中，不同的处理器核对内存空间和设备空间进行着大量的数据读写操作，维护 Cache 一致性面临严峻挑战。集中于控制流方面的验证环境搭建已非常复杂，而包含数据正确性检查的验证由于控制流程复杂、数据量大等问题而更加困难。针对这一问题，本文基于 Cadence 公司提供 CHI VIP、AXI VIP 和 IVD VIP，实现多核环境下的系统级数据一致性验证。本文搭建的验证平台中采用 CHI VIP 通过笔者开发的 CHI 协议转换桥发出访存请求，使用 AXI VIP 收集到达主存的数据，由 IVD VIP 对 CHI 端口的请求数据与 AXI 端口的访存数据进行实时分析比对，实现在较高抽象层次上的激励产生和响应检查。该验证平台能够在子系统级及系统级进行数据一致性验证，具有验证环境搭建快速和功能点覆盖完备的优点。

## 引言

Cache（高速缓冲存储器）是存在于处理器核与主存之间的存储器，在多核的处理器系统当中，当多个 Cache 包含同一块数据时，如果其中任意一个 Cache 修改了该数据块而没有通知其他的 Cache，就会产生数据不一致的情况 [1]。Cache 一致性就是维护多个 Cache 数据的一致性，Cache 一致性协议是多核处理器系统的核心，因此 Cache 一致性的验证是一项非常重要的工作。

现阶段，Cache 一致性的验证一般采用软件模拟的形式，但随着协议复杂性的增加，验证中需要覆盖的状态与路径成几何倍数增加。同时，访存数据在经过片上互联网络写入主存时要经过较长的路径，需要对流经网络的数据正确性进行检查，验证环境的复杂程度越来越高。在验证环境搭建与验证覆盖率收集方面，验证人员往往需要投入大量的精力，导致 Cache 一致性验证周期耗时较长。

## 验证环境结构

为缩短验证周期，提高验证的覆盖率，本文基于 Cadence 公司提供的 VIP（Verification IP，验证 IP）搭建多核 SOC 系统数据一致性验证环境，采用 UVM[2]（Universal Verification Methodology，通用验证方法学）方式实现，具有良好的可重用性，便于其他项目的继承与扩展。

由于所使用的 VIP 为标准 CHI 协议接口，而在待验证 SOC 芯片中采用一套自主设计的片上互联协议，因此在验证环境搭建时需要加入一个协议转换桥，以实现 CHI 协议与自定义互联协议的相互转换。验证系统整体结构如图 1 所示。

CHI VIP 可以实现对 CHI 协议中 RN（Request Node）节点、HN（Home Node）节点以及 SN

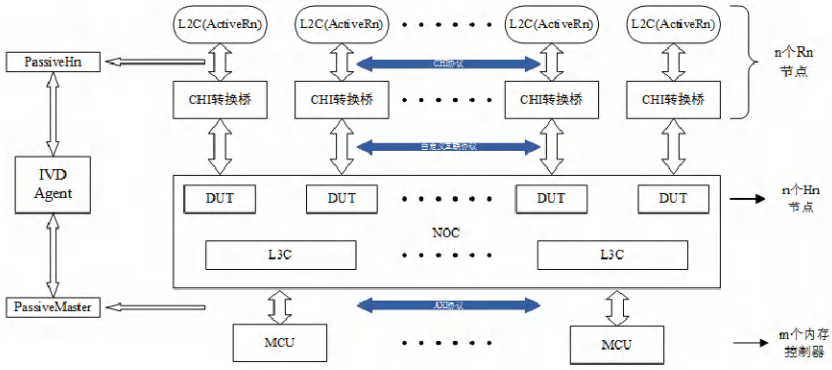



图 1 NOC 验证系统结构

（Slave Node）节点的验证，如图 1 中，DUT（Design Under Test，待验证设计）为 NOC（Network On Chip，片上互联网络），作为一致性协议中的 HN 节点，验证环境中使用 CHI VIP 配置生成 Active RN 节点向 DUT 发送请求激励报文，模拟处理器芯片中的 L2C。DUT 向下连接 MCU（Memory Control Unit，内存控制器）的接口为标准 AXI4 接口，连接作为 Passive Slave 的 AXI VIP 以收集写入主存的具体数据。IVD VIP 将 CHI VIP 中 PassiveHn 收集的 L2C（VIP Active RN 节点）的 CHI 报文作为 DUT 的输入内容，将 AXI VIP 收集的访存读写数据作为 DUT 的输出内容，对输入输出相关联的报文进行比对，以验证数据在经过 DUT 后的正确性。同时，IVD 对 DUT 在一致性维护中的 Snoop 行为进行监测，进一步确保系统的数据一致性。

多核 SOC 系统的片上互联网络具备良好的扩展能力，以满足多样化的功能需求。在分层验证过程中，经常需要围绕片上互联网络构建各种规模子系统验证环境，以加快验证进度。因此，在搭建验证环境时，同样需要考虑良好的可扩展与可配置性，可以根据不同的验证规模配置为不同的 RN/HN 节点数，并且可以与其他模块的验证环境进行整合。使用 VIP 搭建的验证环境具有良好的可配置性，可以根据实际需求调整验证环境行为，以满足自定义互联协议的验证需求。

## 验证实施流程

根据上述验证系统的整体结构，在搭建验证环境前首先开发 CHI 协议转换桥，以实现 VIP 与具体 DUT 的兼容；然后采用 CHI VIP 搭建 CC（Cache Coherence）子系统验证环境，并参照具体设计规范调整 VIP，确保 VIP 正确模拟 RNF 节点功能，处理一致性协议相关事务；最后接入 AXI VIP 与 IVD VIP，配置地址映射关系与 IVD 比对策略，收集访存数据并进行数据一致性验证。

### CHI 协议转换桥

为确保 CHI VIP 能够应用于非 CHI 片上互联协议的验证环境中，需解决自定义互联协议报文与 CHI 报文的转换。为此，本文开发了 CHI 协议转换桥。

协议转换桥主要功能包括：各个通道的信用控制及相关信号的转换、标准 CHI 报文与自定义互联协议报文中各个域段的匹配、数据报文的拆解与合并、Snoop 操作的事务 ID 重分配等。

CHI 协议转换桥的开发使得 VIP 在非 CHI 协议片上互联网络的 Cache 一致性验证的使用成为可能，极大的提高了标准协议 VIP 对自定义协议设计的兼容性，对验证自定义互联网络有着很大帮助。

### CC 子系统验证

在进行系统级数据一致性验证前，首先对 DUT 的 cache 一致性事务流进行验证，确保 CHI 协议转换桥和 DUT 对协议的处理流程正确。搭建 CC 子系统验证环境时需重点考虑验证环境的可配置性，以应对各种规模的验证需求。CHI VIP 中 ActiveRn 与 PassiveHn 均采用数组的形式实现，通过宏定义控制环境中例化的 RN/HN 节点个数。在接口连接方面，由于不同设计规模存在不同的硬件层次结构，VIP 与 DUT 连接的接口通过 Python 脚本生成，减少人为错误的引入，加快验证环境搭建速度。

CC 子系统验证环境结构如图 2 所示，为更加充分的验证全芯片真实的访存操作场景，验证环境中除使用 CHI VIP 模拟 L2C（RN-F 节点）向 DUT 发送一致性请求外，还加入一个成熟的验证组件模拟 I/O 设备（RN-I 节点）的 DMA 访存操作。

在 UVM 验证环境搭建过程中，如果希望将多个不同部件的环境进行融合，以实现更高层次的子系统级验证，需要对各个环境中的 ENV、TEST 顶层甚至激励的编写进行调整。在多个环境的融合过程中往往会引入额外的问题，延长调试时间，不利于各个验证环境的分离及模块化组合。鉴于 UVM 验证环境中并未限制 uvm_top 下的叶子节点个数，可将 VIP 验证环境的 TEST 顶层与 DMA 验证环境的 TEST 顶层均通过 factory 机制指定其父节点为 uvm_top，以此来减少对验证环境的不必要调整，将各模块已有环境直接组合为子系统验证环境，如

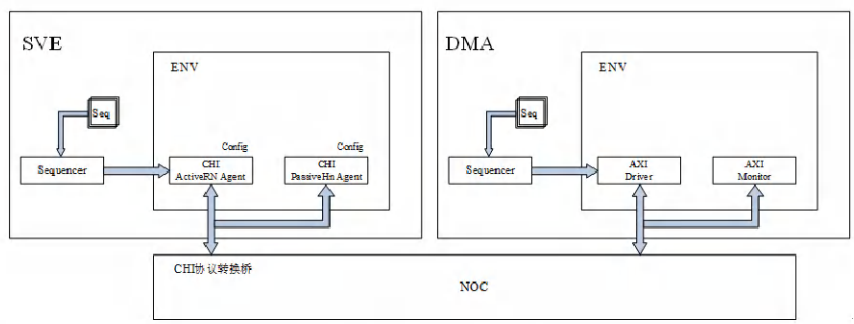



图 2 CC 子系统验证环境结构

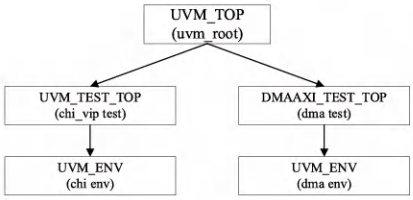



图 3 CC 子系统验证环境双顶层结构

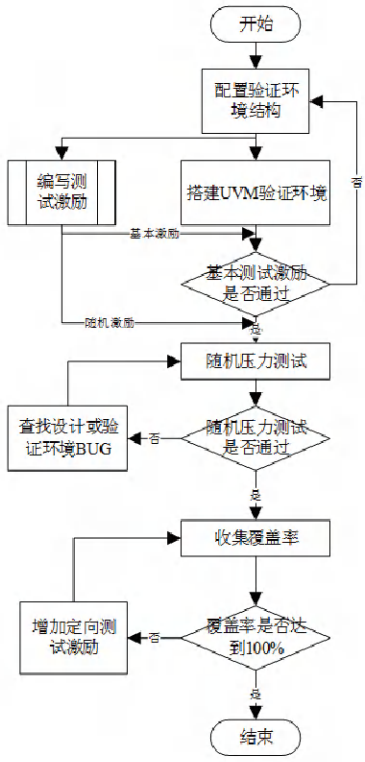



图 4 CC 子系统验证流程图

图 3 所示。

建立双顶层结构后，为保证各模块原有验证环境可继续独立运行，通过添加宏开关 DMA_AXI_RUN 来控制各环境是独立运行抑或是在子系统环境中运行。通过添加 +UVM_DMA_TESTNAME 来指定 DMA 验证环境需要运行的测试激励。

验证环境搭建完成后，按照验证计划以覆盖率为驱动逐步推进验证工作。为尽快达成验证覆盖率目标，这里采用 VIP 提供的 CHI 协议覆盖率模型，其良好的完备性对于整个验证工作的推进有着重要的指导作用，验证的具体实施流程如图 4 所示。

验证环境调试正常后，验证工作将主要集中于测试激励的开发。由于验证规模的不同，测试激励的编写也不尽相同。特别是随机压力测试激励，均采用参数化的形式进行，在配置为不同的 RN/HN 节点时不需要修改测试激励。激励开发采用基本测试激励、随机压力测试激励、定向测试激励的思路进行。其中基本测试激励包括各类型请求的生成及合法 Cache 状态构造；随机压力测试包括请求类型随机、地址随机等；定向测试激励在收集覆盖率之后进行，主要针对尚未覆盖的场景及特定功能进行定向测试。

## IVD 数据一致性验证

在 CC 子系统验证环境搭建完成并且基本测试激励通过后，着手搭建基于 IVD VIP 的子系统级数据一致性验证环境。IVD VIP 在进行数据一致性比对时需要明确数据流的输入与输出方向，当 ActiveRn 的访存数据经 CHI VIP 的 PassiveHn 接入 IVD 后，IVD VIP 通过配置的映射方式监测访问 MCU 的 AXI 接口数据，判断输入数据与流经 DUT 的输出数据是否一致，并在仿真结束后检查所有读写请求是否均已完成数据比对，IVD 可以监控多个输入输出端口，可以实现子系统的数据一致性检查。加入 IVD 后的验证环境结构如图 5 所示。

在基于 IVD 的验证环境搭建过程中，由于 DUT 中自主设计的片上互联协议与标准 AMBA 协议存在差异，因此需要对 IVD 的行为进行调整，使其与真实设计的行为相吻合。主要的调整包含以下几个方面：

（1）Snoop 行为调整。DUT 作为 HN 节点，向 RN 节点发送 Snoop 请求操作，但其具体行为与标准 CHI 协议存在差异，首先 DUT 不会进行 Snoop 的广播，只对存在副本的 RN 节点发送 Snoop 请求；其次，根据待验证 SOC 芯片中真实 L2C 与 NOC 的设计实现，某些 Snoop 操作行为与标准 CHI 协议不同。基于上述差异，需要使能 IVD 当中的 SnoopFliter 与 SnoopToInitMaster 等功能，调整 IVD VIP 对 Snoop 操作的检查，使其可以与 DUT 行为相匹配。

（2）Cache 状态调整。首先在待验证 SOC 芯片当中不支持某些 cache 状态，在进行随机测试时需要对其进行屏蔽。另外由于上述 Snoop 操作修改带来的 cache 状态变换需要使用 UVM 中的 callback 函数对事务包进行修改。例如 ReadShared 在触发 Snoop 操作时，按照 CHI 协议应为 SnpShared，当监听 UC 态时会将其修改为 SC 态，而在 DUT 的真实行为中 ReadShared 触发 SnpCleanShared，其监听 RN 节点 UC 态时并不会修改为 SC 态，造成 IVD 报错。通过调用 callback 函数对上述场景进行判断，将监听的 UC 态修改为 SC 态以保证 DUT 的正常运行。

（3）添加地址映射。IVD 在进行数据比对时默认通过事务 ID 判断输入数据及相对应的输出数据，然后对其正确性进行检查。但在 DUT 当中输入的 CHI 报文与输出的 AXI 报文两者的

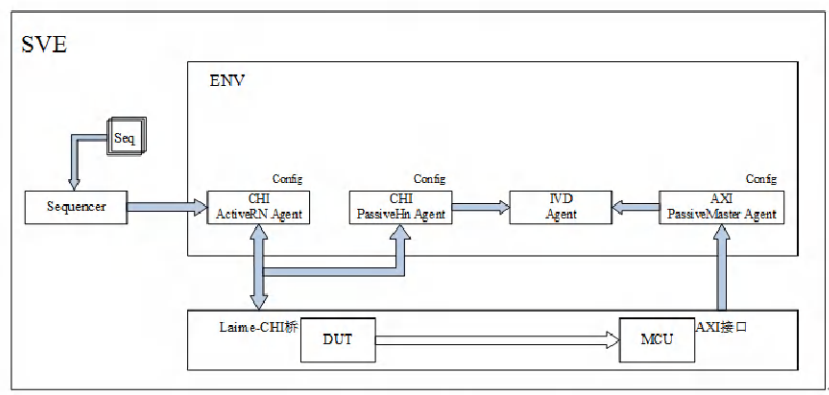



图 5 子系统数据一致性验证环境结构

ID 之间并无关系，而两者的地址信息存在确定规则的映射关系，因此需要调用 IVD 当中地址映射函数，明确输入地址与输出地址的关系，以便工具可以正确匹配输入与输出数据包，完成数据一致性检查。

在进行数据一致性验证中，由于加入了真实 MCU 的 RTL 代码，其在进行正常数据读写前需要较长时间的初始化。为缩短每次仿真运行时间，使用仿真工具的 save/restart[3] 功能，在初始化结束后保存仿真状态，恢复该状态后可加载新的测试激励继续进行一致性相关功能点验证。这样即可省略后续测试时漫长的初始化过程极大地缩短验证时间，提高验证效率。其原理如图 6 所示。在 UVM 验证环境中，由于不同 phase 的调动时间不同，可以在 configure_phase 完成初始化后保存仿真状态，之后通过更换不同的测试激励实现仿真的再次启动。

## 验证成果

采用 CHI 与 IVD VIP 搭建验证环境，相较于完全由验证人员自己开发的 BFM（Bus function model）及验证环境，有以下几个突出的优点：

（1）可以极大的缩短验证环境的开发时间，提升验证效率。一个验证环境若从零开始搭建到功能逐步完善，往往需要数月的时间，而在采用 VIP 后，时间大幅缩短，使得工程师能够专注于 DUT 的功能验证，提升 BUG 定位能力。

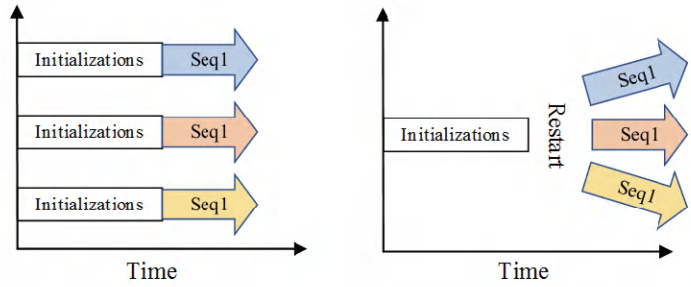
（2）VIP 中的检查机制更为全面与细致，可以完整记录每个事务包的处理流程，对于出现问题的报文可以做到其全流程的完整追踪，极大的方便了错误调试。

（3）针对 Cache 一致性相关协议，由于存在众多的场景与状态需要验证，VIP 提供的覆盖率模型更加完整，对于验证的快速收敛有着极大的帮助。

在本文所述验证环境中，由于所选 DUT 并非全新设计且在采用 VIP 进行验证前已使用自主搭建的验证环境进行了完善的功能验证，DUT 趋于稳定，因此采用 VIP 后并未发现很多设计 bug，但对整个项目有如下两点重要贡献：

（1）完整的构造出所有合法 cache 状态并完成所有类型的请求验证，为之后项目的顺利进行提供方向。方便的构造出之前验证中很难出现的 UPD 态，并完成包含 WriteCleanPtl 和 WriteBackPtl 报文的随机压力测试，而之前对于此类型报文均只能够进行定向测试；

（2）借助 VIP 强大的随机压力测试激励，在系统验证后期发现一处隐藏很深的设计 bug，阻止了该 bug 逃逸到硅后而造成的重大损失。




(a) Save/Restart 实施原理　　(b)UVM 环境中实现 save/Restart 功能

## 总结

本文所述采用 VIP 搭建的全局数据一致性验证环境，为复杂的 cache 一致性验证提供了良好的解决方案。验证环境均采用模块化的形式搭建，可以通过配置完成不同规模的验证要求，同时采用 CHI VIP 与 IVD VIP，可以实现从模块级到子系统级甚至系统级的数据一致性验证。利用 VIP 强大的可配置性和完善的信息输出，实现了对自定义互联协议片上网络的验证，同时极大的改善了一致性协议调试能力，提高了验证效率。基于本文所述的验证方法与验证流程，为之后项目中 Cache 一致性相关验证的开展提供了宝贵经验。

## 参考文献

[1] 王振江，周恒钊．一种验证 Cache 一致性协议的装置及方法．

[2] 张强．UVM 实战 [M]．机械工业出版社，2014.

[3]Save Restart and Dynamic Test Flows in UVM[R].Cadence, 2020.

作者简介：

范君健（1993-），男，硕士研究生，主要研究方向：微处理器设计与验证

晁张虎（1989-），男，硕士研究生，主要研究方向：微处理器设计与验证

杨庆娜（1986-），女，硕士研究生，主要研究方向：微处理器设计与验证

(a) Save/Restart 实施原理

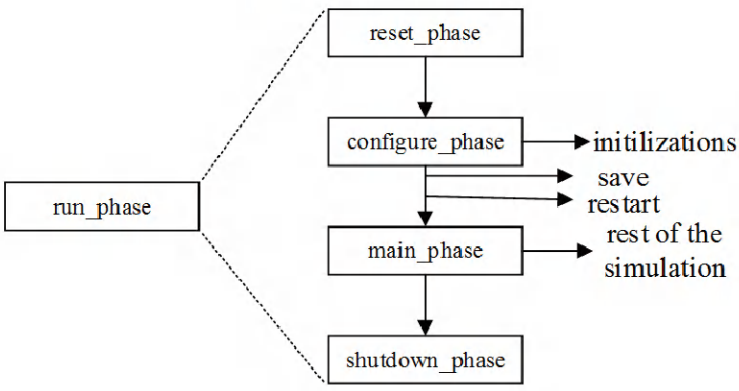



图 6 采用 Save/Restart 实现仿真保存与再次运行

# 为什么IP-XACT对当今复杂的设计如此重要?

Ranjit Adhikary, Magillem SA

半导体设计公司使用 IP-XACT 已有十多年的历史。但是最近，一些大的和小的公司，包括学术和研究公司，已经开始使用 IP-XACT 来开发他们的 SoC 设计。为了理解诸如 ST Microelectronics、NXP、Texas Instruments 等公司为什么开始使用 IP-XACT，有必要了解设计团队在开发 SOC 时面临的挑战。

SoC 设计不再孤立地开发。软件、固件、硬件和验证设计者必须有效协作，以确保 SoC 的开发及时并按规定正常工作。如许多公司所认识到的那样，为了确保成功的 tape-out，有必要采用新的方法。

从硬件的角度来看，设计团队已经复用 IP 一段时间了。但是随着 IP 的日益复杂，管理它们的硬件和软件配置并在整个产品生命周期中跟踪它们变得非常困难。虽然有一些软件解决方案在一定程度上解决了这一问题，但它们对专有技术的依赖以及无法与原有流程共存给许多公司带来了问题。

在过去的五年中，许多公司努力解决这些问题并实现流程自动化，同时将开放标准作为底层基础设施，并确保所有团队之间可以利用通用数据模型。大多数企业选择 IP-XACT 作为基础标准来开发自动化流程，这并不仅仅是巧合。

## 什么是 IP-XACT？

IP-XACT 首先由 SPIRIT Consortium 发布的标准，其唯一目标是在设计社区内促进 IP 的可重用性。它使 IP 提供商能够为组件和设计提供可读和可机器处理的 IP 的单一描述，并与其他所需的数据一起分享给 IP 用户。IP-XACT 还描述了系统设计和 IP 之间的互连以及其他细节，如地址映射、接口等。提供了一个通用的设计表示，可供 IP 供应商、设计集成商和 EDA 工具提供商在其流程内进行交换。

IP-XACT 于 2009 年成为 IEEE 标准，并作为 IEEE-1685 发布。许多公司甚至在它成为 IEEE 标准之前就开始使用它，但随着越来越多的公司意识到它在帮助创建和自动化定制设计流程方面的潜力，这种使用在过去几年开始增加。

## 为什么对 IP-XACT 的兴趣突然增加?

为了在市场上推出新产品并在全球范围内竞争，并确保设计成本低，无论是小型还是大型半导体公司，都必须确保在预定的时间内成功地进行 tape-out。设计流程中的任何延迟都可能影响他们的上市时间和公司的利润。

大多数设计团队试图通过在多个方面并行工作并在模块级和系统级验证上投入大量资金来解决这个问题。例如，顶层和模块级的设计集成与固件、RTL 和验证环境的开发并行进行。但这种方法并不是最理想的，通常需要更多的资源，而且容易出现手动错误。

设计师面临的另一个问题涉及到由许多供应商生产的 EDA 工具，其中许多使用独特和专有的格式。开发人员经常面临如何在不同的设计环境之间有效地交换设计信息的问题。

解决这一问题并确保及时、成功地进行 tape-out 的一种方法是提供一种解决方案，其中包括：

- 适合您的定制需求的设计方法和 EDA 工具
- 设计团队之间的高效设计协作，有时在不同团队之间，尤其是硬件和软件团队之间
- 利用内部和第三方 IP 的 IP 重用
- 设计流程自动化，确保
  - o 更快的设计集成
  - o 选择正确的 IP 配置
  - o 不同工具之间设计信息的顺利交换，确保团队之间的设计交接
  - o 避免对设计规范（如寄存器映射图）的误解
  - o 自动生成 RTL 和其他辅助文件，如 C 头文件、存储映射、UVM 模型、文档等。

过去，许多公司试图通过创建基于自定义脚本、专有技术或两者结合的解决方案来解决这些问题。这种方法的挑战在于，解决方案需要不断维护，并且在管理解决方案的工程师离开公司时往往会崩溃。通过创建定制生成器来配合使用 EDA


socionext™
for better quality of experience

工具并对结果进行反向注释等来集成设计流程的能力，使得很多公司现在不得不重新审视 IP-XACT 作为其工具解决方案的基础设施。IP-XACT 是 IEEE 标准中的佼佼者，这意味着公司不再需要担心维护或增强任何专有基础设施。通过提供标准化的数据交换格式，IP-XACT 能够灵活地表示多种需求，并允许自动提取设计信息并用于流程自动化和高级验证。

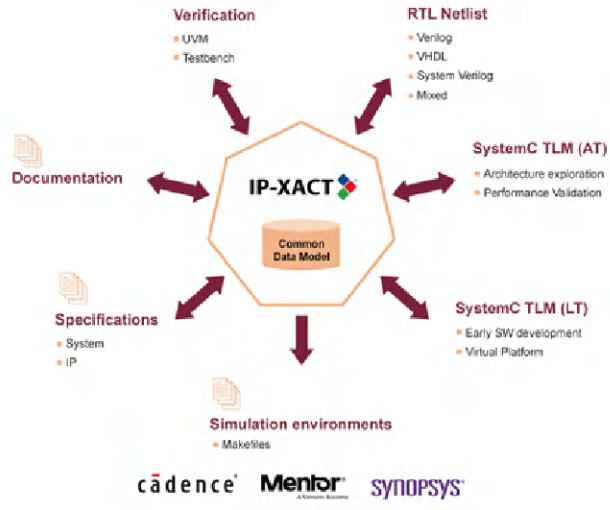
IP-XACT 标准的一个重要价值是它能够将设计打包到 IP-XACT 组件中。组件描述包括每个 IP 块的外围规范以及总线接口、物理信号、它们到逻辑总线接口的映射、配置、地址块、寄存器描述、文件集和文档信息。设计人员可以利用描述中包含的信息，在单一的集成设计和验证环境中自动集成正确的 IP 配置，更快地构建 SoC，同时减少设计中引入错误的可能性。

使用 IP-XACT 的优势在于它不仅有助于改善公司内部的 IP 生态系统，因为设计团队可以轻松地将设计与必要的设计信息打包在一起，而且它作为一个通用的数据模型的使用也使分布式团队能够更有效地协作，并在不同的设计环境之间快速地交换设计信息。IP-XACT 还配备了一个标准 API，可以通过软件来进一步定制解决方案。例如，API 可以与 EDA 工具一起使用，通过利用 IP-XACT 数据库中可用的设计信息，实现与客户流程交互。使用 API，利用生成器，并用于捕获生成器内的配置智能，以自动生成 IP 的最终配置 IP-XACT 描述。这项功能对于 IP 提供商来说是非常有价值的，因为它能够精确和受控地使用所选配置。

IP-XACT 标准的多功能性及其与其他系统（包括用于 IP 重用和流程集成的现有流程）共存和工作的能力使其成为许多公司的最佳选择。

## 使用 IP-XACT 的优势

IP-XACT 最重要的一个方面是它是一个由领先的半导体公司支持的 IEEE 标准，这些公司投入巨资将其用于工具和 IP 重用。事实上 IP-XACT 的开发始终牢记 IP 重用，这使得在企业内部构建 IP 生态系统非常理想。




设计团队可以利用这个生态系统来创建更多的 IP 子系统和 SOC。为了更快地组装设计，设计者可以使用 IP-XACT 中定义的连接特征，为他们的设计快速创建互连结构，并利用 IP 的寄存器映射来计算设计的完整系统存储映射。设计者还可以使用设计数据库来生成寄存器 C 头文件，产生 VHDL、Verilog、System Verilog 或 System C 格式的网表、UVM 模型、测试平台、文档等。

IP-XACT 的一个鲜为人知的优点和最重要的功能之一是，它可以广泛用于工具化和流程自动化，许多公司最近开始利用这一点。

IP-XACT 拥有的其他一些功能包括

- IP-XACT 是为 IP 重用而设计的
- 更快、更轻松的系统集成
  - o 对多层抽象（设计和协议）的支持使集成者能够快速为设计创建顶层。
  - o 内置错误检查可降低出错的可能性
- 可扩展性以添加设计和流程信息
- 通过对视图 / 文件集等功能的支持，可交付成果的管理变得简单且完全自动化。
- 支持设计可追溯性，这是 ISO 26262 认证的关键要求

一个标准不一定是完美的，但如果随着时间的推移有足够多的人采用它，它就可以被认为是一个好的标准。这也适用于 IP-XACT。随着采用该标准的公司数量稳步增加，毫无疑问，该标准将继续存在。

## 找到正确的解决方案

为了加快 SoC 或 IP 的开发过程，有必要使用经过尝试和测试的解决方案，这些解决方案是多家公司标准流程的一部分。有关如何使用 IP-XACT 更快地构建设计的详细信息，请访问 www.magillem.com 或者联系 qian.wang@magillem.com 。Magillem 的客户包括全球排名前 20 位的半导体公司。

Magillem 是一家领先的半导体解决方案供应商，旨在为行业提供颠覆性的解决方案。设计公司可以使用他们提供的解决方案更快地实现自动化设计流程，并成功地降低设计成本。

它也是 IP-XACT 标准的权威机构之一。Magillem 是 IP-XACT 2021 Accelera 委员会的联合主席，自 IP-XACT 标准成立以来一直是积极的成员。

四川和芯微电子股份有限公司
IPGoal Microelectronics(Sichuan)Co.,Ltd.

# IPGoal助您用芯胜出

## 专研16年，做高性能数模混合IP设计专家

sales@ipgoal.com www.ipgoal.com

**IP及定制服务**

为客户提供经过批量生产验证或硅验证的IP产品，可根据客户要求量身定制。

**SoC设计服务**

凭借丰富的IC设计经验、多样化的IP产品及紧密的产业链合作关系，为用户提供完整的一站式SoC/ASIC设计服务。

**芯片封测服务**

提供高效率、低成本的定制化一站式芯片封装测试服务及解决方案。

# ARSIM:基于C/C++模型的SoC验证工具

Ashraful Islam, Moazzem Hossain, Bob WangASA 微系统有限公司

## 摘要

对于任何 SoC 来说，从概念到生产都要经历一个复杂的设计周期。硬件和（ 应用 ）软件必须一起工作，为一个期望的 SoC 产品。尽管嵌入式 SoC 在复杂性、规模和功能方面不断增加，但上市时间却在缩短，目前 IP 和 SoC 的验证流非常复杂，是设计周期持续时间、设计成本和硅成功的主要决定因素。为了缩短设计周期，使验证过程缩短，引入了 ARSIM。

关键词 :SoC 验证，基于周期的验证工具，基于 C/ C++ 模型的验证工具。

## 介绍

随着设计复杂性的增加，验证的范围也在演变，不仅仅包括功能。SoC 的验证过程被认为是设计生命周期中非常关键的一部分，因为设计中的任何严重缺陷在被流片之前没有被发现，将导致显著的上市时间延迟，并可能增加数百万美元的设计成本。验证的主要目标是在流片之前确保设计功能的正确性。

ASA Microsystems 一直致力于工业上最小的脚印 RISC-V 处理器核心，具有最低的功耗和最高的性能。ASA RISC-V 核心之一是 AR32Z。它在 FPGA 和 ASIC 实现中被证明是性能最高、功耗最低的核心。AR32Z 可以在 28nm 或更小的进程节点上实现千兆赫 + 频率，而所用处理器的大小只是现有处理器的一小部分。基于 AR32Z SoC 的应用是嵌入式系统，AI 处于边缘，以最低的运行功率获得最高的性能是实现的重要标准。

虽然 ARSIM 有内置的 AR32Z 处理器作为 SOC 模拟的一部分，客户可以使用其他 RISC 处理器在 ARSIM 中使用。正如在后面的章节中提到的，ARSIM 有许多内置的 IP C/ C++ 模型，客户可以为他们的专有或在 III 引入 C/ C++ 模型 一方 IPs 或带来的 HDL 和 ARSIM 可以自动转换 HDL 代码为 C/ C++ 模型。

## 相关的工作

在之前的研究中，已经引入了一些仿真工具，如 OVPsim、Spike、Renode、gem5 等。OVPsim 是由 Imperas 开发和维护的多处理器平台仿真器，由开源仿真器、快速 OVPsim 仿真器和建模 api 三个主要组件组成。它们是为易于编译具有复杂内存层次结构、缓存系统和嵌入式软件层的多核异构或同构平台而设计的，这些嵌入式软件可以在标准台式机上

以数百 MIPS 的速度运行。是指令准确，不是周期准确。Spike 是以 golden Spike 命名的 RISC-V ISA 模拟器，它实现了一个或多个 RISC-V 转换器的功能模型。它展示的主要特性包括多个 ISAs（RV32IMAFDQCV）、多个内存模型（弱内存顺序和总存储顺序）、特权规范、调试规范、多个 CPU 支持、JTAG 支持等。Renode 是 Antmicro 开发的开源框架，它可以可靠、可伸缩、高效地为包括 CPU、外设、传感器等在内的多节点设备系统构建、调试和测试软件。它的主要优势是完全确定性、调试透明和健壮、易于集成、具有附加功能的丰富模型抽象、模块化平台描述格式、自动化测试和 CI 集成。Gem5 仿真软件是通过合并 M5 和 GEMS 模拟器而创建的。它提供了灵活的，模块化的仿真系统，能够评估一个广泛的系统。

## ARSIM 是什么？

ARSIM 是一个基于循环的模拟器，用于建模和联合模拟 SoC 的硬件和软件，并提供了带有 RTL 仿真工具的 DPI-C 库接口，用于 RTL 验证。ARSIM 可通过 MATLAB、ANSYS 和 COMSOL 等高级仿真软件进行广泛的 SoC 产品仿真，包括 RF、高速 SERDES、MEMS 等。

## ARSIM 特性

ARSIM 允许使用实际应用程序进行自动早期系统架构分析。它支持在设计周期的早期开发应用程序和嵌入式固件。ARSIM 消除了 FPGA 映射之间耗费大量时间的迭代，运行实际的程序来发现架构中的缺陷，并返回到架构重新设计或架构修改。ARSIM 将验证周期减少了 50%。它还使硬件和软件的共同开发成为可能。在整个开发周期中可能使用相同的应用程序软件。可以使用 ARSIM 与 3 进行联合仿真一方 RTL 验证 / 模拟工具的硬件和软件验证。该工具可以直接生成可合成的模型，用于 FPGA 开发和原型设计，从而缩短开发周期。

## ARSIM 架构和组件

ARSIM 架构包含 3 个重要的组件来运行整个验证过程。

### RTL 到 C/C++ 的转换引擎

在大多数情况下，客户拥有 RTL 格式的 IPs。ARSIM 转换引擎可用于将客户 RTLs 转换为 ARSIM C/ C++ 模型进行 ARSIM 验证。

### ARSIM C/ C++ 模型库

ASA ARSIM 在模型库中提供了大多数必需的和通用的 IP C/ C++ 模型。它们包括 ASA RISC-V 处理器和 ASA 向量处理器，大多数公共总线结构，以及外设和计算 IP。其中大多数 IP 都是物联网 / SoC 系统开发所需要的。此外，客户可以添加他们的自定义或专有的 IPs 到 IP 库 SoC 系统设计和验证。

### ARSIM 验证引擎

这是 ARSIM 验证的核心。客户特定的 SoC 可以被动态构建，以使用作为 ARSIM 验证环境一部分的 IPs 和总线结构为特定的客户应用程序创建 SoC。一旦 SoC 构建完成，ARSIM 允许客户将应用程序 C/ C++ 程序加载到 ARSIM 中，运行应用程序特定程序，运行 SoC 系统的验证和分析。

## 结论

ARSIM 已经被测试为一个快速，用户友好，即插即用模拟器。这个独立于操作系统的工具比其他开源模拟器有更多的调试选项和开关。用户可以逐个检查指令的执行和寄存器和数据存储器的实时更新。

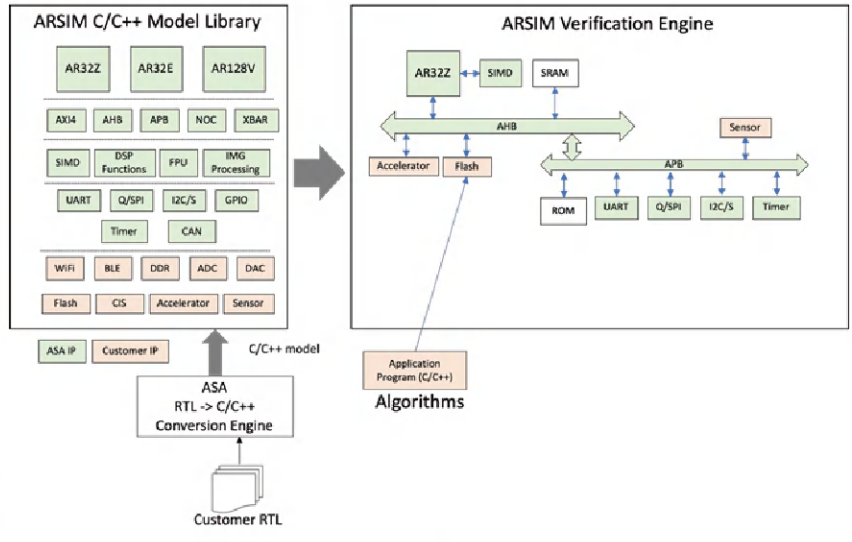



图 :ARSIM 架构及组件

# 迎接国产集成电路设计IP的春天

作者：潘中平 （芯动科技有限公司）

## 前言

回顾世纪之交的2000年左右，中国大陆吹响了发展本土集成电路产业的号角，本土的芯片代工厂相继在上海张江破土动工和投产，中国台湾及其它半导体产业先进地区运作多年的集成电路设计（Fabless）和芯片代工制造（Foundry）模式及其产业生态也在大陆兴起；但是，限于当时的集成电路工艺发展水平（0.18um主流工艺），致使大陆屈指可数的fabless公司面对这一产业新生态，在产品设计方法上基本还是基于传统ASIC设计为主。尤其是，当时集成电路设计知识产权（Design IP）不仅对非专业人士是个陌生的概念，即便对很多沿袭传统电子电路设计的从业人员而言也是新事物，对IP产品形态、交付项和授权使用规则等更缺乏实际体验。随着2000年后移动通信技术从2G向3G的演进，以及集成电路制造工艺向更先进工艺的发展（如2000～2010年代主流工艺从130nm，90nm向65/55nm演进），加上移动终端应用处理器需求带动了ASIC设计从单纯集成纯数字CPU内核，向集成包括接口类IP、存储类IP在内的更多模拟，数模混合信号设计的SoC（系统级芯片）演进。基此，一方面，Fabless设计公司把设计和复用IP的选择成为其必须面对的、几乎需要与Foundry工艺同时考量的关键因素。与此同时，Foundry厂商为打造芯片制造平台，在向客户提供成熟可用的工艺前（PDK1.0 ready前），也必须未雨绸缪地规划并开发验证基础性IP（如标准单元库，efuse，若干模拟IP等），且考虑引进并提前验证一些关键性第三方IP（除了仍然可能包括标准单元库/存储编译器IP外，一些诸如USB、DDR PHY etc、OTP/MTP NVM等关键性数模混合电路高速接口类IP，高精度模拟IP等也在考虑之列）以便导入客户SoC产品投片并实现量产。

## 1. 国产集成电路IP的发端及成长

### 1.1 SoC所用到的标准接口类IP基本特征

伴随着移动终端产品对计算性能更优，功耗更低的应用处理器SoC的需求的持续增长，以及其它消费电子产品应用需求的增长，除ARM公司处理器内核作为核心IP取得了普遍的运用外，一些外围接口电路IP如USB1.1/USB2.0，DDR2在2010年左右也开始推广运用。

但是与移动终端CPU处理器几乎是ARM公司一统天下不同的是，这些SoC所用到的标准接口类IP（如USB，DDR等）具有以下基本特征：

（1）任何有技术积累的公司遵循某种行业标准，都可以尝试开发自己的IP产品，类似ARM公司CPU核那样的市场垄断性并没有也难以形成。

（2）今日一些国外大牌IP厂商也是通过不断收购，兼并一些中小规模IP公司获得IP相应技术及产品，然后通过与其它设计资源如EDA工具整合，借助市场手段形成品牌效应。

（3）一些具有创新精神的本土创业企业，十几年前就先后尝试不同类型的设计IP研发，在实践中认识到未来采用IP核进行SoC设计是大势所趋，尤以一些冠以“xxxxSilicon”的创业公司为主成为率先服务国内fabless领先设计企业的设计IP先行者。

### 1.2 国产集成电路IP的成长动因

（1）IP设计公司与IP应用大客户的紧密结合，得到市场的认可及大客户量产芯片的迭代验证。应该看到，IP设计公司的IP定制化设计，经过在”xxSilicon”，“xxChip”等大客户的实际SoC产品磨刀石上锻炼，使它们定制化设计的一系列IP从成熟工艺向先进工艺演进过程中得以验证及产品磨砺，从而在如DDR，USB，SERDES，MIPI PHY等IP设计研发水平方面，对比国外大厂甚至在PPA参数方面形成较为明显的优势。

（2）IP设计公司与Foundry的紧密结合，实现SoC芯片量产。应该看到，针对不同的目标客户应用市场需求，基于自主技术积累（know-how），设计转化成IP形式、且在芯片设计的关键指标PPA方面做出优化设计及定制服务；尤其是，所设计的IP通过相应Foundry合作验证后，对照国外IP产品具有明显性价比优势，授权给fabless客户用于SoC设计，帮助更多本土fabless企业获得质量可靠、性价比高的IP。综上所述，通过Foundry实现SoC芯片量产是国产IP创新创业设

计公司获得快速成长的关键所在。

### 1.3 国产集成电路 IP 设计公司发展

在中国“国家集成电路发展纲要”全面贯彻落实下，国产集成电路 IP 设计公司获得较大发展，其中以两家“xxxxSilicon”为代表的集成电路高速接口类IP 已成为可以完全替代国外 IP 厂商产品的高质量，高性价比之选，且采用它们 IP 的客户产品正以每年数十万计的晶圆量产规模源源不断地从多个Foundry 发货交付客户。图 1 显示了 2001-2018 年间国产 IP 设计公司发展情况，具体表现：

1）2001~2003 年间。以中科龙芯、杭州中天微、苏州国芯、芯原微电子为代表的获得授权开发的国产 CPU IP 及设计服务公司为主；

2）2004~2009 年间。以武汉 / 苏州芯动科技、上海灿芯、四川和芯为代表的模拟及高速接口 IP 为代表；

3）2010~2015 年间。以成都锐成芯微、成都纳能、芯启源为代表的模拟 IP，IoT 及高速接口 IP 为代表的企业；4）2016~2018 年间。以寒武纪、阿里平头哥、芯来科技为代表的 AI 及 RISC-V CPU IP 为代表的企业。

## 2. 国产集成电路 IP 的市场及机会

### 2.1 国产集成电路 IP 设计公司的优势

（1）在 IP 授权商业模式方面。它们与国外其它IP 厂商交付的“标准 IP 交付项”对比，形成明显竞争优势。这从一些与国产 IP 领先企业”xxxxSilicon”合作经年在多个量产项目上获得成功的客户体会即见一斑。国产IP公司的IP开发交付更可以针对客户芯片应用需求的差异，提出特定的PPA定制需求，经过合作双方科学评估，在技术可行性许可的前提下通过风险共担，致力于在芯片面积，功耗方面进一步优化，与国外其它IP厂商的“标准IP交付项”方式相比，具有明显竞争优势。

（2）在 IP 开发方面，定制 IP，为客户芯片产品在应用市场上差异化竞争带来优势。而这些定制 IP需求的实现是国产 IP 公司技术，工程团队在与客户合作定制 IP 项目实践中历年淬炼积累的独特know-how，例如超低功耗设计技术，面积缩小的优化设计等。

### 2.2 国产集成电路 IP 设计公司发展的市场

今天，集成电路制造主流工艺已从 28nmCMOS平面晶体管制造工艺向 16/14nm 推进，随着 12/10nm、7/5nm 的立体晶体管制造工艺（FinFET）不断演进，每一颗 SoC 不仅需要集成 CPU，GPU 等数字处理器 IP 核，同时在一颗 SoC 设计上集成多颗数模混合类 IP 及存储器类已经成为主流。

图 2 显示了 SoC 芯片设计中所需的平均集成电路 IP 个数与工艺节点对照，鉴此，国内 Fabless 设计公司在选择 IP 时必然面临更大的成本压力及产品差异化竞争带来的定制需求，更需要与本土集成电路 IP 设计公司的战略合作，而技术上尤其在FinFET 工艺 IP 设计量产日益成熟的国产领先 IP 供应商”xxxxSilicon” 已经具备为本土 Fabless 设计客户提供高性价比的一站式接口 IP 的授权，可以明显降低客户整个 SoC 集成 IP 的成本。

图 2 中的数字、混合信号等 IP 数量的备注说明：

1）Digital IP 数量的计算包括标准单元库；

2）Mixed signal IP 数量计算包括 Analog IP；

3）所有 IP 数量的计算包括 hard-cores，soft cores；

4）Memory IP 数量按每一个 instance 计算一次。

### 2.3 国产集成电路 IP 设计公司发展的机会

图 3 显示了 2019~2027 全球集成电路设计 IP授权费营收预测。从中看出，全球 Design IP 营收将从 2018 年的 46 亿美元，发展到 2017 年的 101 亿美

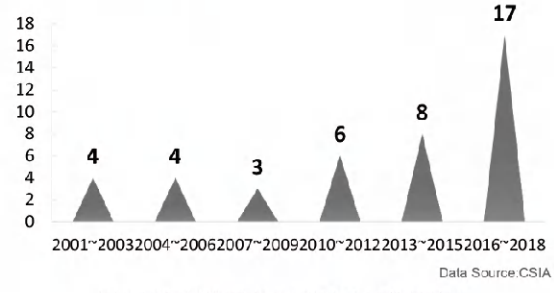



图 1 历年新增国产 IP 设计公司数量情况

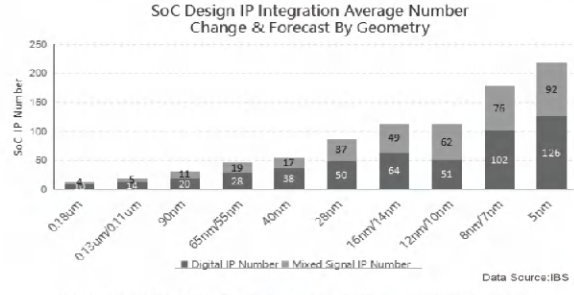



图 2SOC 设计平均集成电路 IP 个数与工艺节点对照

元，10 年间翻了一番之多。这也展现了国产集成电路 IP 设计公司发展的机会。

图3中的数字IP营收预测备注说明：

1）Design IP 市场未来 10 年将保持比整个半导体产业平均增速高 10%；

2）据 IBS 等市场分析机构预测，Digital IP 在2009~2027 年间的年均 CAGR 预计将达 9%，其中：

A. CPU/GPU 等数字 IP 年均 CAGR 将达 10%；B. 混合信号类 IP 年均 CAGR 则有望达到 7%；

C. 射频(RF) 类 IP 年均 CAGR 则将超过 8%。

近年来，国产领先 IP 企业以质量稳定，高性价比，服务响应及时的优势，取得了不俗的业绩，享誉集成电路设计行业，成为众多领先 Fabless 设计公司的合作伙伴。为适应不断发展的 IP 市场需求，国产领先 IP 企业依然持续加强研发力度，强化项目管理责任，对标国际标准，采用国际先进高效的技术手段提高设计效率，强化品质管理，文档管理，目标是帮助客户在 IP 的授权使用，服务支持方面获得高性价比的优质体验；同时，对外则拓展客户合作渠道，扩大技术交流，分享国产 IP 设计成功应用的案例，服务产业，为中国集成电路设计产业发展持续努力。

## 3 结束语

集成电路设计 IP 是快速发展的半导体 / 集成电路产业的上游产业，据权威机构统计，其具有针对电子制造业产值高达 600 倍放大的“杠杆效应”；为此，美国出台了针对中国企业芯片设计采用技术源头在该国的 IP 不能超过 25%的限制政策，以制约中国芯片设计制造业的发展。毫无疑问，集成电路 IP成为中国大陆集成电路产业链与全球合作的关键环节，国家相继出台了从政策到资金扶持本土集成电路产业的优惠政策(见图 4)，其中集成电路设计 IP及 EDA 工具作为国家基础产业环节的重要性得到充分的重视。

随着 5G 时代的来临及人工智能 AI/IoT 应用的需求，我们有理由相信集成电路产业必将迎来又一轮发展高潮。而 AI 时代应用的特点就是智能化、多样化、个性化；国产 IP 多年来不仅与全球 IP 业界领先的设计 IP 厂商（如 CPU/GPU IP、模拟 IP 及存储IP 公司等）建立了良好的战略合作关系，也通过 IP定制设计服务积累了包括芯片面积优化、超低功耗等独特技术积累（know-how）。这些似乎是针对 AI/IoT 应用的芯片设计需求有备而来，实际是研发团队将客户需求置于首要的工作目标，敢为人先，勇于探索的创新精神，工匠精神的具体体现。

通过十几年来与多家 Foundry，以及包括国际级大客户项目的合作，国产 IP 设计领先企业芯动科技不仅紧跟国际集成电路产业工艺演进的节奏，实现了全系列自主知识产权高速接口 IP 开发；同时，在多家 Foundry 的多个工艺节点（如成熟工艺 0.18um/0.13um,65/55nm 及相对先进工艺 40nm，28nm 上，以及 FinFET 先进工艺 16/14nm）得到验证，与 Foundry 工艺紧密绑定实现国产 IP 被众多本土及境外Fab-less 客户采用并实现大量量产；与此同时，其混合信号集成电路 IP 设计能力正在帮助并促进本土 Foundry 最先进工艺优化加速实现 IP 验证的进程。

其中，国产高速接口 IP 供应商芯动科技开发的IP 如 GDDR6 PHY 在 FinFET 先进制程上率先于全球实现量产，而 32GHz 以上的高速 SERDES PHY IP 也在 FinFET 上获得验证正一站式推出。毫无疑问，国产集成电路 IP 产业的春天来了，春天是百花齐放的季节，不论源于国外的，本土创新的集成电路 IP企业一定都会在中华大地这片创新的沃土上撒下创新的种子，与众多本土 ASIC/SOC 设计企业一起努力克服中外贸易纠纷可能引发的集成电路 IP 限制的挑战，实现中国芯片设计制造业的创新及跨越发展！共同谱写 AI，5G 时代芯片设计的新篇章！

**附件：英文术语的关键词注释：**

集成电路设计 IP：指具有明确技术规范具有可验证的特定功能且拥有独立知识产权可授权给包括Fabless 设计公司在内的客户集成使用的电路设计模块；

Foundry：指专注集成电路制造的代工厂，如 TSMC，UMC，SMIC 等；

Fabless：指无晶圆集成电路设计公司为主的自身不拥有 IC 制造厂的单位；

AI:ArtificialIntelligence 人工智能；

SOC:System-On-Chip 系统级芯片；

NVM：指非易失性（Non-Volatile）存储器；

PPA：PerformancePowerArea——指芯片设计的性能功耗面积参数指标；

PDK：Process DesignKit——指由 Foundry 针对特定工艺开发的设计套件。

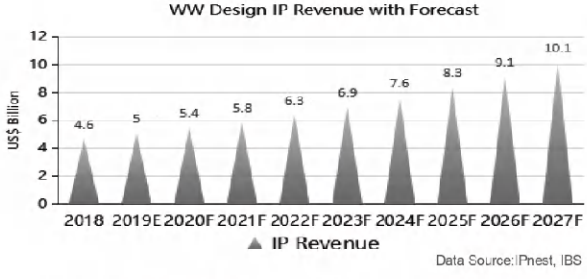



图 3 2019~2027 全球集成电路设计 IP 授权费营收预测

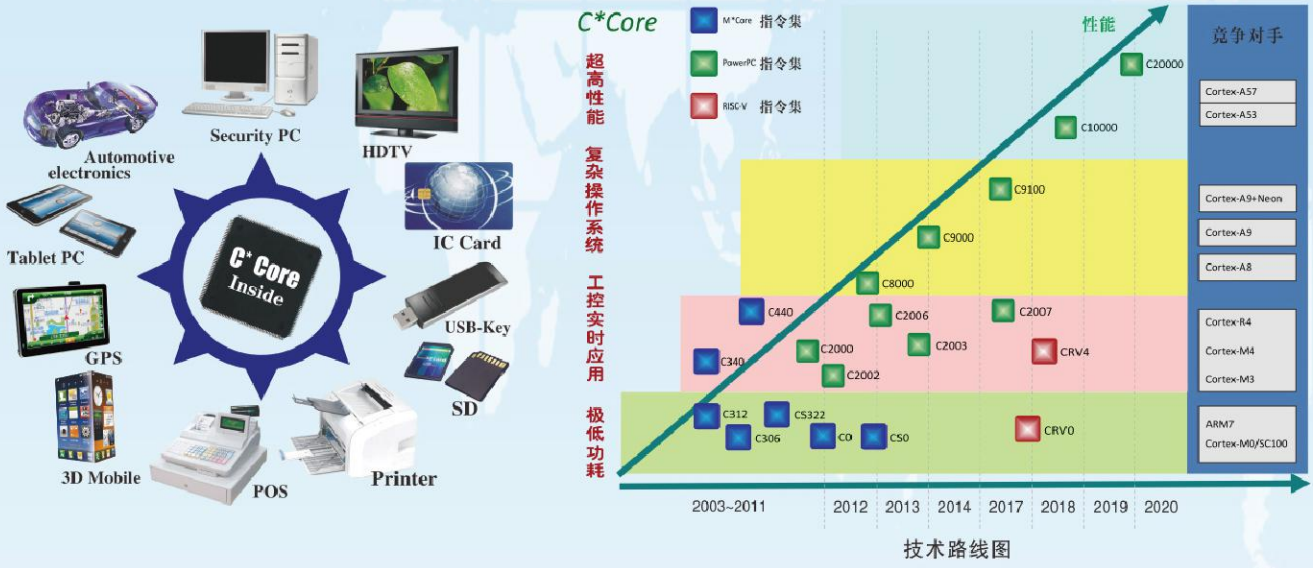

信息来源：《中国集成电路产业发展白皮书》

图 4 国家集成电路产业发展推进纲要

C*Core®
C*Core Technology Co.,Ltd.

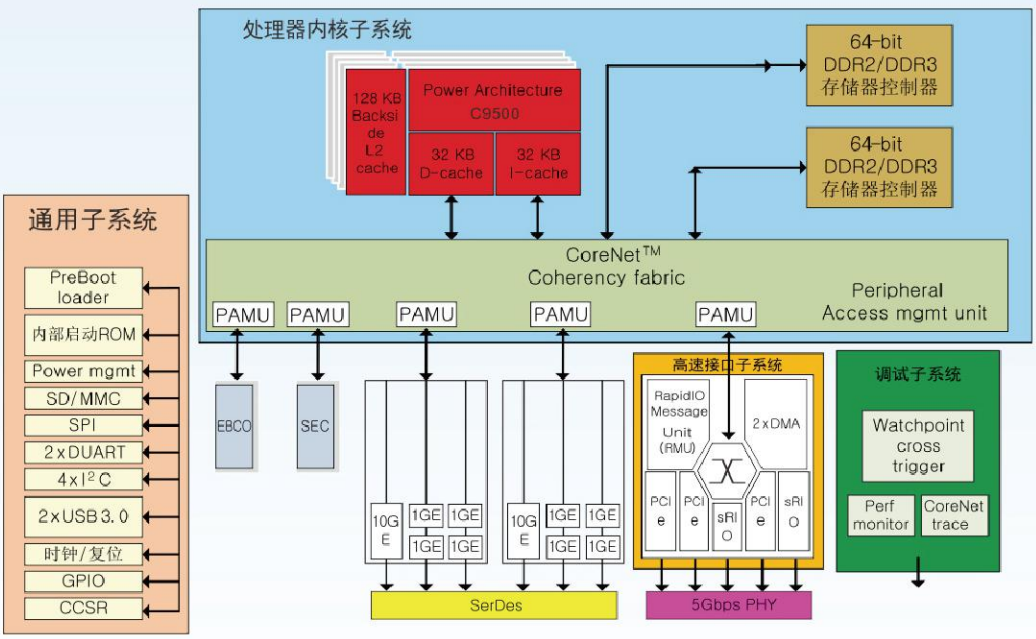
# 公司简介

苏州国芯科技股份有限公司是领先的国产化CPU IP和IC设计服务供应商，公司引进IBM PowerPC系列CPU及指令集架构授权和飞思卡尔（原摩托罗拉）先进水平的低功耗、高性能32位RISC嵌入式CPU技术及其SoC设计方法；以高起点建立苏州国芯自主产权的完全兼容PowerPC架构及M*Core架构的系列C*Core CPU。




技术路线图

高性能SoC设计平台CSOCH2040，基于苏州国芯自主知识产权的C*Core 32位高性能信息安全处理器C9100MC，支持ISA V2.05指令集架构（Power Instruction Set Architecture），兼容NXP E500MC核。




高性能SOC设计平台CSOCH2040

# 智能硬件如何提升您的数据中心

## 高性能IP模块可卸载网络和安全处理

云计算得到了前所未有地蓬勃发展，新型的主机应用程序通常被设计成可为数百万个客户端提供服务的高性能架构，并且使每一个客户端都能获得高速的服务、最小的延迟和最有效的安全保障。但是这些数以百万计的连接可能导致数据中心的服务器过热并宕机。

## 云计算正以前所未有的速度在增长

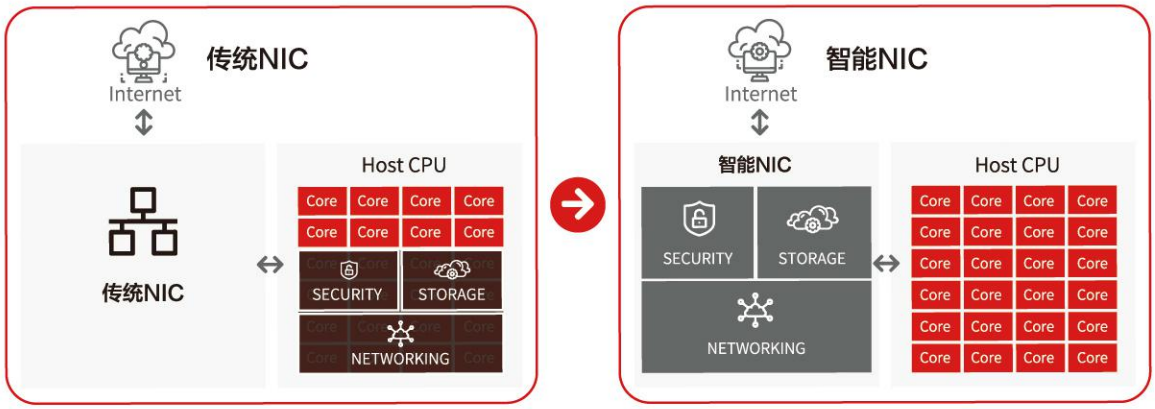
目前用户需要用大量的时间来管理主机处理器网络流，而不是运行有效的应用程序。因此，将越来越多的网络和安全处理快速地卸载硬件成为了一种趋势，如安全加速器和智能NIC（智能网络接口卡）。这将释放主机处理器，使其能够更好地完成设计任务，并降低数据中心的所有权成本。

**将智能NIC引入数据中心来提供高速服务**

云服务器中的硬件卸载并不是全新的技术，在具有10Gbit/s访问权限的数据中心中，传统的NIC可能已经接管了一些网络处理功能，如校验和计算。

但现在有100Gbit/s和更高速的应用前景，结合云处理的爆炸式增长、新兴的 5G 革命以及虚拟化等新技术，这需要新的解决方案。在这种情况下，高效的加密加速器是必不可少的，传统的NIC正在发展成为智能NIC，可配置的网卡可以接管更多的网络处理功能。

加速器和智能 NIC 都可以作为 FPGA 板或通过专用的第三方 IP 模块作为 ASIC 实现。但是，这些模块必须来自可靠的合作伙伴，并且它们具有可扩展性、易于集成性，并且能够为将来的超高性能数据中心做好准备。




使用智能NIC解决方案可以释放应用程序的CPU周期

## 网络负载：网络结构和数据包的写照

计算机和应用程序之间的数据通信高度标准化，数据被切成帧和段，通过地址、簿记将完整、真实的信息进行加密和封装。数据通信是一个多层系统，其表面层处理物理位信号，第二层处理两台计算机之间的连接…仅最后一层处理实际数据。我们可以想象成在一张纸条上的数据，将其放入带有地址的信封中，然后将其放入第二个信封中，依此类推。

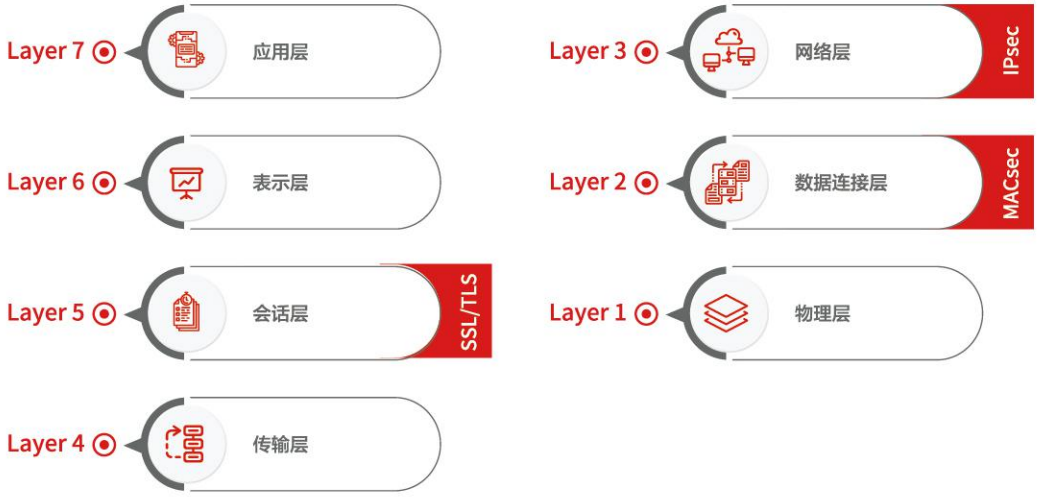
理想的情况下，在云服务器上运行的应用程序应仅与应用程序数据有关。但实际情况中可能有成千上万个客户端会随时访问服务器，因此在大多数情况下，处理各个层的协议可能会占用服务器。处理流程一般都是：打开信封，检查内容和地址，然后将内容放入正确的抽屉中。

这种检查和记账的大部分内容与应用程序无关，因此只要足够快，就可以由单独的处理单元进行处理。关键示例如下：

**真实性**
检查传入请求的真实性并设置加密/解密，这是第5层的SSL / TLS握手

**检查/订购**
通过第3层中的IPsec协议检查和排序路由数据包

**规制**
由第2层的MACsec协议调节两个物理机之间的帧流量




开放系统互连（OSI）网络参考模型

# 为数百万个连接启用安全握手

保障主机应用程序和客户端之间通信安全的基础是传输层安全协议(TLS)及其前身安全套接字层协议(SSL)，提供了端到端的身份验证和机密性。

在当今的数据中心系统中，每次对发起方进行身份验证并建立安全的加密通道时，云应用程序可能必须每秒接受和处理数千至数百万个连接。但是SSL / TLS处理到涉及复杂的数学函数时，这些函数本身可能已经使用了应用处理器80%到100%的可用计算能力。因此，分流这些处理功能已成为必不可少的工作。

**在当今的数据中心里，云应用程序可能每秒必须接受并处理数以千计的连接**

为了解决这个问题并释放出应用处理器，Silex Insight开发了一套超高性能IP模块，它们共同构成了SSL/TLS的硬件加速器，可以作为ASIC来实现，或作为FPGA的主要技术之一来实现。这套IP模块经过验证，是目前市场上最快、最高效的工具之一。

Silex Insight的SSL / TLS加速器涵盖了连接握手所需的所有复杂密码计算，即通过非对称密码进行身份验证和交换对称密钥。这些算法包括RSA、ECC、AES、SHA和真实随机数生成等算法。重要的是，该加速器可以100%卸载所有操作和内存访问。这是通过内置的分散收集DMA和基于高度流水线实现的可伸缩数据路径完成的。为了实现非对称操作，IP内核配备了内部微编码定序器，这样就可以根据非常多样化的应用程序和平台的需求来确定芯片的占地面积以及相应的硬件成本，最终取得最佳的平衡决策。这也使Silex Insight的内核能够基于速度、性能、适用面积而成为业内效率最高的内核。

## TLS 连接性能 (Ops/s)


在以上结果中，每个运算包括2个乘法点和1个符号运算


## 处理高达1.5Tbit / s的数据流

随着100Gbit/s和更高数据流的应用前景，传统NIC正在演变为智能NIC。这些是专用的可重配置板，可接管越来越多的网络数据包和安全处理功能。这种流水线内联过程中，主机将数据包发送到NIC，然后在其中将数据包通过各种模块在硬件中进行处理，最后将结果返回到主机。

Silex Insight作为全球安全IP的领先供应商之一，已经为智能NIC开发了几款基本IP模块，可应用到网络第2层、第3层的MACsec和IPsec处理。这些一流的IP模块可以轻松地集成到由数据中心或硬件供应商开发的智能NIC平台中，从而缩短此类产品的上市时间，并降低服务器所有权成本。

Silex Insight的MACsec和IPsec引擎符合最新的标准，它们在第2层、第3层提供了无连接方式的数据完整性、数据源真实性和保密性。

主要功能：

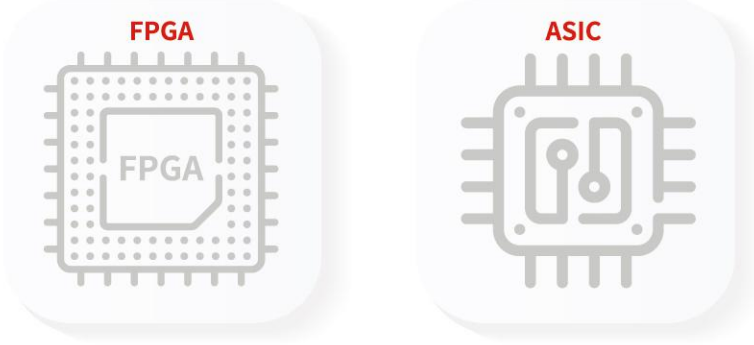
**低延迟**
可选的创新设计助力对延时敏感的应用场景的技术实现

**线速加速**
高效的加密内核，可对64byte数据包进行线速处理

**重播保护**
卸载重播保护和数据包编号管理可进一步减轻CPU负载

**这些IP模块集成了针对应用程序实际需求进行优化的加密引擎，因此IP模块具有无与伦比的可扩展性，并可在吞吐量、面积和延迟要求之间取得平衡。**

**两种引擎的设计均完全独立于技术，可以集成到各种FPGA和ASIC技术中，借助FPGA平台(例如Xilinx ®Alve-oTM数据中心加速器），通过为供应商定制的方式来获得更高的吞吐量。**




智能NIC 可以集成在FPGA和ASIC技术中

## 用IP模块设计灵活的、面向未来的解决方案

设计一款能同时保证高安全性、高性能IP模块并非易事，需要深入的专业知识，较长的开发周期，并且对产品进行持续的改进和开发。因此，通过集成可靠供应商的第三方模块来简化开发变得很有价值和意义。

## Silex Insight的IP模块具有使其脱颖而出的几个优势：

由安全专家设计，包括最新标准和见解

独特的可扩展性，可以在性能和芯片面积（以及成本）之间取得最佳平衡

经过硅验证的各种应用程序，
包括非常苛刻的安全支付解决方案

设计时易于集成

如果需要，Silex Insight的专家也可以帮助您设计出符合客户需求的最佳解决方案，其中包括技术和成本/性能折衷的选择。

## 结论

数据中心是一个高度复杂且对安全性非常敏感的环境，与单一客户端应用程序不同，安全隐患可能会产生深远的影响。更重要的是，云端应用程序的成功极大程度上取决于数据中心的响应能力。

因此，将网络处理和加密技术转移到非常快的硬件上已成为势在必行的改变。

可信赖供应商的高性能IP模块，例如Silex Insight，可提供以经济高效、快速安全的方式集成此类加速器和网络板。

Silex Insight提供增强数据中心的关键组件，其中包括业界最快的SSL / TLS握手引擎之一，以及超高性能的MACsec和IPsec处理性能（FPGA上为100 Gbit / s，ASIC上为1.5Tbit / s）。

更多信息和技术内容，请访问 **www.silexinsight.com.cn**

## 关于Silex Insight

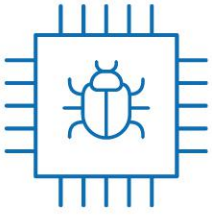
Silex Insight是全球领先嵌入式系统安全IP解决方案独立供应商，为嵌入式系统提供安全IP解决方案，并为AVoIP /视频IP编解码器提供定制OEM解决方案，可提供高端图像和视频压缩解决方案，以便通过IP分发低延迟的4K HDR视频。Silex Insight的安全平台和解决方案凸显出加密引擎的高性能和易于集成的灵活性，以及为所有平台提供完整安全解决方案的eSecure IP模块。

Silex Insight研发和制造是在比利时布鲁塞尔附近的总部进行，各国家或地区销售服务和技术支持由全球各分支机构提供，相关信息请访问www.silexinsight.com.cn。

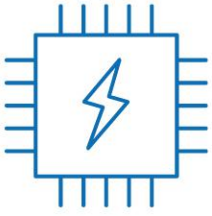
onespin

确保芯片完备性

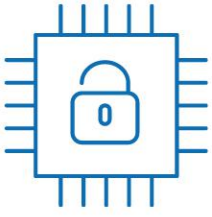
## 芯片完备性解决方案



功能正确性

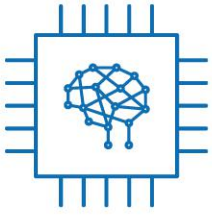


安全

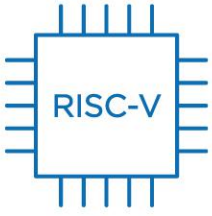


信任与安全

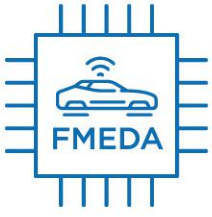
## 應用领域



异构计算



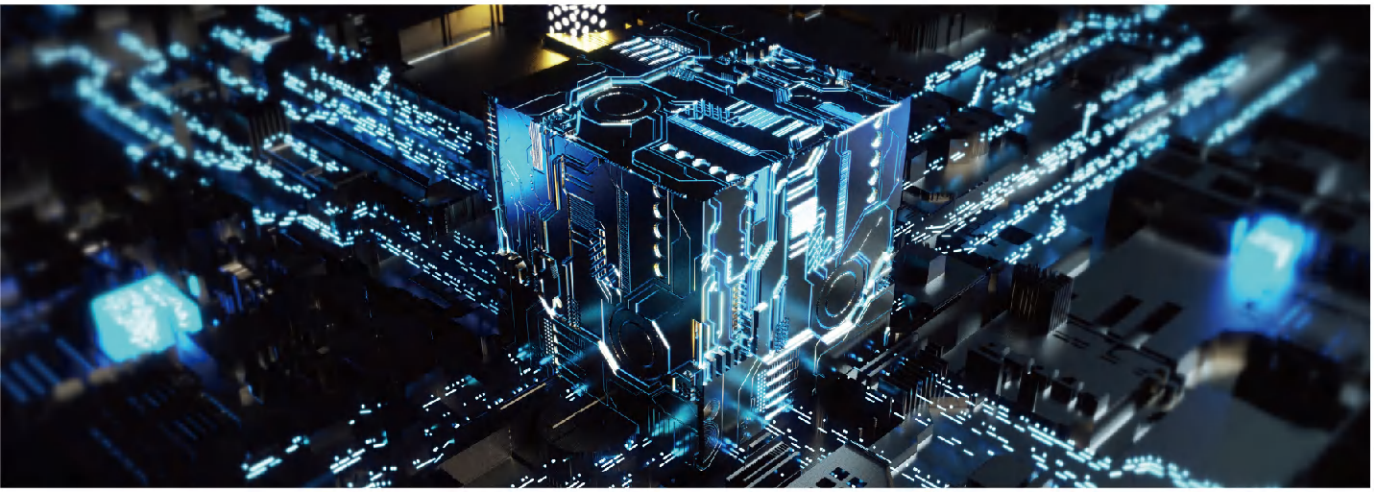

RISC-V




汽车和工业

OneSpin提供最先进，最强大的验证平台，以解决当今的关键性芯片完备性问题。 我们的专家致力于解决最棘手的下一代验证挑战，并提供使设计团队能够创建功能正确，安全，可靠且可信赖的SoC的解决方案。

www.onespin.com



# 通过可靠的验证流程和广泛的生态系统提供高质量的IP

Mike Gianfagna　PLDA

对于设计先进且复杂 SoC 的工程人员来说，“现成的 IP”一词可能是水月镜花。尽管市场上各种 IP 标题中都冠以”现成的”，但要获得最高性能或最低功耗的系统目标可能会需要 IP 的是定制的。

PLDA 已经熟知市场对复性能高复杂度 IP 的这些需求，例如 PCIe 5.0 或 CXL。PLDA 客户通常会需要某些非常特定的功能和配置，这些功能和配置会触发 IP 修改。尽管如此，每个客户也还是都希望交付的 IP 产品经过详尽的验证，健壮可靠，甚至希望它像已多方流片量产验证一样。这是一个艰巨的任务，但这是进入高端 IP 市场的代价。

PLDA 已经开发出一种全面周到而又严谨细致的方法来应对这一挑战。他们甚至开发了一个生态系统来支持自己的工作－稍后再介绍。我有幸从 PLDA 的市场经理Romain Tourneau那里获得了IP验证工作的概述。

Romain 首先概述了需要理解和管理的客户的需求规格，包括：

功能要求：行为规则（事件与后果）

参数要求：性能，门数，功耗

结构 / 物理要求 必须是可综合，易收敛（CDC）

追求高质量的可交付成果意味着需要久经验证的经验来识别“Golden”或最重要的关键点。然后，专注于最大化验证这些 Golden 需求的方法。这一环节遵循实施、调试和改进过程。有许多方法可以管理此过程，包括：

标准方法（自始至终单一流程）

增量方法（按照设计更改增量逐一验证）

“冲刺”方法（项目拆分为较小的增量版本）

“超级冲刺”方法（与“冲刺”相同，但周期加快）

PLDA 使用超级冲刺方法，总结如下：

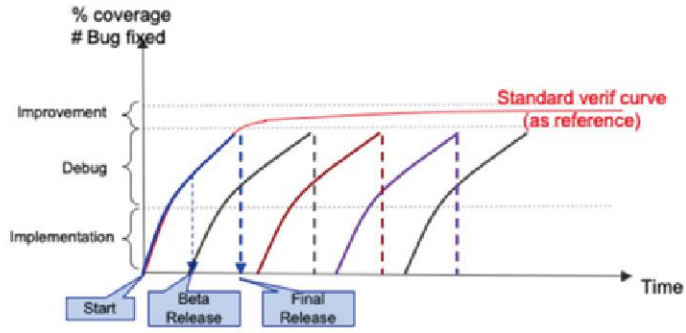
尽管仍有许多手动和费时的任务要执行，但“超级冲刺”方法的迭代特性可促进与客户进行有效的协作。在项目启动伊始就与客户进行深入的验证讨论，以便于：

•了解客户的流程和工具

•了解客户的验证计划，IP 使用情况和相关成本

•解释 PLDA 流程和工具

•找出与设计标准的差异及可能的解决方案




| | |
|---|---|
| Model | New implementation starts when previous release is in debug phase (= beta release) |
| Benefits | Super-short project cycle (<2months): flexibility to adapt releases to Customer schedules and feature content + additional beta release |
| Requirements & Challenges | Faster verification sign-off than "sprint":<br>- Fast debug with efficient fail-case triage Dana<br>- Fast predictable regressions (directed tests & configurations)<br>- Fast incremental coverage gap analysis and improvements implementation |
| Cost & drawbacks | Requires more verif resources (people + licenses) to handle sprints overlaps |

•PLDA 可以提供现成的验证环境来更早地执行此独立验证，并说明客户在项目早期开始 IP 验证的优势和重要性

•为了进一步巩固对稳健验证的承诺，PLDA 最近发布了“稳健验证”工具集，可提高具有 CXL®，PCIe®6.0 或 Gen-Z® 互连的下一代 SoC 的设计准确性并缩短设计到量产周期。该发布详细介绍了全面的验证策略，其中包括 PLDA 自有验证流程中的组件以及 Aldec，Avery Design Systems 和西门子 Mentor 的工具。

通常，您不会看到关于 IP 验证方法如此主动而广泛的要求 - 这非常值得关注：

“IP 设计验证过程通常发生在芯片的前端设计阶段，要求高度可靠以防生产延迟。诚然，实现必要级别的验证很耗工时，但是在验证过程中走捷径往往会在芯片制造结束时发现昂贵且难以修复的错误。所以，始终确保健壮和高质量的验证过程其实效率更高。”在我看来，这是一个非常有见地的观点。

PLDA 被称为 ”稳健验证”的工具集包括：

•验证 IP，涵盖 PCIe，AMBA AXI，CXL，CCIX 和 Gen-Z 的标准合规性

•支持带有 UVM 测试平台的混合语言设计的模拟器

•经典 EDA 提供者提供的综合和静态验证工具，可对 RTL 设计和 CDC 的质量进行验证

•为了管理在验证和验证过程中由“稳健验证工具集”生成的数据，PLDA 开发了一个名为 DANA 的接口。

•DANA 接口是 PLDA 专有的工具，用于通过一系列自动报告，流程自动化和严格的后续流程来提供高效的供应链管理。完整工具集的数据将自动收集，分析和报告，减少了由数据管理引起的审查周期，加快了决策过程。对于项目负责人和验证工程师而言，这都将节省他们的宝贵时间。

了解更多关于 PLDA 验证解决方案的信息：

•回顾 Mentor 和 PLDA 在 DAC 2020 上的技术文章：“使用 Mentor QVIP 和 PLDA PCIe 控制器加速 DMA 应用的 PCIe 模拟”。

•不要错过与 PLDA 和 Avery 在 DAC 2020 合作举办的 Aldec PCIe 5.0 模拟 / 验证演示

•有关 PLDA 验证过程的更多信息，请访问 PLDA 官网：www.plda.com

# 回答社区有关RISC-V验证的问题

OneSpin

可以肯定地说，RISC-V 在设计社区中正迅速普及。开源特性不仅使其成为一种经济高效的选择，而且指令集体系结构（ISA）的设计也具有灵活性。它可以映射到许多实现以及微体系结构，包含许多可选的指令和功能，允许开发自定义指令和功能，并支持广泛的最终应用程序。但是，这种灵活性带来了验证挑战以及有关如何最好地解决这些验证挑战的问题。

开发和使用 RISC-V 内核时，必须满足许多要求。最大的需求之一是对 IP 实施的信任。是否已实现所有功能？ 它们是否已正确实施？ 实施中是否存在任何错误？ 此 IP 内有木马吗？ 模拟分析很难回答这些问题，导致越来越多地使用形式来回答这些问题。形式的详尽性使其成为确保对核心置信度的理想选择。

为了更深入地了解如何有效验证 RISC-V，我们对社区进行了调查，询问他们与该主题相关的特定问题。以下是我们的 OneSpin 驻地验证专家对问题的细分以及相应的解答。

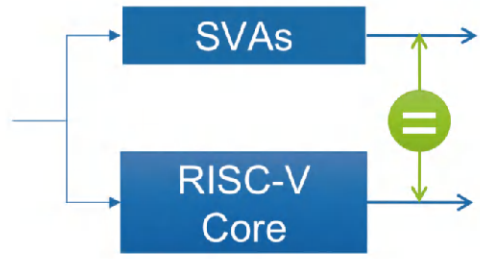
问：是否只有 RISC-V 有特殊的形式技术？

答：RISC-V 没有特定的内容。但是，您需要对 RISC-V ISA 有相当详细的了解，才能创建正确的属性集并确保属性集完备。

用于创建属性的一种形式技术应该是间隔属性检查。这些是可重用的 SystemVerilog 断言，以实现无限的证明。这些断言有几个重要方面。它们不是从复位开始，而是从通用有效状态开始。达到通用有效状态的周期数有限。将 ISA 规范要求与微体系结构细节分离开来是至关重要的。

这些可操作的 SystemVerilog 断言可实现高级的、不重叠的断言，以简洁明了的方式捕获端到端交易和需求：

- 以形式和模拟可执行格式捕获功能需求
- 与时序图类似，以简洁明了的方式捕获整个流程交易
- 通过易于查看的高级断言实现 100%的功能覆盖
- 采用一致的断言样式，适用于广泛的应用程序，并能够为模拟器和形式工具提供最佳性能
- 将可用于实现的特定支持验证代码与可重用的规范级代码完全分开




完全验证 RISC-V 设计需要构建许多属性。这可能需要数月才能完成，并且需要形式工具的详细知识才能完全融合。市场上有可以大大减少时间的解决方案。

问：由于 RISC-V 是一个庞大的设计，如何验证它以及它最初的假设是什么？

答：很难回答最初的假设应该是什么，因为根据特定的设计，这些假设应该有所不同。

但是，在处理诸如 RISC-V 内核这样的大型设计的验证时，最好的方法就是分而治之。专注于核心应该是第一步。这包括确保不违反协议，分别验证缓存以隔离相关的复杂性，查看不同块和单元之间的互连并执行 x 传播。请务必注意，在此步骤中，x 传播应在块和单元级别而不是整个核心上进行。另一种技术是使用“假设保证”来验证端口。

值得一提的是，这些方法并非特定于 RISC-V，可应用于任何处理器验证。但是，RISC-V 的复杂性意味着可能要花费数月才能对核心进行完备而详尽的验证。

市场上有像 OneSpin’s Processor Verification solution 那样的解决方案，其设计考虑到了复杂性，可以在短时间内生成可重用的断言 IP 并实现全面验证。

问：对于想要按照关键安全标准认证实施 RISC-V 的公司，使用形式验证而不是模拟有什么好处？

答：形式化优于模拟的主要好处之一是它提供的详尽性。这不仅适用于 RISC-V，还适用于任何处理器。关键是随着复杂度的增加，模拟有时不再详尽。对于当今的设计，该复杂度阈值相当低。由于它与 RISC-V 有关，因此可以通过对 ISA 正确了解，完备的属性集和正确的形式引擎来实现详尽的验证。

形式验证比简单地通过模拟运行的传统一致性测试套件要强大得多。无论多么广泛，模拟都只能行使可能设计行为的极小一部分。即使是最精心设计的合规套件，也会在设计覆盖范围上留下空白。在无数情况下，未经测试的特定操作数值或特殊情况都存在，其中一些可能会触发隐藏的设计错误。算术运算尤其会遇到此问题。RTL 描述中的单个错误键入的数组索引可以产生一种设计，其中意外的和非直观的操作数生成错误的答案。模拟的本质以及加速和仿真，使其不可能尝试所有可能的情况。形式工具不会遍历测试用例；他们从数学角度对设计进行了整体分析。

在安全性方面，了解是否可以避免漏洞，存在什么漏洞以及所有错误的位置，甚至所有路径是否正确都是至关重要的。模拟很难提供完备的图片。由于连续运行无法找到所有答案，因此模拟运行存在收益递减点。形式是唯一可以最终证明不存在某些东西（如错误）的技术。有一些安全标准要求使用特定的验证技术，以及定义明确的彻底验证过程。这意味着验证必须更加严格。如果需要考虑安全性，那么仅凭模拟是不够的，进而，形式验证必须是验证计划的一部分。

问：我听说 RISC-V 内核是用 Chisel 编写的。形式如何处理呢？

答：有一些开源的核心，例如伯克利（Berkeley）的核心，都是用 Chisel 编写的。但是，大多数形式解决方案都不直接支持该语言。尽管有许多方法可以轻松将 Chisel 转换为 Verilog，但市场上的形式工具广泛支持这些方法。当然，有许多直接用 Verilog 编写的 RISC-V 内核，因此对于这些内核而言，转换不是问题。

问：我是否需要验证从 RISC-V 核心提供程序接收到的 RISC-V 核心是否没有错误？

答：简短的回答：是。核心提供者应对核心进行完整的完备性验证，并提供结论文档。为了对核心的完备性充满置信度，形式验证应成为其验证流程的一部分。

不过，因为核心仅已过形式验证，并不意味着它可以完全集成到设计中并且没有任何问题。将 RISC-V 内核引入最终设计时，应重新运行所有验证步骤。

问：如何验证 RISC-V 内核已正确集成到设计中？

答：建议使用针对 RISC-V 复杂性的形式解决方案。该过程必须包括自动代码检查，以在功能验证和逻辑综合之前快速消除许多类的常见编码和设计错误。RTL 的验证应从三个不同的角度进行：

•结构分析：对源代码进行集中的语法和语义分析。

•安全检查：彻底验证不存在常见的顺序设计操作问题

•激活检查：证明特定的设计功能可以执行并且不会由于代码不可达而被阻止

间隔属性检查还应按照上述上一个问题的答案中的描述进行使用：“是否有仅针对 RISC-V 的特殊形式技术？”。

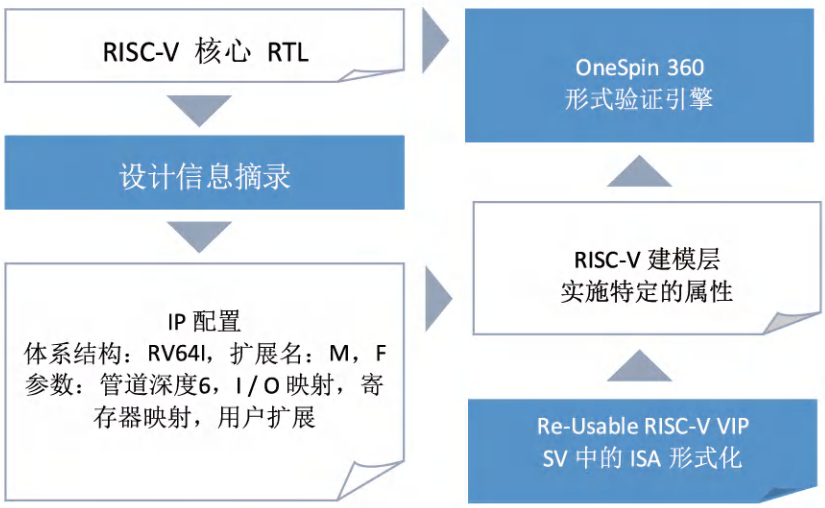
问：我添加了自定义说明。我需要重新验证整个 RISC-V 内核吗？

答：做任何修改自定义指令的操作都意味着已添加或更改了功能。为了确保设计按预期运行并且不会做任何意外的事情，强烈建议您进行完全重新验证。

问：我需要一个无错误的 RISC-V 内核。我应该使用哪些供应商或开源内核？

答：寻找提供开放源代码核心的供应商，这些核心已经使用形式方法进行了详尽的验证。这将大大减少错误逃逸到最终设计中的机会。请务必索取有关供应商验证过程的文件，以确保已使用该形式文件。开始使用经过形式验证的开源内核的一个好的地方是与 OpenHW Group（www.openhwgroup.org）联系。核心开发包括考虑形式的验证计划。

正如我们所讨论的那样，RISC-V 除了降低了处理器成本壁垒之外，还提供了灵活性和定制化的优势。但是，好处增加了复杂性，因此可能会使验证过程复杂化。任何对 RISC-V 感兴趣的设计人员来说，了解验证挑战以及如何克服挑战都是至关重要的。我们希望提供的答案能加深如何应用验证以及相关工具和技术来实现完备验证的理解。




OneSpin Processor Verification Flow　OneSpin 处理器验证流程

# 多格式8K视频解码IP 内核

Doug Ridge博士，韦裕京，Allegro DVT

## 概述

Allegro DVT 已经推出了能够支持到 8K 解析度每秒 60 帧的多格式视频解码 IP 内核。此内核可以使用 16nm 或者更加先进的芯片制程来实现。其低时钟频率的要求使芯片布局简单易行并保证首次即成功的顺利实现。

## 引言

Allegro DVT 研发领先的视频编码及解码 IP 内核已经有十几年的经验。近年来新的视频格式如 AV1 和 VP9 的推出意味着 8K 解析度和每秒 120 帧率的规格带来了更高的复杂度从而对保持领先的途径提出了新的要求。

我们将技术定位于满足当前的市场需求并兼容未来更高的分辨率和帧率以及新格式的要求，Allegro 开发了一个可扩展的架构以支持：

- 多格式解码
- 解析度和帧率到 8Kp60
- 8，10，12 位
- 4:4:4，4:2:2 和 4:2:0 色度采样
- 多路码流

## 实现 8K60

解码器 IP 内核实现 8K60 所需的性能不是简单的任务。首先，直接为 8K60 设计的内核对于不需要该分辨率的其他大部分应用来说将会太大，因此会导致更高的实现成本。因此，Allegro 开发了一种可扩展性能的架构，以优化芯片面积并降低总体解决方案的成本。为满足市场需求，我们还设计了用于 16nm 或者更先进制程工艺的内核。

体系结构的可扩展性来自于在设计的关键路径中复制关键模块。复制量取决于需要与目标制程节点一起支持的视频解析度和分辨率。如下图所示，通过定位 5nm 而不是 16nm 可以实现 2 倍的性能提高，因此需要更少的复制就能实现与 16nm 相同的性能。

该体系结构的可扩展性和灵活性允许针对内核和目标制程节点的任何给定参数集实现最有效的实现。例如，某些应用程序（例如游戏）需要具有 4：4：4 色度的 12 位采样。这些要求导致的实现难度远大于满足使用 8 位或 10 位进行 4：2：0 色度采样所需要的实现，因此，基于最终的应用选择参数非常重要，而我们研发的架构正是通过这种方式实现的。

## 内核灵活性

Allegro 在开发 AL-D3xx 视频解码器系列时，其内核建立在前几代支持 HEVC/H.265 和 AVC/H.264 等成熟格式的核心之上。AV1 和 VP9 的支持是以这些现存格式的解码框架作为一个起点

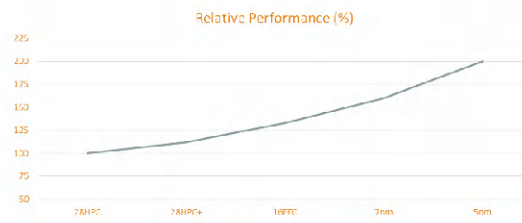



Figure 1. 制程节点的相对性能

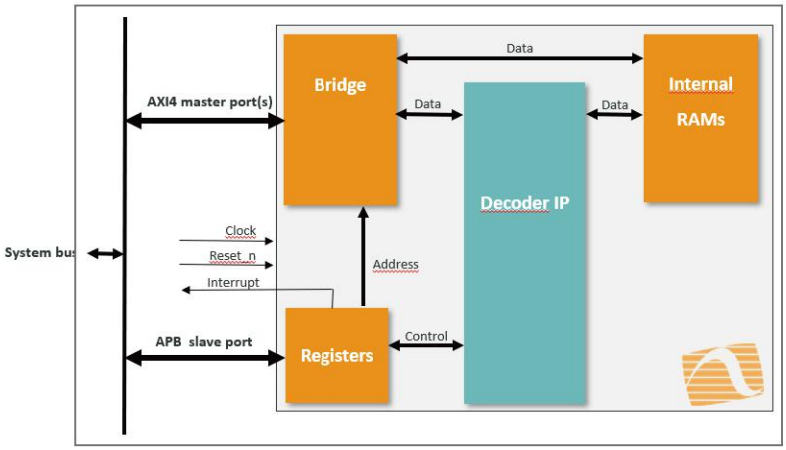



Figure 2. 解码流程框架

| Elementary streams |
| --- |
| H.264 / AVC |
| H.265 / HEVC |
| AVS2 |
| AVS3 |
| VP9 |
| AV1 |
| H.266 / VVC |

Figure 3. Available compliance stream formats.

而添加，而不是从头开始。客户的关键受益点是，生成的基础内核同时支持新的视频格式和现有的成熟的格式，这增加了内核兼容性使之能够接收来自多个信源的码流包括不同的编码格式。

内核能够支持多种格式同时实现 8K60 的能力，也可以轻松针对所选制程中的满足性能需求的格式子集进行配置，从而最大限度地减少最终客户的实现复杂度。这种按需配置的方法已经在客户中取得了成功，通过该解决方案，客户可以定制化地以最小的芯片面积和简化的芯片集成工艺满足其视频解码的要求。

## 框架

灵活可配置的解码 IP 内核有时会被误解可能在验证中产生挑战，客户是否有信心定制化配置的内核能够一次成功。Allegro 在其内核开发中通过使用 AXI4 和 APB 总线来标准化内核与外设通信的方式，从而解决了这一问题，如下图 2 所示。

Allegro 的 AL-D3xx 系列主要的解码成员包括以下配置 ：

- 支持 AV1, VP9, HEVC, AVC
- 8 和 10 位
- 4:2:0 and 4:2:2 色度采样
- 8K60

## 验证

内核利用从各种来源获得的码流进行了广泛充分的验证。这些码流包括：

- 语法码流
- 性能码流
- 纠错码流
- 客户码流

验证是一个耗时耗力的过程，此处要进行的工作是利用一系列基于 FPGA 的系统以实现在实时的 1/6 至 1/10 时序之间执行相应的验证任务。作为全球领先的兼容性测试码流的媒体提供商，Allegro 可以使用自己生成的前沿码流以及从其他来源包括客户码流获得的测试流进行验证。Allegro


Figure 4. FPGA System used for verification.

提供的码流可以应用于语法，性能和错误恢复能力的不同格式的测试。

验证的过程使用了基于 FPGA 的已有现成系统来加速进程，这些系统包括了如下所示的 Pro Design ProFPGA duo V7。

## 总结

Allegro DVT 开发了世界领先的视频解码 IP 内核，能够兼容 AV1、VP9、HEVC 和 AVC 格式编码的码流。高度紧凑而灵活的架构建立在基于数代更迭，多次得到量产芯片验证 过的，适用于多种芯片制程的 Allegro 的成熟解码内核。

更多信息

有关 Allegro 产品组合中此 8K 视频解码 IP 内核和其他内核的进一步信息，请发送电子邮件至 info@allegrodvt.com。

# PUF: 在供应链中管理安全

**现实需求**

IoT时代互联设备越来越多，出于安全目的(例如以防止间谍活动) 需要对设备进行身份验证。身份验证意味着密钥需被嵌入在设备中，应该如何管理这些密钥以确保必要的安全性呢?
通常，将凭据（例如master key or authorization keys）注入依赖于密钥管理系统的设备。 关于供应链，则需要一个新的角色来发挥作用。 从攻击面来看，端点和操作员都是潜在的目标。这涉及到有问题密钥的所有权。解决这些问题的方案是使用由PUF生成的硅提取密钥。该方案为密钥提供了唯一性。该密钥也可以由ODM签名以提高可信度，这使ODM可以使用PUF来认证设备。

**安全实例**

RTL密钥或OTP密钥的问题在于它们可以被回读。例如故障分析实验室知道如何对低至10nm技术的芯片进行反处理，这种侵入式攻击可以获得密钥。然而PUF生成的密钥则无法从芯片中提取。逆向工程技术无法恢复PUF生成的密钥，因为此操作会破坏PUF生成的密钥，而且诸如探测之类的物理攻击也无法恢复该密钥。当PUF输出停留在设备本地时，PUF为无法复制（无法物理克隆）且无法模拟（无法数学克隆）的系统提供易失性密钥。

**Secure-IC PUF 技术关键词**

稳定性：PUF响应对噪声不敏感
唯一性：每个设备都有自己的签名
随机性：PUF具有加密等级的比特熵
抵抗攻击的鲁棒性：PUF可承受物理和数学克隆
灵活且可定制：PUF解决各种灵活，且可基于熵，吞吐量等进行配置以实现最优化。

**应用领域**

PUF是一种通用解决方案，可适用于多种应用场景:

1. 安全启动：PUF生成主密钥以检查固件的真实性。 随后经过身份验证的外部闪存可以用作安全存储器。
2. 从云端配置和激活芯片。
3. 用于身份验证的Challenge-Response协议
4. 设备不可伪造ID
5. 确定性随机位发生器的唯一种子
6. 借助适当的密钥派生功能（KDF），根密钥可生成辅助密钥

通常，PUF可提供密钥，因此可用于加密和身份验证。

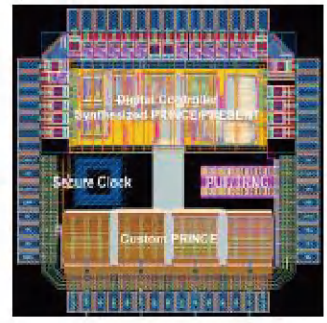



图1集成在IC (FDSOI 28nm) 中的LPUF的示例

**易整合性**

Secure-IC PUF嵌入了可在芯片启动或其生命周期期间使用的健康测试程序。

例如，对于生成128位密钥的PUF，注册过程可能持续20毫秒，而在boot过程中的密钥重建过程持续时间可能为10毫秒（这些数字代表了行业水平）。 PUF可以使用或不使用所谓的辅助数据来实现。 显然，使用辅助数据时可靠性更高。
Secure-IC PUF的实现可基于标准单元，因此可通过任何设计套件来实现，从而可以轻松地实现技术的移植。同时PUF可以由安全的软件API控制以调整其性能。
Design-For-Test (DFT) 是非常有益的方式，它是在工业中的标准做法，用于筛选功能芯片与制造损伤。Secure-IC PUF具有特定的模式用于支持DFT。

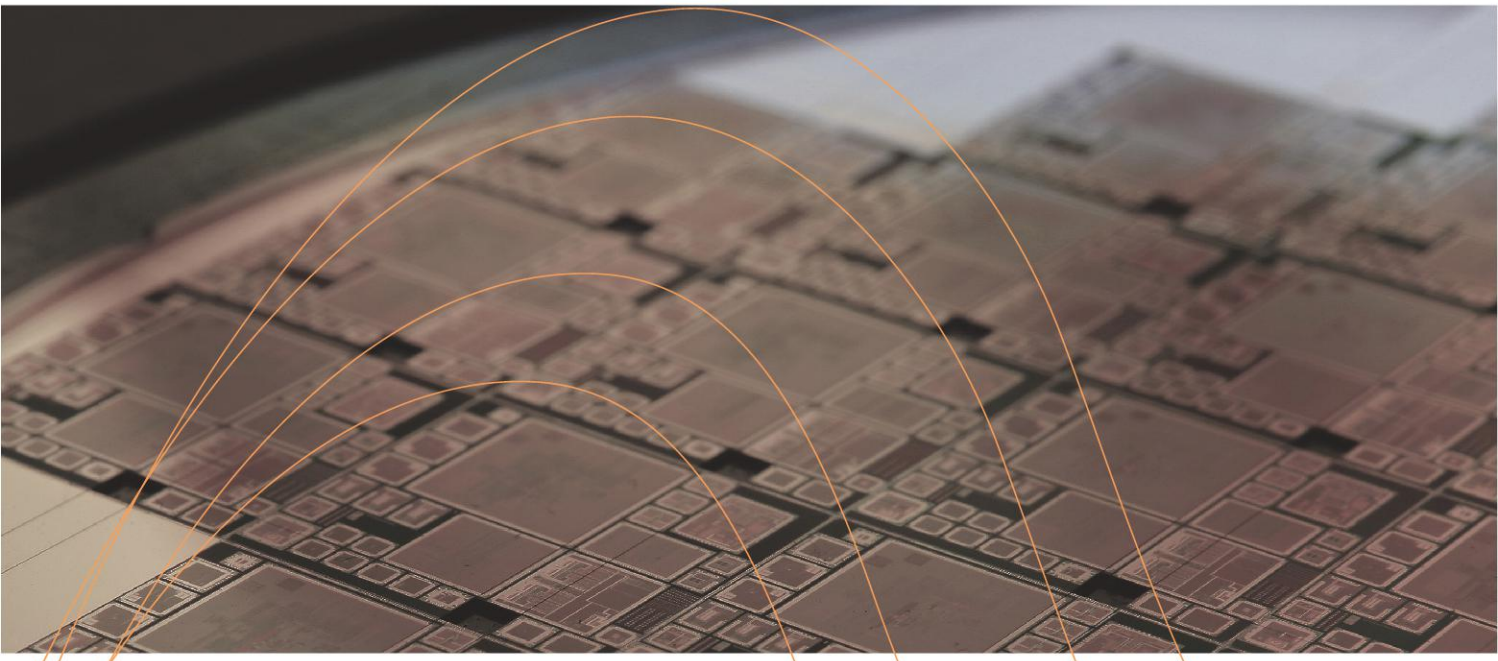
**国际标准**

有关PUF安全要求和测试方法的标准正在进行中，其编号为ISO/IEC DIS 20897-1和20897-2，Secure-IC是 ISO/IEC JTC 1 / SC 27技术委员会的成员，该委员会致力于ISO/IEC 20897的安全要求，其标题为 «Security requirements and test methods for physically unclonable functions for generating non-stored security parameters — Part 1: Security requirements, Part 2: Test and evaluation methods» 。

**您也可以登录我们的中文网站查询更多信息:**
**https://cn.secure-ic.com/**

ALLEGRO

Digital Video Technology



## Leading provider of video compliance streams and hardware video IPs

- World-leader of H.264/AVC, H.265/HEVC, AVS2, AVS3, VP9, AV1 and VVC compliance test suites
- AV1, VP9, H.264/AVC, H.265/HEVC and JPEG encoder and decoder hardware (RTL) IPs
- Allegro DVT products have been chosen by more than 100 major IC providers, OEMs and broadcasters

Allegro DVT is today a recognized market leader in video compression technologies and has been a long term partner for brand name semiconductor companies worldwide. Along with the rapid growth of our IP business in greater China area, Allegro established local engineering team in Beijing and in Shanghai.

www.allegrodvt.com

# 量子穿隧PUF信任根：PUFrt

PUFsecurity 熵码科技

PUFsecurity 熵码科技于八月推出市场唯一一个高度整合多项基础安全功能的硬件信任根 IP 模块 —PUFrt，该 IP 的核心技术主要整合了母公司力旺电子的量子穿隧 PUF (NeoPUF)、一次性编码的内存 (NeoFuse)，以及高效能的真随机数生成器 PUFtrng。

在一个安全 SoC 系统中可以分成应用层、软件层以及硬件层，其中硬件层包含硬件逻辑电路、工作内存、非挥发性内存以及加密算法引擎部分。而根据柯克霍夫原则所言，安全核心的定义是最重要的机密信息或者是密钥部分，而非加密引擎的设计，所以一个安全系统里面真正重要的，就是如何提供一个唯一能相信且绝对安全的秘密信息或密钥，并保护这个秘密信息或密钥的核心区块，就是所谓的硬件信任根。

一个硬件安全信任根必须拥有几个重要的元素，分别是完整的机密数据的读写权限管理、安全储存，真随机数生成器，芯片指纹与完整的抗攻击设计。而 PUFrt 可以一次满足这些需求。

PUFrt 拥有五大重点模块(如图 1 所示)：

一、PRTC：专一的 PRTC 控制接口，提供完整的机敏数据读写权限控制，以及抗攻击信道的数字设计。

二、PUFuid：利用每颗芯片独一无二的「数字指纹」(PUF) 生成 UID，可直接作为身分识别应用于生产管理，或产生密钥来支持更多的芯片安全需求。

三、PUFtrng：透过真随机数生成器来输出密钥生成所需的随机数、来满足整个安全系统对于动态随机数的需求，以及用于保护加密算法引擎。

四、PUFkeyst：以加密 OTP 储存重要的密钥，保护重要数据免受物理篡改。

五、完善的抗攻击设计，其中包含对于物理性攻击或者是电性攻击等的防御。


图 1：PUFrt 功能架构

以下针对五大模块进行更进一步的说明：

## 一、PRTC（图 2）：

专一的 PRTC 控制接口，提供完整的机敏数据读写权限控制，以及抗攻击信道的数字设计，可以保护通道以及抵抗恶意读写的攻击。PRTC 还提供了系统总线和功能块之间的标准接口 APB 以及内存映像的指令集，更提供 API 指令集使软件工程师可以简易使用 PUFrt，从而增强了客户使用经验以及提供客户快速导入量产的优势。

## 二、PUFuid（图 3）：

PUFuid 是利用每颗芯片独一无二的「数字指纹」(PUF)，产生独一无二的芯片密钥来支持更多的芯片安全需求，其中包括加密、身份辨识、身份验证，安全密钥生成等。PUFrt


图 2：PUFrt 内核 PRTC 特色


图 3：PUFrt 内核 PUFuid 特色


图 4：PUFrt 内核 PUFtrng 特色


图 5：PUFrt 内核 PUFkeyst 特色

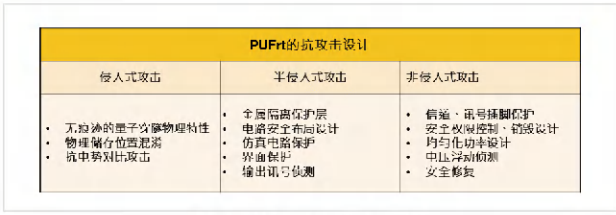



图 6：PUFrt 的抗攻击设计

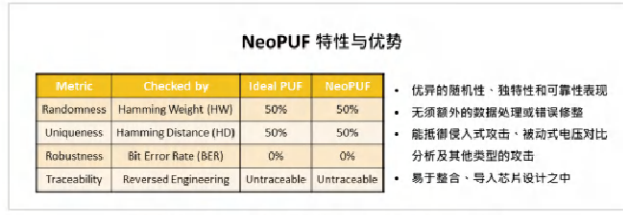



图 7：PUFrt 核心技术 NeoPUF 的杰出特性

可以解决芯片设计师面临的关键问题，提供了一种简单又安全的方法，从芯片内自 PUF 提取随机数串，免除外部注入密钥的风险。

## 三、PUFtrng（图 4）：

PUFrt 透过 PUFtrng 真随机数产生器来输出密钥生成所需的随机数、来提供整个安全系统对于动态随机数的需求以及保护加密算法引擎。PUFtrng 是真正的随机数生成器，优势在于极短的初始准备时间及超低功耗。

## 四、PUFkeyst（图 5）：

PUFkeyst 内含 4kbit OTP，其特色是运用 PUF 和 PUFtrng 随机数双重强化 OTP 存储的安全性，用于保护安全功能运作中最重要的密钥或重要数据免受物理篡改。

## 五、抗攻击设计（图 6）

完整的安全性必须要全面考虑在系统上下电期间，对于侵入式、半侵入式与非侵入式攻击的抵御能力。利基于 NeoPUF 无痕迹的量子穿隧物理特性，以及模块内全面的电路布局设计、访问权限控管、自动销毁 / 修复等设计，可以大幅提升 PUFrt 作为硬件信任根的可靠性。

PUFrt 的技术核心环绕着 NeoPUF，可以满足真正的硬件信任根的根本要求，包括理想的随机性，唯一性、稳定性和不可追溯性。详细数据如图 7 所示。

重要的是，NeoPUF 是一个独特的 MOS 器件设计架构，其原理是对两个相连的 MOS 存储器施以高电压，利用电子在栅极氧化层中的悬键间游移产生的量子穿隧电流来运作（图 8）。在高电压之下，我们无法预测该电流会随机发生在哪一个 MOS 存储器中，且另外一个 MOS 存储器将会受到抑制而不会发生隧穿现象。我们将设定两两一组的 MOS 各代表 1 和 0 的数值，透过多组的操作，就能生成一组随机数。除了 600 摄氏度以上的高温，一般的环境变化因子，例如干扰、温差和电压，皆无法改变氧化栅极中悬键的状态，因此我们可以说由 NeoPUF 产生的随机数列是非常可靠的。此外，由于使用 NeoPUF 的设备上没有储存任何电荷，因此一旦设备断电，就无法物理追踪内部的 PUF 值。而且发生在氧化物栅极中产生的量子隧穿通道，是没有办法利用任何仪器侦测，如图 9 所示，不管是 SEM 或者是 TEM 都没有办法获得任何信息。这是每片芯片与生俱来的秘密，而且每个芯片都会有完全独立的结果。

考虑芯片设计工程师的需求，PUFrt 的设计易于采用及导入芯片设计。这颗新 IP 已通过验证，可导入 28nm 制程的半导体设计中。预计于不久的将来推出在 55nm 和 40nm 嵌入式闪存制程的 PUFrt 新版本。PUFsecurity 也计划导入 FinFET 制程，抢攻车用和人工智能应用市场。

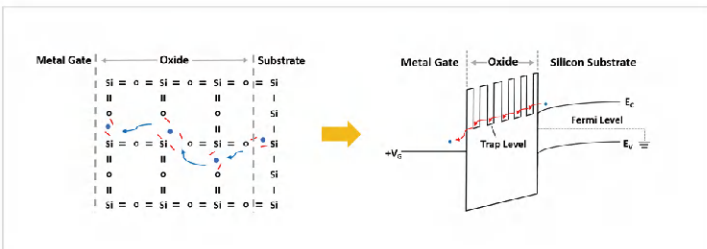



图 8：NeoPUF 量子穿隧机制示意图

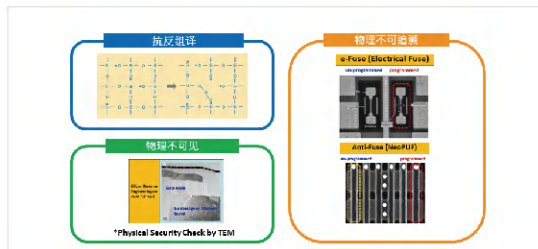



图 9：NeoPUF 抗攻击、不可追溯性

# Empyrean ALPS-GT：首款商用模拟电路异构仿真系统

北京华大九天软件有限公司 资深技术支持工程师 吴涛 | 高级市场拓展经理 余涵

随着集成电路的工艺进入深亚微米（16nm 及以下）阶段，电路设计规模急剧增加，设计工艺复杂度也不断提高。与此同时，产品上市周期变得越来越短，不仅仅要实现功能，还需要综合考虑功耗、时序、寄生参数等对电路的影响，后仿真验证任务变得愈加重要而艰巨，对设计验证效率的要求也越来越高。由于后仿电路的寄生器件规模急剧增加，设计工程师在使用传统 SPICE 仿真工具进行功能验证时遇到了前所未有的挑战。

虽然业内各大 EDA 公司都在纷纷推出或升级各自的后仿工具，但这些工具仍然不能满足业内的需求。一方面是性能出现瓶颈，对一些后仿真电路需要几个星期甚至几个月的情形不在少数；另一方面，对于某些精度要求高，对寄生参数敏感的模拟电路，传统的后仿真工具为提高仿真速度而尽量采用一定程度上牺牲精度的寄生参数约简技术，导致仿真结果精度不满足要求。

目前市场上的 SPICE 仿真工具虽然算法各异，但都是基于 CPU 架构的软件算法。我们通过对比研究发现，由于 CPU 架构和运算单元的制约，整体运算效率已无法再得到质的提升，以适应先进工艺设计的需求。受此限制，用户要么只能挑选部分 PVT corner 进行仿真，或通过子模块级仿真来推导芯片顶层的仿真结果，这为芯片的最终量产质量埋下了不可预知的风险；而通过寄生参数约简技术来加速的仿真结果精度却无法满足验证要求。为此，华大九天在自有模拟仿真器 ALPS 的基础上，开发了 EDA 行业内第一款商用的基于 GPU 加速的模拟电路异构仿真系统 Empyrean ALPS-GT：

我们认为，GPU 由于采用了较 CPU 多两个量级以上的并行架构，其正在定义一种取代摩尔定律的全新超负荷定律（或称“后摩尔时代定律”）。GPU 服务器经过算法优化，在特定的计算领域可以取代数十台商用 CPU 服务器，从而大幅提升应用程序吞吐量并节省成本。在许多传统 CPU 架构的计算任务遇到难以提升的性能瓶颈之时，GPU 异构计算已经成为推动软件发展的必然趋势之一。


图 1. ALPS-GT 的基本理念

采用 GPU 架构的 ALPS-GT 的价值在于确保 True-Spice 精度的同时，能够对模拟电路后仿真带来平均 10 倍以上的加速比。ALPS-GT 的核心运算硬件是英伟达 Telsa V100，这是一款已广泛应用于图像处理、高性能计算、深度学习等领域的利器。表 1 为 CPU 服务器常用的英特尔 Platinum 8180 与英伟达 Tesla V100 的算力比较。


图 2. GPU 的算力显著高于 CPU

可以看出 GPU 相比 CPU 架构来说，无论在运算单元的数量还是总体浮点算力，均有明显优势。业内也早已有学术机构和公司进行过类似异构仿真的开发，但受限于无法充分利用 GPU 的并行算力的瓶颈等一系列原因，一直没有

| | Platinum 8180 | Telsa V100 |
|---|---|---|
| 运算单元 | 28 physical cores | 5376 FP64 cores |
| 浮点计算能力 | 2T flops | 7T flops |

表 1. 硬件运算能力对比

| | 运行时间（ms） | | 加速比 |
|---|---|---|---|
| | NVCUDA求解器 | SMS-GT求解器 | |
| 测例 1 | 130 | 22 | 5.9X |
| 测例 2 | 116 | 46 | 2.5X |
| 测例 3 | 441 | 39 | 11.3X |
| 测例 4 | 171 | 48 | 3.6X |
| 平均加速比 | 5.8X | | |

表 2. 矩阵分解性能对比

形成成熟的模拟仿真方案。

华大九天在模拟仿真领域有着长达 10 多年的技术积累，在 CPU 架构的时代，我们自研的仿真器 ALPS 通过独有的 SMS（Smart Matrix Solver）技术，已能实现在复杂电路后仿真方面相较同类 CPU 仿真器的数倍提速。SMS 的核心内容主要包括：

• 独有的智能矩阵切分技术，相较于传统仿真器，能够将总矩阵切割成更多的子矩阵，分配到各个 CPU 核去进行仿真，以提高 CPU 核的平均利用率。

• 包含较传统仿真器更多的 matrix solver 供选择，对于每个子矩阵而言，自适应的选择特定的 Matrix Solver 可以得到更高的求解效率。当可供选择的 Matrix Solver 越多，那么每个子矩阵获得更高求解效率的概率也就越大。

新一代智能矩阵求加算法 SMS-GT 技术，其架构来源于 CPU 时代的 SMS 技术，并针对后仿真整体时间中占比最重的矩阵求解（Matrix Solving）和器件计算（Model Evaluation）两部分进行了优化和创新，以适应于 GPU 架构大量并行计算的特点。经实际对比，SMS-GT 可以取得相较于直接使用硬件原厂求解器更高效的计算速度：

通过在国内一线设计公司的大量测例验证，基于 SMS-GT 核心算法的 ALPS-GT 对不同电路类型和各工艺节点均普遍适用。在确保精度的前提下，对常见的电路类型（PMU、ADC、DAC、PLL、Serdes 等），ALPS-GT 相较于市面主流的 CPU 架构仿真器均有明显的加速比：

总的来说，ALPS-GT的技术特点包括：

• 完全 True-Spice 精度

• 独创 GPU 矩阵求解方案，相对于基于 CPU 架构的仿真器提供平均 10 倍以上加速比

• 支持超过 5 亿器件的超大仿真容量，为先进工艺的后仿真提供保障

• 支持从传统工艺到 7+nm 的设计，得到国际领先 foundry 的工艺认证

作为国内最大的 EDA 供应商，华大九天在包括模拟仿真在内的模拟和数字设计流程领域中有长达 10 年的深耕。创立前期不断夯实基础，开发和完善模拟 / 数模混合设计全流程平台工具。近几年，随着软件的不断成熟，技术能力不断提升以及人员和市场规模的扩大，华大九天加速推出 EDA 新品工具，在填补空白的同时，逐步在某些 EDA 产品方向引领前沿设计方法学。ALPS-GT 致力于解决先进工艺下大规模仿真带来的技术挑战，目前已在诸多国内一线 IC 设计公司和研发机构中投入使用，得到了客户的高度认可。

未来，华大九天将进一步加速发展，逐步完善 EDA 产品工具链，在仿真方向，充分发挥技术特长，打造优势产品集群“高速高可靠全仿真系统”及其应用解决方案，将全面覆盖模拟仿真、射频仿真、Fast SPICE、数模混仿等领域，赋能我国集成电路设计验证事业高质量快速发展。

| 测例 | 运行时间 | | 加速比 |
|---|---|---|---|
| | CPU仿真器 | ALPS- GT | |
| 高速 ADC | 100.8 天 | 6 天 | 16.9X |
| Serdes_TX | 115 天 | 5 天 | 23X |
| Serdes_VCO | 94.9 小时 | 9.8 小时 | 9.7X |
| PLL | 735.3 小时 | 100.8 小时 | 7.3X |
| DC DC Converter | 38.4 小时 | 7.3 小时 | 5.3X |
| CIS 阵列 (300X300) | 94 小时 | 4.5 小时 | 21X |

表 3 ALPS-GT vs. CPU 仿真器对比数据

# E-pak 1.6T以太网SOC IP内核

Precise-ITC

Precise-ITC 的 E-pak SOC 内核是一种多速率的以太网聚合器，它支持 800GE 到 1GE 的支路组合。E-pak 1.6T 采用了 112G/s serdes 和 56G/s serdes，是我们第四代 E-pak 解决方案。SOC 包括 Epak 1p6T MC PCS 和 Epak 1p6T MC MAC 内核。

支持以太网协议为 800GE，400GE，200GE，100GE，50GE，40GE，25GE，10GE 和 1GE。这款 IP 内核支持以太网速率聚合高达 800GE 的任何合法组合。这款 IP 内核支持多达 8 个以太网通道。它与最新型 112G/s serdes 一起运作时发挥最高效能。在以太网 SOC 市场的类似解决方案中，这款 IP 内核能够为时钟频率为 670MHz 至 1.6GHz 的 7nm 芯片提供最小内存占用面积。

## 800GE 支持

这款 IP 内核支持使用一个完整 800GE MAC 和一组 2x400GE“绑定”的 PCS。800GE 利用 112G/s serdes，并在一个“绑定”的 2x400GE PCS 上使用虚拟逻辑通道，这大大提升了 800GE 运行的电源效率。这款 800GE 符合以太网技术联盟标准（Ethernet Technology Consortium Standard）。

## 综述

多通道 MAC 的北向接口提供了一个可配置的系统接口。多通道 MAC 管理各个 MAC 与分配的 I/O 或 I/O 组之间的映射。

南向接口是映射（在 PMA 层）到片上的 SERDES。这款内核起到信道校准和 FEC 作用（如果适用）。

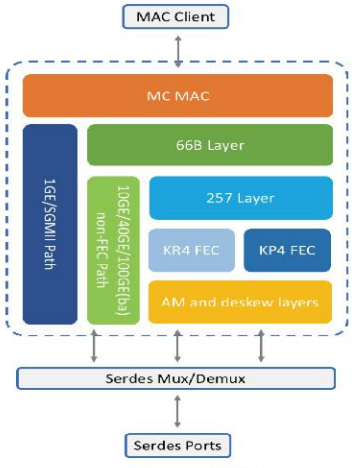



图 1 E-pak 1.6T 框架图

## 优势

- 在 serdes Mux/Demux 中的 TX 和 RX 方向上的所有 serdes 通道之间的数字交叉开关
- 将各种速率的以太网流组合到 MAC 的单个多通道接口上
- E-pak 1p6T 允许在任意端口或端口组上支持 1GE*，10GE，25GE，40GE，50GE，100GE，200G，400GE 和 800GE 的上限带宽为 1.6Tbps 的任意组合的访问连接
- 支持 IEEE 802.3 所需的 FEC 差异 - LL FEC RS（272，258），KR4 FEC RS528,514，KP4 FEC RS544，514，FC FEC（2112，2080）
- 支持 HiGig，HiGig+ 和 HiGig-lite
- 在不会影响现有流量的情况下动态更改任何端口上的速率
- 标准的 ETC 800GE 支持绑定的 2x400GE PCS 和单个 800G MAC
- 每 800G 充分利用 112G serdes 的优势获得尽可能高的端口密度
- 提 供 OTN，FlexE，FlexO，OUT25/50-RS，xGFC 访问端口（可选添加）
- 可选 FC1200 至 256GFC FC2 监控
- 超低延迟和高能效的 FEC
- 支 持 1588，802.1Qbb(FEC) 和 802.3 br express traffic(TSN)

## 应用（图 2）

- 用于数据中心的高密度路由器
- 接入交换机

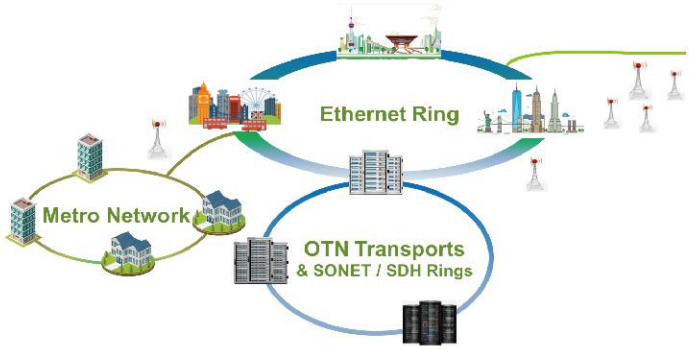



图 2：典型应用

## 功能

### 800GE BASE-R PCS 内核功能

• PCS 层由 PCS 层中绑定的 2x400GE PCS 合成

• 使用 32 个基于 2x400GE PCS 的虚拟逻辑通道来降低 800G 运作的功耗

• 精心设计使用 112 G/s Serdes 为 800G 以太网解决方案提供最高端口密度。

### 400G/200G/100G/50G/40G/25G/10G BASE-R PCS 内核功能

PCS TX Core

• 256/257B 转码（减少 FEC 插入的开销）（不适用于 10GE）

• X58 加扰（可选 bypass）（不适用于 10GE）

• 输入 MII 信号的 64B/66B 编码

• 删除 Idle 块(减少 AM 插入的开销)

• 插入对齐标记（AM）。每个通道的 AM 唯一标记部分是可以通过 S/W 配置的。

• 生成测试模式（test pattern）（乱码）

• 支持第 45 条款 MDIO 寄存器设置

• 检测错误和中断报告

800GBASE-R/400GBASE-KP4/200GBASE-KP4/100GBASE-KP/50GBASE-KP 具体的 KP4 FEC 功能

• KP4(RS544,514) 前向纠错（FEC）的奇偶校验计算和符号分配的插入

100GBASE-KR4/CR4，50GBASE-KR2 和 25GBASE-KR 的具体 KR4 FEC 功能

• KR4(RS528,514) 前向纠错（FEC）奇偶校验计算和符号分配

50GBASE-R4，40GBASE-R，25GBASE-R 和 10GBASE-R 的具体 FC FEC 功能

• RS（2112，2080）前向纠错（FEC）奇偶校验计算和符号分配

PCS RX Core

• 64B/66B 解码到 MII 信号

• 256/257B 反向转码（不适用于 10GE）

• X58 解扰（可选 bypass）（不适用于 10GE）

• 对齐标记（AM）删除（如适用）

• 每个通道的对齐标记上（AM）的唯一标记部分是可以通过 S/W 配置的（如适用）

• 测试模式 (test pattern) 的监控

• 第 45 条款 MDIO 寄存器设置

• 检测错误和中断报告

• 从 TX MII 环回到 RX MII

• 性能监控和数据统计

800GBASE-R/400GBASE-KP4/200GBASE-KP4/100GBASE-KP/50GBASE-KP 的具体 KP4 FEC 功能

• 对齐锁定和通道偏移

• 对通道进行重新排序

• KP4(RS544,514) FEC 解码和纠错

100GBASE-KR4/CR4，50GBASE-KR2 和 25GBASE-KR 的具体 KR4 FEC 功能

• 对齐锁定和通道偏移

• KR4(RS528,514) FEC 解码和纠错

50GBASE-R4，40GBASE-R4，25GBASE-R 和 10GBASE-R 的具体 FC FEC 功能

• 对齐同步

• FC FEC (RS2112, 2080) 前向纠错（FEC）解码和纠错

### 800G/400G/200G/100G/50G/40G/25G/10G MAC 内核功能（每通道）

• TX FCS 的插入

• 生成 TX MAC 控制帧（TX MAC control frame）

• TX 性能监测和数据统计（计数器是 38 位，以容纳 1 秒的速率统计计数）

• 检查和删除 RX FCS

• RX 暂停帧的处理

• RX 性能监控和数据统计（计数器是 38 位，以容纳 1 秒的统计计数）

其他附加功能

• HiGig，HiGig+ 和 HiGig-lite

• 1588v2，OAM，OWAMP，TWAMP 一步和两步时间戳

• xGFC/FlexE/OTN/FlexO/O-TU25/50-RS 访问端口

• FC1200 至 256GFC FC2 监控

• 802.1Qbb 优先级流控制（PFC），多达 8 个优先级

• 802.3br Express Traffic

## 关于我们：

Precise-ITC Inc.（弘智精创高科技公司）正式成立于 2003 年，公司总部位于加拿大首都渥太华，是一家全球首屈一指的 IP 核研发和销售的高科技企业。

公司自成立以来，专注于 IP/ASIC Design/SOC 晶片 / 硬件的技术开发、产品销售以及产品和技术定制服务。目前是以 Ethernet 和 OTN IP 开发为主，最新的产品有 E-pak 1.6T/800G/400G/-FlexE SHIM 和 Cross-connect/Switch IP 核。

公司一直坚持以人才为本，荟萃业界精英，不断研发新项目，与业界各大顶尖科技企业紧密合作，已拥有品质优良的 IP 核 200 多个，并且得到广泛应用。

了解更多产品信息请访问我们的网站 http://www.precise-itc.com

UC TECHIP
优矽科技

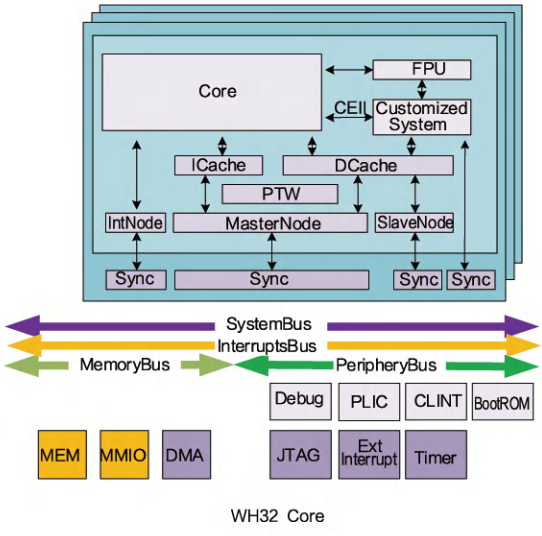
优矽科技成立于2018年3月，是一家以RISC-V开源指令集为基础，深耕处理器微架构知识产权（IP）研发及片上系统（SoC）芯片应用解决方案的科技创新企业，致力于实现处理器及芯片系统与软件的自主可控、安全可信、国产替代。

## WH-32 Processor

WH32 is a Silicon-Proven 32-bit High-Performance Low-Power Processor IP Core

### Feature

uBright Instruction Set Architecture (ISA) compatible with RISC-V architecture
- 1-4 Cores Cluster, 5-stage integer pipeline, 6-stage floating -point pipeline
- Support 32-bit RISC-V [I|M|A|C|F] Instruction Set
- Machine/Supervisor/User Mode
- 4K-64K ICache & DCache
- Dynamic branch prediction to speed up control instruction flow code
- Return Address Stack (RAS) to speed up procedure returns
- Support up to 16 Physical Memory Protection (PMP)
- Support 1-256 Platform Level Interrupt
- Support Virtual Memory Architecture (sv32)
- The CPI for most basic instructions is 1 cycle/inst
- mul may have 3-5 cycle latency
- div may have 3-33 cycle latency
- load may have 2-3 cycle latency if cache hit
- atomic may have 6-7 cycle latency
- 16/32 bit mixable instruction format for compacting code density
- Custom Extension Instruction Interface for customized accelerator
- Support Hardware Performance Counter
- Both RTOS & Linux OS supported




WH32 Core

### Performance、Power、Area[1]

- 64-bit CSR.mtime to record the clock cycle of program execution,64-bit CSR. minstret to record the number of instruction retired.
- Synthesis Frequency/Signoff Frequency[2]: 1.05GHz/~800MHz@22nm
- Performance:

Dhrystone[3]: 1.69 DMIPS/MHz
CoreMark[4]: 2.44 CoreMark/MHz
Whetstone[5]: 18.1 Whetstone/MHz
Area[6] & Power[7]

| Area | | Power | | |
|---|---|---|---|---|
| Total Area （μm²） | 464,641 | Total Power （mw） | MemoryPower （mw） | LogicPower （mw） |
| Memory Area （μm²） | 292,528 | 159.97 | 143.34 | 16.63 |
| Logic Area （μm²） | 172,113 | Total （mw/MHz） | Memory （mw/MHz） | Logic （mw/MHz） |
| Logic Gate Count | 455,325 | 145.43 | 130.31 | 15.12 |

**Notes:**

1.RV32IMAFDC/Single Core/32KB L1I$(VIPT)/32KB L1D$(PIPT) w/i ECC/256Entries TLB, evaluated under 22nm Low Power Process Technology, by using 9track StarndardCell
2.HVT+RVT+LVT/SSG/0.72V/125C+-40C
3.-O2 in Linux4.19 Kernel
4.-O2 in Linux4.19 Kernel
5.-O2
5.HVT+RVT+LVT /1GHz Synthesis/ SSG/0.72V/125C° +-40C°
6.HVT+RVT+LVT /1GHz Synthesis/ SSG/0.72V/125C° +-40C°

## 优矽科技-致力于提供更好的RISC-V解决方案

www.uctechip.com aries.chen@uctechip.com

# Seamless Microsystems

Digitizing Your World Seamlessly

## Best ADCs and DACs


RADAR
LiDAR

Wireless

Imaging

www.seamlessmicro.com
info@seamlessmicro.com

# Pulsic Unity 芯片规划器

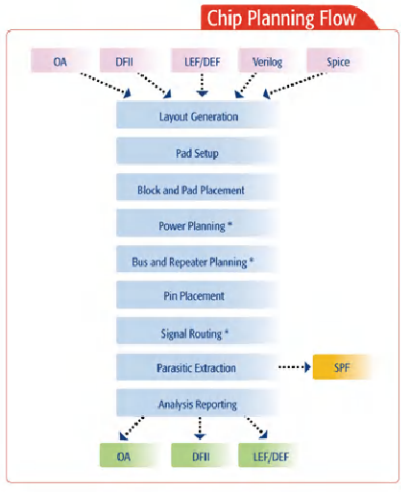
凯为科技股份有限公司

## 针对客制化设计的阶层式芯片平面规划

近年来半导体工艺的进步，芯片朝着体积越来越小和越来越复杂的设计。但仍然有很多的客制化设计团队使用着和10年以前相同的芯片平面规划的手法。Pulsic（派斯克） Unity 芯片规划器是第一个实现针对客制化设计的阶层式平面规划，这可使客制设计团队有效的管理复杂的设计并可以缩短设计的时间和提升设计的质量。

## 芯片复杂程度提升需要新的处理方法

当各领域的芯片设计越来越复杂，设计工具的目标也必须持续改善来维持设计速度甚至加快。自动化、阶层式的平面规划在数位设计流程是基本的步骤。但许多的设计工具却无法处理客制化设计的特别需求。所以直到现在，需多的客制化设计团队仍然是由下至上的手法来做设计，但这类的手法在完成设计前无法了解芯片的拥挤程度和顶层的寄生参数。



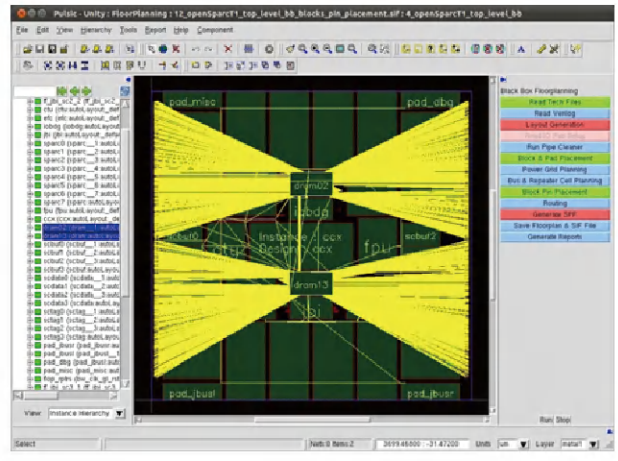

在手工设计中缺少自动化针脚放置和布线成为了问题，而且每的层别一般都是独立建立无法互相的思考配合，所以在由下至上的设计过程中往往在完成设计时会将Si资源和人力资源浪费。另外在设计过程中也会遇到前端的设计改变，这会导致效率管理的困难同时也会失去生产力。

## 完整的阶层式平面规划快速客制化设计的完成

Pulsic（派斯克） 芯片规划器使用一个初步的完整阶层，可以处理许多关键的问题，无论是由下而上或由上至下的平面规划。藉由高度自动化芯片规划器提供精准且高质量的结果并且能使客制化设计团队快速且轻易的反应任何前端设计的变化。芯片规划器也将经常使用且必要的工具整合在平面规划器的环境界面中，让使用者可以依照界面提供的流程快速的完成设计。

## 客制化设计的全新方法

当设计者面对各种独特的挑战，客制化设计往往会包含大量



# 新一代人工智能芯片与系统方案

| 25 年 VLSI 优化设计 | 5 年 + AI 设计 | 10+ 成功案例 | 客户满意度 |
|---|---|---|---|

风兴科技 WindoRise Tech

## 高性能 CNN 推理 IP

- 支持稀疏神经网络，包括随机和规则稀疏，网络运算量与总体稀疏度成反比
- MAC 数目不变的前提下，神经网络的推理速度与稀疏度成近似正比例关系，可以将稀疏度直接转换成更高的能效和推理速度
- IP 的 MAC 数目可以裁剪，可以使用从端到云的推理应用场景。典型的 MAC 数目包括 64/128/256/512/1024/2048/4096，能够满足端到云的全栈需求
- 特别适合执行 ResNet/MobileNet-V2/ShuffleNet 等轻量级残差神经网络计算，支持 FC 网络
- 支持 Activation 稀疏，所有运算都为有效运算，不执行（被）乘数都为零 MAC 运算
- 支持新型 Log-Domian 浮点推理，模型不需要重新训练，推理过程无乘法，总体功耗低于定点推理单元

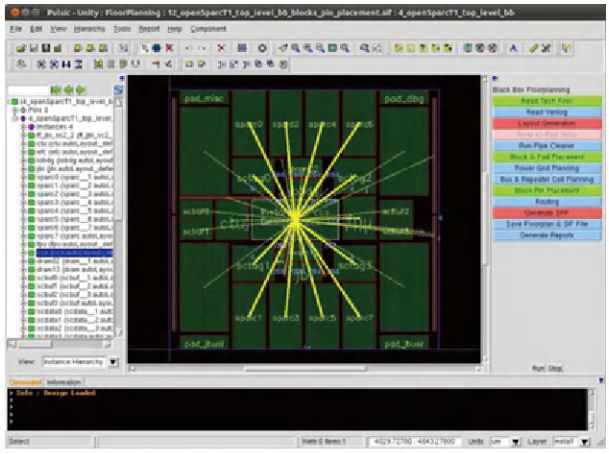
## 低复杂度、低功耗 LSTM 加速 IP

- 采用算法 - 硬件联合优化策略
- 支持稀疏 LSTM 网络
- 处理并行度可调节，能够适应不同的算力需求
- 片上存储最低可达 30KB
- 采用自主研发的量化机制，核心计算单元免除使用乘法器，以降低功耗
- 具备较强的灵活性，支持各式 LSTM/Bi-LSTM 网络，网络层数不限

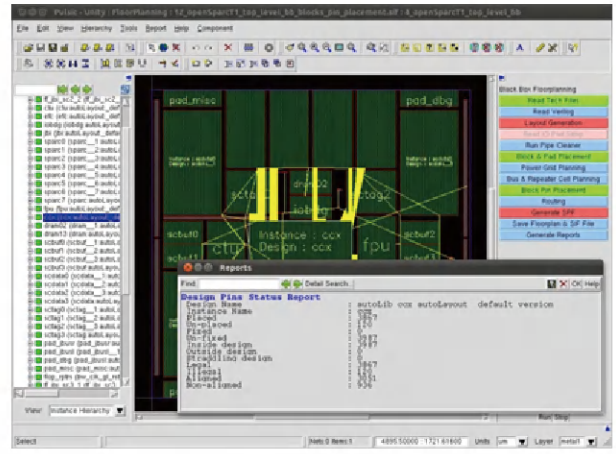
## 行业算法解决方案

- 通过与行业客户的充分合作，风兴掌握了下列行业算法解决方案
- 完整的人脸处理相关算法
- 多相机人体再识别算法（Re-ID，公开文献中表现达到 SOTA 水平），用于智慧零售，人员监控等
- 多种光谱下的高鲁棒性物体检测算法（掌握热红外目标检测算法）
- 货物标签精准识别算法，可以用于低成本物流管理
- 车辆类识别算法，包括车牌，车体再识别等，可用于智慧交通
- 工业瑕疵检测算法
- 工业现场检测算法，指针仪表读数提取、石化现场异常识别等
- 基于 AI 的图像视频压缩算法

**强大的 AI 算法开发能力，快速为客户定制算法解决方案**



將詳細的飛線彙整為總線簡易的表達連線情況



芯片规划器透过设计的向导快速地完成设计

的IP和类比设计，但又只能在有限的层别完成绕线。还有工艺越来越小的时代能够绕线的范围也越来越小还要考虑金属层相关的寄生参数。在高端工艺中(28nm以下)，设计工艺的规则限制也有新的方法。Pulsic(派斯克)已经雍有超过10年高端客户的经验并开发出芯片规划器来处理独特的需求和客制化设计。

高效的客制化设计平面规划需要一系列的上至下设计和下至上设计的优化，并可以考虑下方阶层将针脚放置，然后使用此针脚作为各个阶层的连接点。

芯片规划器的面积评估工具可以精准的分析每个阶层的设计需要的面积来符合内部的所有元件。另外针脚的放置也会考虑下层的让走线尽可能减少与减少线之间的交错，而且也可以轻易的添加屏障，这些都可以帮助设计减少噪声得到更好的结果。另外芯片规划器的块摆放工具可以自动的摆放IP和软块。还有”Push Down”的工具，这可让设计者将上层的电源总线和绕线架构放至下方的阶层，使下层可以看到上方阶层的信息，可以让上层的信息可以遍及所有的设计阶层。另外芯片规划器还有阶层ECO(Engineering Change Order)工具，这个工具能使设计者快速的载入新的设计来替换原本旧的设计。

## 快速的平面规划

由于现代设计的周期如此紧奏，设计者往往没有时间去发掘新的平面规划的方法，但在Unity平面规划器的可变动性很大，可以让使用者随意变更界面结构使使用者可以发掘不同的方法去完成芯片的平面规划，从中寻找更快速更理想的方法。

## 优势

- 针对客制化设计唯一由上至下的阶层式平面规划器，并达到快速完成设计。
- 发掘更多的选择和工具快速完成平面规划，并且可以精准的面积评估和寄身参数计算。
- 可以在设计初期快速取得精准的寄身参数来做时间的分析。
- 快速且精准的执行ECO。

## 特点

- 阶层化的平面规划设计。
- 包含数位电路和类比电路的阶层式面积评估。

•自动摆放IP及软块和自动调整软块的外型。

•阶层式针脚的自动摆放并自动分类优化针脚的位置。

•依照针脚位置取得最佳的绕线结果。

•完整的阶层式ECO解决方案。

•可使下方阶层看见顶部的电源线和讯号线

•设计的划分

•提供多种输入格式LEF/DEF, CDBA, OpenAccess®, Verilog®, SPICE, CDL, .LIB and .SDC

## 系统规格要求

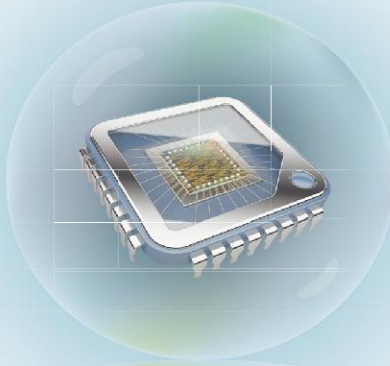
- Linux : x86 and x86_64
- Solaris : Sparc 64 and x86_64

公司网址 : www.kaviaztech.com

SOFICS
SOLUTIONS FOR ICS

SOFICS IP助您提升芯片性能降低成本，缩短上市周期

# ESD保护



# FINFET工艺

**提高性能**

SOFICS IP降低漏电电流，IOT产品单次充电续航时间更长

降低寄生电容可实现更高接口速率（最高可达112GBPS）

支持高压信号提升产品兼容性

**降低成本**

芯片面积更小：同等ESD保护我们的IP只需更小的面积

久经验证的成熟技术不仅降低技术风险，更缩短产品上市周期

货架产品，成本效率更高

## 经高端应用验证的先进工艺

| 16NM | 12NM | 7NM | 5NM |
|---|---|---|---|
| 2017年硅验证 | 2019年硅验证 | 2019年硅验证 | 2020年硅验证 |
| 多家客户量产 | 2家客户量产 | 4家客户量产 | 已有意向客户 |

# 采用IRIS软件进行工艺角与温度扫描分析

翁寅飞——芯和半导体

采用芯和半导体 IRIS 软件来进行集成无源器件仿真分析，配合工艺角与温度扫描模块，快速了解工艺状况和器件随工艺变化特性，对器件精确建模有较大指导意义。

## 前言

随着半导体制造能力的提升，从亚微米进入到纳米阶段，主动式电子元件的集成度随之大幅提升，相应的搭配主动式元件的无源元件需求量也迅速增加。一方面，包括滤波器、耦合器、巴伦等无源器件已成为射频 / 微波电路系统的重要组成部分。另一方面，随着工作频段的提高，需要对这些无源器件进行精确的 EM 仿真，得到无源器件的高频特性。如何快速准确实现无源器件的设计已成为射频工程师面临的一个关键问题。本文的目的是给大家介绍如何采用芯和半导体的 IRIS 软件实现无源器件的 EM 仿真。

IRIS 是一款射频 / 微波芯片、模块、封装和电路板的无源器件和互连结构的三维电磁场仿真工具。软件采用了业界领先的多层结构矩量法加速技术，快速精确模拟复杂电磁效应，包括导体趋肤效应、邻近效应和多介质损耗。支持多核计算和分布式计算等加速技术，大大降低了电磁场仿真时间，提高设计效率。IRIS 是专业针对无源器件进行三维电磁场仿真的软件，软件提供的这种设计流程将帮助工程师大大减少无源器件设计时间。

## 仿真流程

### 模型导入

IRIS 提供的无源提取方案是集成于主流的 IC 版图设计工具之上，避免了数据转换，导入导出带来的风险。同时版图和仿真设置在界面上是一体化的，默认设置也可以得到较好的仿真精度。IRIS 将每个仿真单元称为一个 iCell，用户需要在版图上选取关心的提取部分进行 iCell 的创建，设置完频率范围、温度等就可以提交仿真提取任

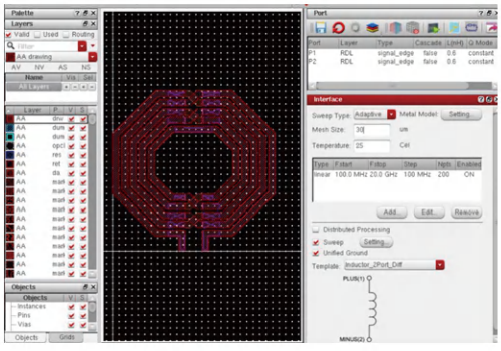


图 1 E-pak 1.6T 框架图

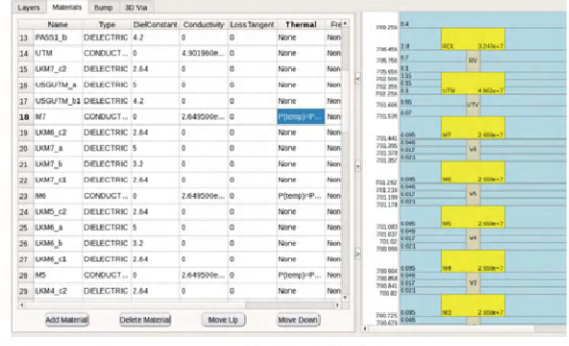


图 2 叠层和材料设置

INTRINSIC ID

# 基于SRAM的不可克隆的设备身份标识

“用兵之法,无恃其不来,恃吾有以待也;
无恃其不攻,恃吾有所不可攻也。”
------孙子

## 为保护物联网安全而与如下攻击作斗争

- 逆向工程
- 伪造
- 克隆

## 主要对标市场

- 各类安全芯片
- 通用MCU芯片
- 连接类芯片
- 蜂窝网络物联网
- 传感器芯片
- 工业物联网

www.intrinsic-id. com

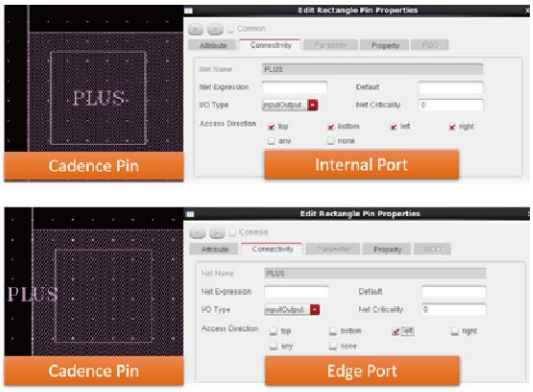



图 3 端口设置

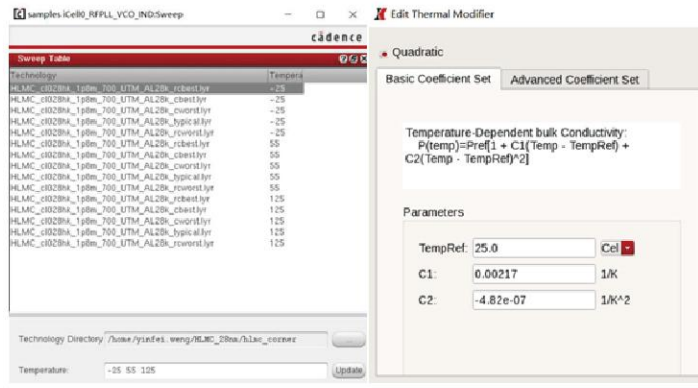



图 4 仿真环境设置

务。其中界面上 Sweep 按钮，提供了温度和工艺角扫描的功能入口。作为用户在做扫描前，需要准备好不同工艺角的工艺文件。

### 叠层设置

IRIS 支持叠层的分层设定，支持叠层的增加和删除，可以对叠层信息进行修改编辑操作。并支持材料信息的增加，修改和删除操作。金属材料包含温度系数设定,材料包含 DK/DF 模型设定。

### 端口设置

IRIS 支持版图工具 Pin 或 Label 标识自动生成仿真端口，包括 edge 和 internal 两种类型。

### 扫描仿真环境设置

IRIS 提供一个直观的界面，通过选择工艺角文件夹、指定温度个数，软件会自动生成各种扫描场景的组合。右侧是金属温度系数的表格，包含了基准温度和两个可自定义的温度系数。

### 仿真结果查看

温度扫描设定 -25℃，55℃，125℃三个值，工艺角固定为 typical，结果如下图。理论分析和仿真趋势一致，即随着温度增加 Qmax 值降低。

工艺角扫描设定 rcbest，rcworst，typcial，cbest，cworst 五个值，温度固定为 125℃，结果如下图。理论分析和仿真趋势一致，即 cbest 下电感的谐振频率最大，cworst 下电感谐振频率最小。

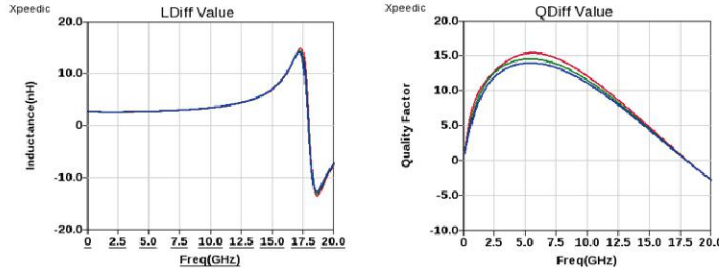



图 5 仿真结果

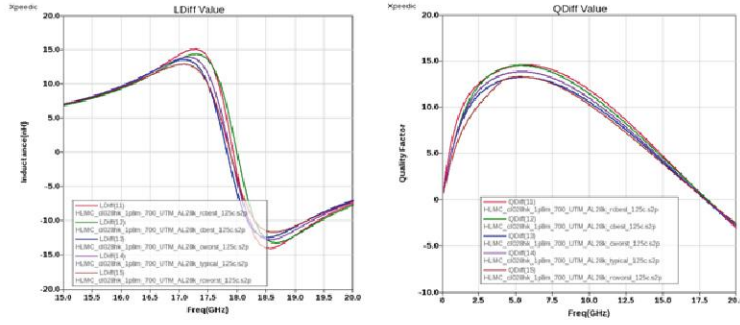



图 6 仿真结果

## 小结

本文介绍了采用芯和半导体的 IRIS 软件进行无源器件的 EM 仿真方法。根据具体的电感仿真案例介绍了 IRIS 快捷的温度及工艺角扫描仿真流程。


# 万物的GPU

A系列GPU是Imagination 25年行业经验的结晶。凭借灵活的设计和可扩展的架构，“万物的GPU”将帮助您获得绝对竞争优势。

imaginationtech.com

Imagination


## 设计服务 Design Service

星矢集成电路设计公司的核心团队拥有非常强大的技术背景，成员主要来自 Hisilicon、IBM、AMD、Qualcomm、Nvidia 等知名企业。专注于集成电路设计服务，包括短期和长期的服务。我们可帮助客户开发下一代旗舰产品系列 ( 移动设备、复杂路由器 / 交换机、消费产品、存储、微处理器、图形处理器等 )。在构建复杂的 SoC 方面，我们致力于为客户提供高效、可靠的模拟版图、数字验证、DFT 及数字后端的专业化服务。

## 驻场外包 Onsite Outsource

我们帮助客户以高效、低成本的方式找到他们需要的专业知识。我们的工程师拥有丰富的的行业经验，在在多个项目、技术和应用领域积累了专业知识，包括在 7nm 节点范围。星矢的设计中心位置是根据技能水平、可负担性和可扩展性来选择的。我们的项目经理可以迅速创建一个理想的团队适合您的要求，时间表和预算；我们的工程师使用经过测试的沟通和报告流程，与客户团队顺利集成。

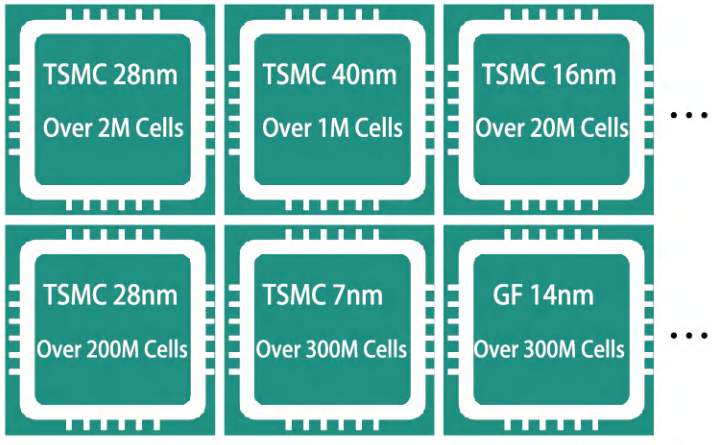
## 技术亮点 Skill Highlights

- Wide range technology project experiences, from 180nm to 7nm
- Experience on both top and block level PNR design
- End to end capability from RTL to GDS out
- One Button automatic flow to run through the block level PNR
- Rich in house utilities and scripts, covering all stages across the PNR

**Seiya Design**
无锡星矢集成电路设计有限公司

(+86)13512529756
www.seiya-da.com
sales@seiya-da.com
江苏省无锡市新吴区国家软件园天鹅座 C 栋 19 楼 1901 室

## 项目案例



# 硅验证的混合信号 IP 核
# SILICON-PROVEN MIXED-SIGNAL IP CORES

Mixel 是一家领先的混合信号 IP 提供商。我们提供广泛的高性能混合信号连接解决方案。我们的使命是为我们的客户和合作伙伴提供卓越的混合信号、经硅验证的 IP 核，在此过程中创造出差异化的技术，让您的产品脱颖而出。Mixel 的混合信号组合包括 PHYs 和 SerDes，如 MIPI® PHYs (D-PHY℠、C-PHY℠ 和 M-PHY®)、LVDS 和 Multi-standard SerDes IP 核。我们的 IPs 是完整的集成解决方案，包括 PHY、控制器和平台。

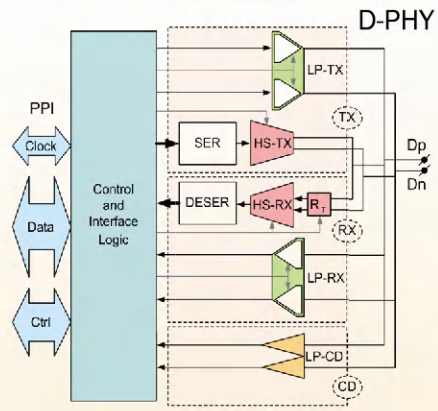
## 特色产品

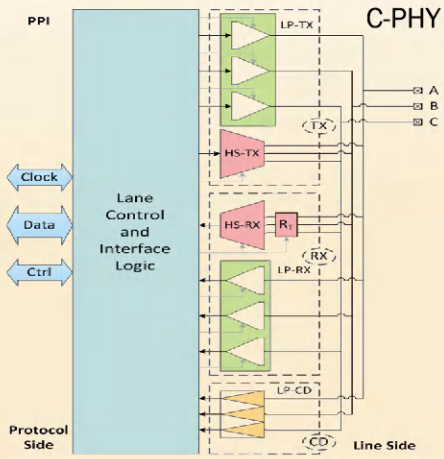
### MIPI D-PHY Universal

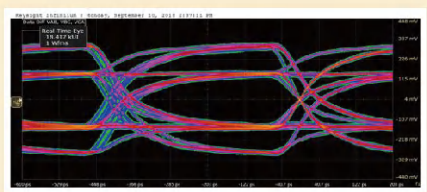
- MIPI Alliance Specification for D-PHY v2.5
- Backwards compatible with MIPI Specifications for D-PHY v2. 1, v1.2, and v1.1
- Configurable for CSI-2, DSI-2, or DSI: RX or TX
- 1 clock lane, 4 data lanes
- Embedded high performance, highly programmable PLL
- PLL supports SSC, Fractional, and Integer modes
- High-speed and low-power modes
- Up to 4.5 Gbps per lane with Deskew calibration
- Supports high-speed TX De-emphasis Equalization
- Supports high-speed RX CTLE
- 10 Mbps data rate in low-power mode
- Low power dissipation
- Loopback testability support
- Calibrator for resistance termination

### MIPI C-PHY/D-PHY Combo

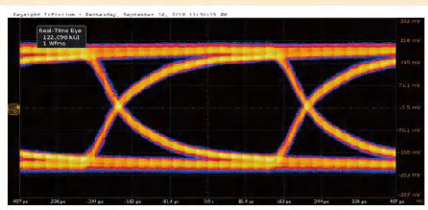
- MIPI D-PHY v1.2 and C-PHY v1.1
- 1 clock, 4 data lanes in D-PHY mode
- 3 data lanes in C-PHY and PLL and bias circuitry
- Configurable for CSI-2 and DSI, RX or TX
- High-speed and low-power modes
- Up to 2.5 Gbps per lane in high-speed D-PHY
- Up to 2.5 Gsps per trio in high-speed C-PHY
- 10 Mbps in low-power mode
- Low power dissipation
- Deskew calibration support in D-PHY
- Loopback testability support



D-PHY@2.5Gbps



C-PHY@2.5Gbps
（5.7Gbps）


mixel
Mixed-Signal Excellence
97 E. Brokaw Road, Suite 250
San Jose, CA 95112
(408) 436-8500 | info@mixel.com

# 广告索引 Advertisers & Web Index

IP与SoC设计

| Advertiser | 广告商名称 | 网址 | 页码 |
|---|---|---|---|
| 北京华大九天软件有限公司 | | www.empyrean.com.cn | IFC |
| cadence | | www.cadence.com | 1 |
| 熵码科技 | | www.pufsecurity.com | 3 |
| 芯动科技有限公司 | | www.innosilicon.com | 5 |
| Perfectvips | | www.Perfectvips.com | 7 |
| FARADAY 智原科技 | | www.faraday-tech.com | 15 |
| 奇捷科技 | | www.easylogic.hk | 19 |
| 平头哥 | | www.t-head.cn | 23 |
| Altran | | www.altran.com | 27 |
| precise-ITC | | www.precise-itc.com | 29 |
| codasip | | www.codasip.com | 31 |
| 成都旋极星源信息技术有限公司 | | www.star-source.cn | 33 |
| 成都纳能微电子有限公司 | | www.nanengmicro.com | 35 |
| SECURE-ic | | www.secure-ic.com | 37 |
| 成都锐成芯微科技股份有限公司 | | www.analogcircuit.cn | 39 |
| CAST | | www.cast-inc.com | 41 |
| Brite | | www.britesemi.com | 43 |
| 南京尔芯电子有限公司 | | | 49 |
| socionext | | www.socionextcn.com | 55 |
| 四川和芯微电子股份有限公司 | | www.ipgoal.com | 57 |
| 苏州国芯科技股份有限公司 | | | 63 |
| onespin | | www.onespin.com | 69 |
| ALLEGRO | | www.allegrodvt.com | 77 |
| Seamless Microsystems | | www.seamlessmicro.com | 85 |
| 风兴科技 | | www.windorise.com | 87 |
| Sofics | | www.sofics.com | 89 |
| INTRINSICID | | www.intrinsic-id.com | 91 |
| imagination | | www.imagination.com | 93 |
| 无锡星矢集成电路设计有限公司 | | www.seiya-da.com | 94 |
| mixel | | www.mixel.com | 95 |
| 国奇科技 | | www.qualchiptech.com | IBC |

## 投稿指南

《IP与SoC设计》杂志和网站www.ip-soc.com欢迎您提供技术性文章、新闻和新产品介绍等等。

为丰富杂志内容、增加在集成电路设计界的知名度，扩大其涵盖范围并更好地服务于本地厂商，《IP与SoC设计》杂志面向广大IP/DesignService/EDA/Foundry厂商征集优秀文章、最新产品和及时性信息。

如果您有什么好的见解需要和我们分享，请联系编辑。

中文稿件（有英文原稿的请附上）优先采用，本刊有权自主修改、编辑文章内容。

**技术文章**

1.一篇技术文章的字数应该在2000至6000字之间；
2.请分别提交文字和插图（文字当中没有内嵌的图片或图形）；
3.文章应该包含适当的设计信息或基本原理、照片、图形、仿真和实测数据；
4.请注明作者姓名、职务及所在公司或机构的名称；
5.论文将经过《IP与SoC设计》编辑审查委员会的审查程序；

**新品发布**

1.请尽量提供简体中文稿件（可附上英文原文），中文稿件会被优先采用。
2.请清晰地写明新产品的名称、型号、性能、独特之处和用途等。
3.产品介绍应少于300字（英文少于150字）。
4.来稿请附产品照片，其分辨率不低于300dpi。
5.留下能提供进一步信息的人的姓名、电话、E-mail。

**产品特写**

1.产品特写集中报道一个具体产品（或产品系列），字数应该在1000字左右，最多不超过2000字；
2.请提供一个描述产品的图片，它将出现在产品特写开始的标题区域（无需说明文字）；
3.重要——请分别提供文字和插图（文本中无嵌入的图片）。文本应该是一个Word文件，每幅图像必须是上述文件格式之一的一个单独文件。为了说明插图在文字中的位置和说明文字，可以提供另一份文字和插图在一起的文件（可选）。
4.产品特写不包括作者署名。
5.请提供联系信息，包括公司名称、联系方式、公司网址。

详情请联系：朱 慧　　电邮：zhuh@jsic-tech.com　　电话：15895811108

QUALCHIP

# 国奇科技

## APPRY优化设计方案 一次量产成功保证!

## High-end SoC Design & Turnkey Services Provider.
## We Guarantee “Direct Volume Production Success”!


优化设计 助造优秀中国芯!

*Optimal Solutions for Total Quality!*

www.qualchiptech.com

# 中国集成电路设计业2020年会

## 暨重庆集成电路产业创新发展高峰论坛

## ICCAD 2020

重庆悦来国际会议中心

2020年12月10日-11日

无锡国家“芯火”双创基地(平台)
WUXI NATIONAL XINHUO INNOVATION BASE(PLATFORM)
地址:无锡市新吴区菱湖大道111号无锡国家软件园天鹅座C座