LPC5500 系列MCU

主打安全 适合通用、工业和IOT应用

基于CORTEX-M33内核的新一代微控制器

SECURE CONNECTIONS
FOR A SMARTER WORLD

LPC5500 MCU 家族

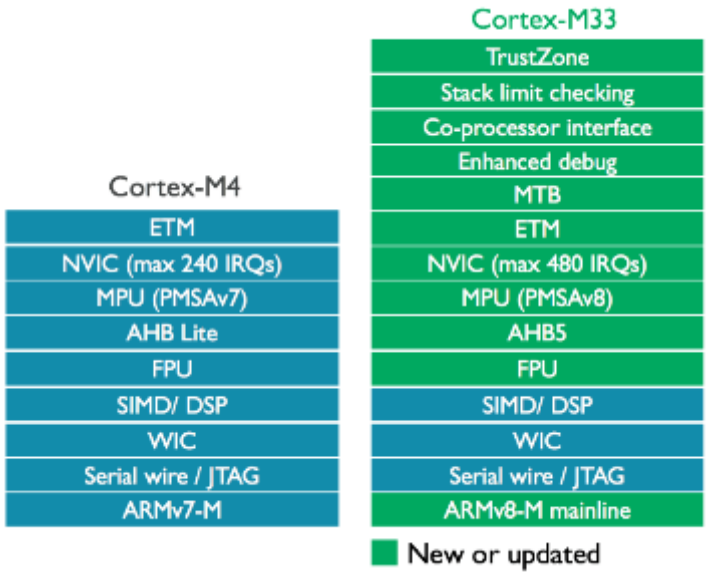
NXP目前能耗最好的

基于Cortex-M33内核的MCU

业内领先的安全功能

- 优秀的能耗数据 - 32 µA/MHz
- 数字型号处理的能力增强了10倍有余
- 集成丰富的安全功能，适用于传感器应用以及安全链接
- MCUXpresso生态环境，可扩展的硬件和软件

首颗全功能的ARMV8-M微控制器



性能对比 和 特色功能

- **相对于Cortex-M3内核，M33内核提升了近20%的性能** (重新设计的流水线)

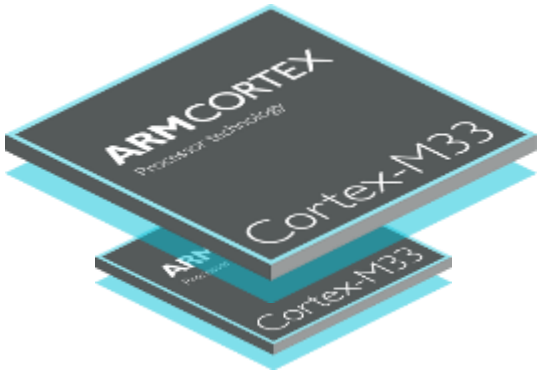
	Cortex-M0+	Cortex-M23	Cortex-M3	Cortex-M4	Cortex-M33
DMIPS/MHz	**0.95**	0.98	1.25	1.25	**1.50**
CoreMark®/MHz	**2.46**	2.50	3.32	3.40	**3.86**

Prelim. Data from Arm for Cortex-M33 implementation at 40LP (9-track, typical 1.1v, 25°C)

- **TrustZone适用于系统级的资源安全隔离，** 可在嵌入式MCU上实现程序的可信执行和物理保护
- **通过协处理器总线可扩展紧耦合加速器**

优秀的能耗

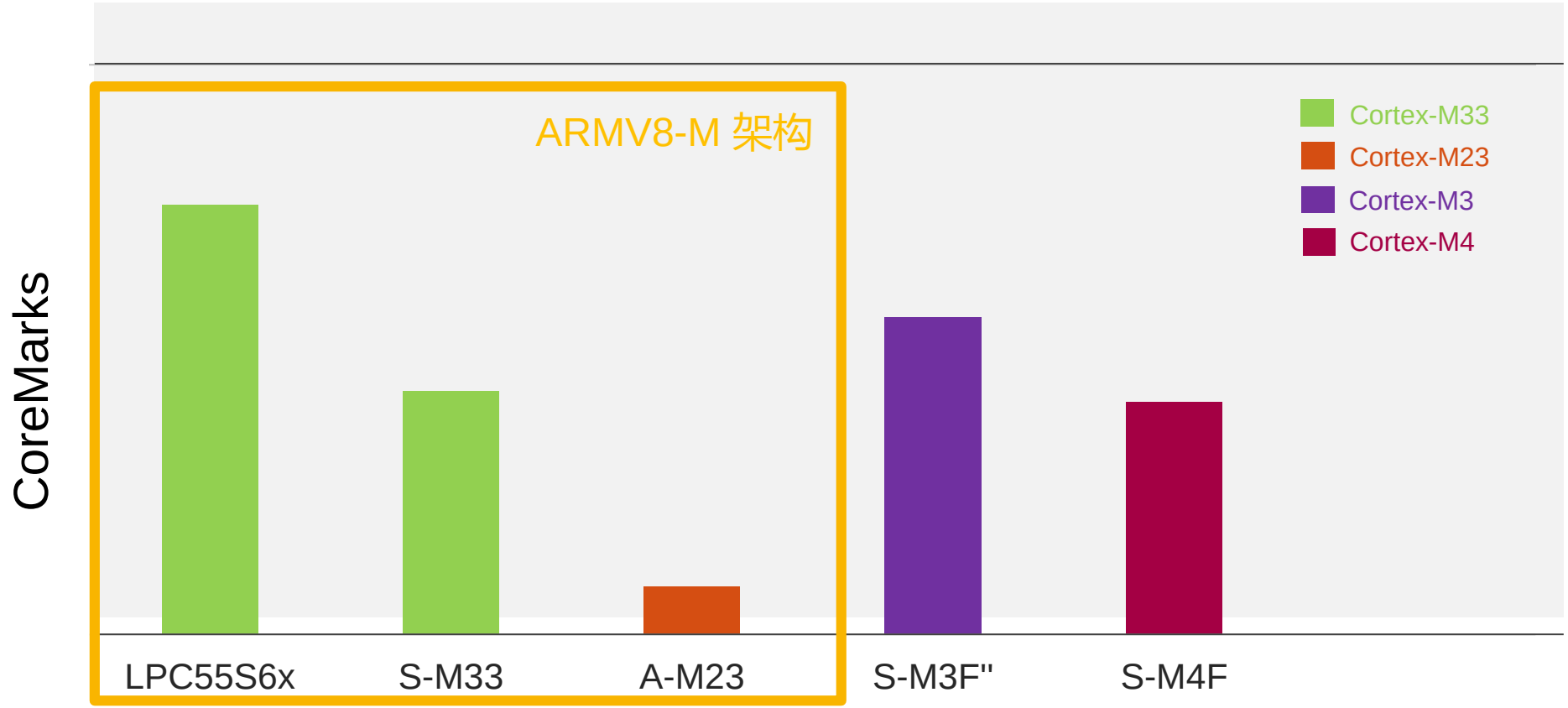
NXP目前能耗最好的MCU系列



- **更强的性能与更低的功耗：可选单双核， 32 µA/MHz 动态功耗**
- **CoreMark实现 755分(100MHz 双核) 确保高性能**
- **通过异步外设和集成电源管理单元来优化系统功耗(集成降压型DC/DC转换器)**
- **NXP轻量级协处理器，可以有效加速DSP和加解密运算的性能，减轻 内核 的负担**
  - ***PowerQuad:*** 10倍以上加速性能，兼容CMSIS-DSP API。有效减轻内核负担
  - ***CASPER:*** 10倍以上的加速非对称密码的运算过程 (mbedTLS)
  - 支持对称加密算法（AES-256）和 哈希(SHA-2)的专用加速器

*vs Cortex-M33

与目前业界MCU的对比



	LPC55S6x	S-M33	A-M23	S-M3F"	S-M4F
CoreMark	755**	427.25**	84.54**	557.76”	404.8**
主频	100MHz†	110MHz	32MHz	168MHz	120MHz
µA/MHz (动态)	32 µA/MHz	60 µA/MHz	25 µA/MHz	517µA/MHz	43 µA/MHz

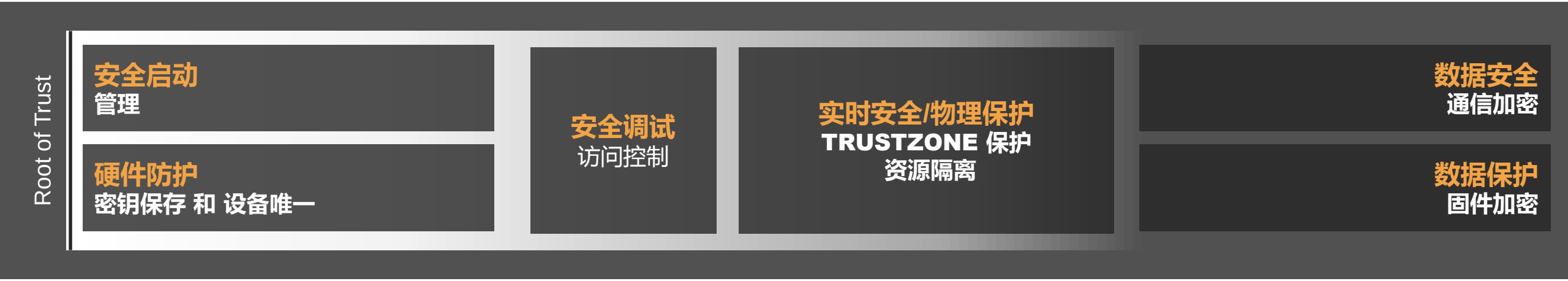
† Dual-core

”Estimated by NXP

** source: http://www.eembc.org/coremark/index.php

NXP 安全执行环境

保护产品免受外界的威胁和攻击



易于扩展的NXP MCUXpresso软件和工具

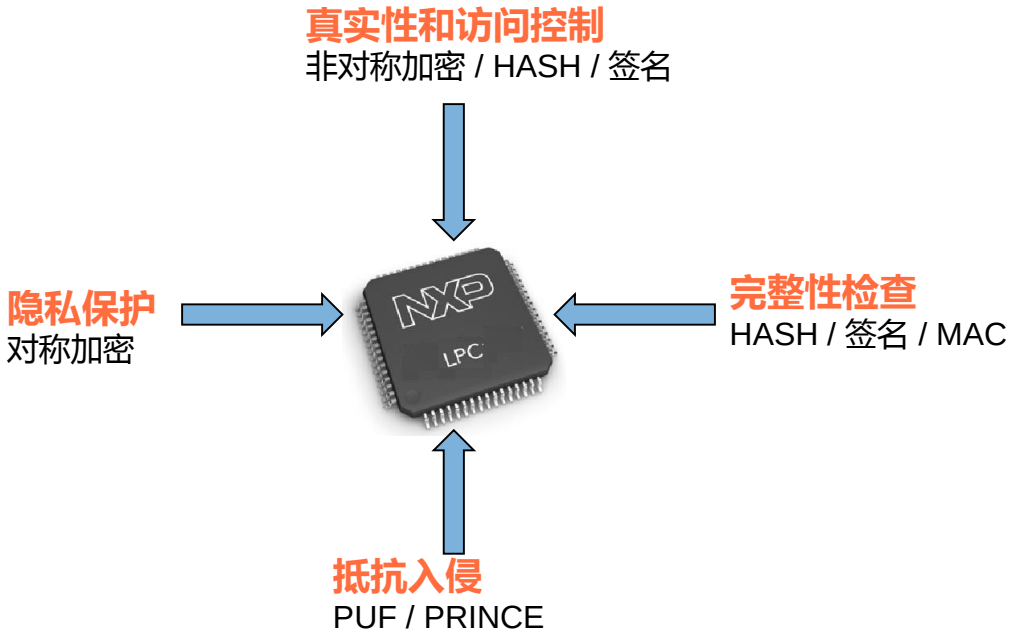
- MCUXpresso配置工具，支持TrustZone配置器
- Flash命令行烧录工具blhost(可以通过串口或者USB接口），具有PUF密钥注入的功能，适用于Windows/MAC/Linux
- 具有 带签名的安全固件生成的上位机工具(elf2sb)，该工具开源并且有命令行和GUI两个版本
- 支持 安全调试身份验证 和 调试身份证书生成工具

支持第三方开发生态增强产品安全访问的特性

- 从产品的 **安全** 开发 / 配置 / 注入密钥 到 **安全** 编程 / 部署 / 管理

加密解密加速器

功能	算法	加速器
对称加密	AES (ECB, CBC, CTR)	**HashCrypt** 128, 192 和 256位密钥
	PRINCE (CTR)	**PRINCE**
非对称加密	RSA, ECC	**CASPER**
Hash	SHA1, SHA2-256	**HashCrypt**
MAC	HMAC, CMAC	**HashCrypt + 软件**
签名	HASH (SHA256) + 非对称加密(RSA, ECDSA)	**HashCrypt + CASPER**



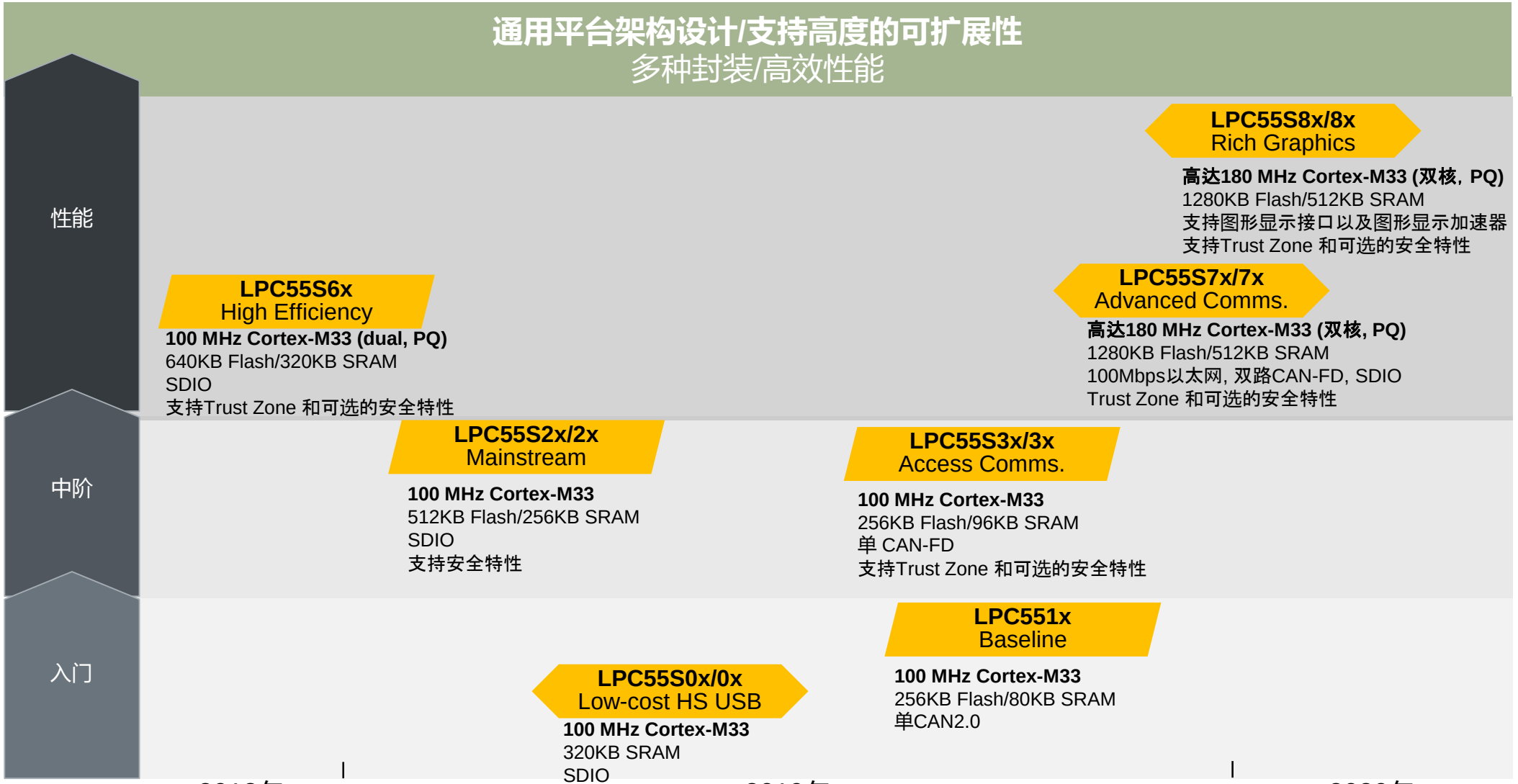
NXP 通过POWERQUAD DSP协处理器提高型号处理的性能

FFT 计算性能 – 消耗的时钟周期

功能	纯C语言实现 -Ofast优化 基于Cortex M33	CMSIS DSP	PowerQuad DSP	HiFi4 DSP
FFT real N=32	6163	2295	273	586
FFT real inverse N=32	8951	2453	329	692
FFT real N=64	13856	5718	465	583
FFT real inverse N=64	20517	6009	553	657
FFT real N=128	30761	10798	1066	993

- 4x 32b 单精度浮点MAC
- 支持以下算法的硬件加速:
  - FFT/IFFT/DCT/IDCT
  - FIR/Dual Biquad IIR
  - Convolution/Matrix
  - Trigonometric Functions/ CORDIC/Sqrt..
- 相对于CMSIS-DSP，PowerQuad至少提高10倍的计算性能
- 有效降低执行DSP任务时的功耗

家族图谱



家族特色外设，

- 全速USB (wo xtal)
- 高速USB集成PHY*
- 50MHz SPI,
- 支持8/10路串行接口 (FlexComm)
- I3C 接口 (LPC557x/8x系列)
- 16位ADC支持1Msps采样率
- 模拟比较器
- 温度计传感器
- RTC
- 工作电压:1.8 到 3.6V
- 工作温度 :-40到105 °C

**不是所有的封装都有该外设*

NXP LPC5500 系列MCU

高度扩展性

家族特色外设:

- 全速/高速USB接口（集成PHY），50MHz SPI，8路或者10路串行接口 (FlexComm)，新型I3C接口
- 支持2Msps采样率 16位 SAR型ADC，比较器，集成温度传感器 和 RTC
- 工作电压1.8 到 3.6V。工作温度 -40 到 105 °C

LPC5500 家族	WLCSP	QFN 48	QFN 64	QFP 64	QFP 100	QFP 144	BGA 98	BGA 196
Rich Graphics LPC558x/S8x					x	X		X
Adv. Comm. LPC557x/S7x					x	X		X
High Efficiency LPC55S6x			x	x	X	x	X	
Real-time Comm. LPC553x/S3x	x	x	x	X	X		x	
Mainstream LPC552x/S2x			x	x	X		X	
Access Comms. LPC551x	x	x	x	X	X		x	
Low-cost HS USB LPC550x					X			

管脚兼容

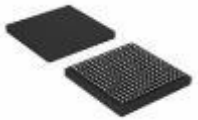
LQFP

LQFP144 vs MaxQFP144

HLQFP100
14x14mm-x,y, 1.4mm- z
0.5mm pitch

HTQFP64
10x10mm-x,y, 1.0mm- z
0.5mm pitch

BGA



BGA196
TBD

VFBGA98
7x7mm-x,y, 0.86mm- z
0.5mm pitch *(depopulated)*

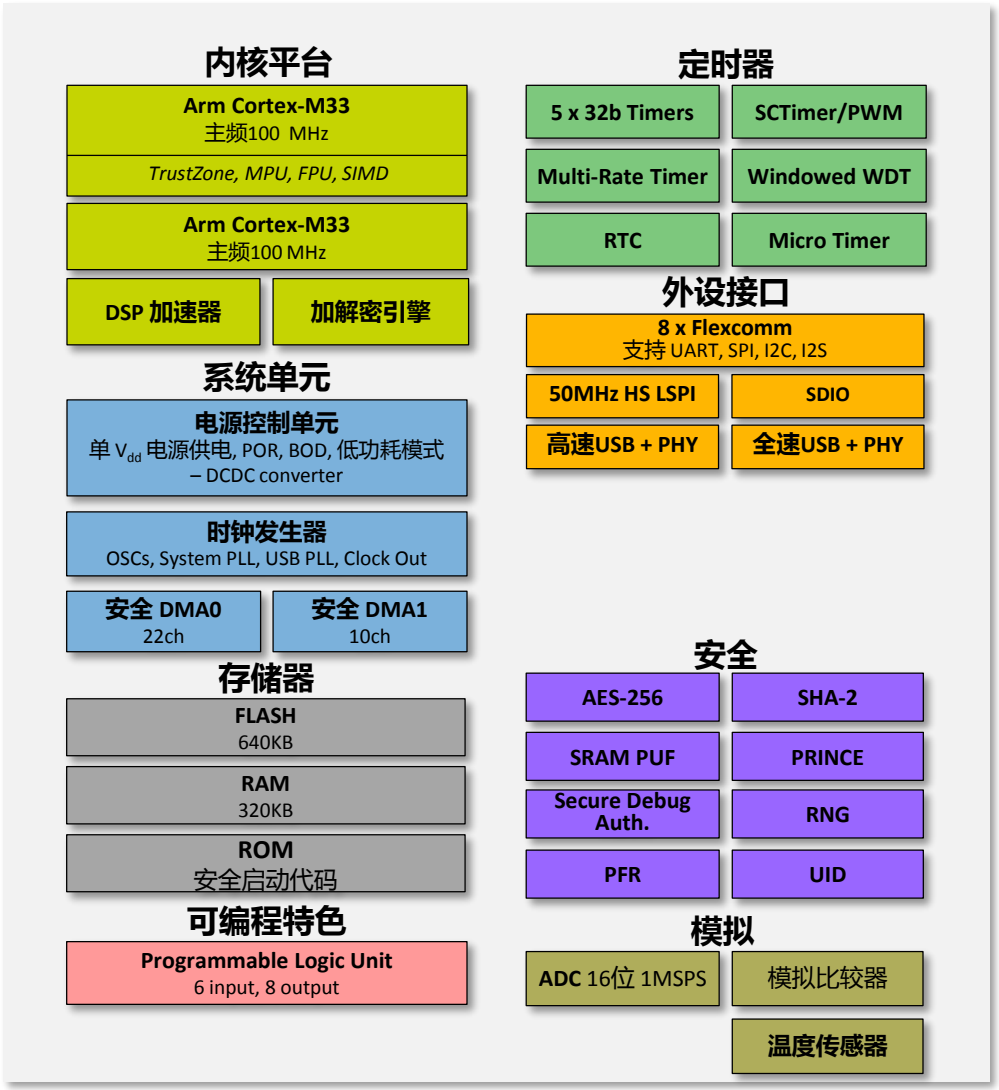
QFN

HVQFN64
9x9mm-x,y, 1.0mm- z
0.5mm pitch

QFN48
7x7mm-x,y, 1.0mm- z
0.5mm pitch

***关于封装信息请参考最新的文档**

LPC55S6x 产品介绍



内核平台

- 100MHz Cortex-M33
  - TrustZone, MPU, FPU, SIMD
- 100MHz Cortex-M33
- 协处理器Coprocessors
  - DSP 加速器 PowerQuad
  - 加解密引擎 Casper
- 多重矩阵总线

存储器

- 640KB FLASH (包括 PFR区域)
- 320KB RAM
- 128KB ROM

定时器

- 5 x 32b Timers
- SCTimer/PWM
- Multi-Rate Timer
- OS Timer
- 窗口看门狗定时器
- RTC
- Micro Timer

外设接口

- 高速USB，集成PHY支持主从模式
- 全速USB，集成PHY支持主从模式，无需外部晶振
- SDIO, 支持两个片选
- 1 路高速SPI接口，时钟可达50MHz
- 8 x Flexcomm 最多支持 8x SPI, 8x I2C, 8x UART, 4x I^2S (双工)

高阶安全子系统

- 受保护的Flash区域 (PFR)
- AES-256硬件加解密引擎
- SHA-2
- SRAM PUF 用于生成和保护密钥
- PRINCE – 加密Flash，边解密边执行
- 安全调试身份认证
- RNG

模拟

- 16位ADC, 16通道, 1MSPS
- 模拟比较器
- 温度传感器

封装

- LQFP100
- VFBGA98
- LQFP64 或 QFN64

其他

- 可编程逻辑单元
- 降压型 DC-DC
- 工作电压 : 1.8 到 3.6V
- 工作温度 : -40 到 105 °C

开发生态系统 - MCUXPRESSO软件和工具

低成本的开发生态

MCUXpresso SDK

MCUXpresso IDE

MCUXpresso Config Tools

易于开发的评估板

- 板载调试仿真器
- 开源PCB，原理图和板级驱动

LPC55S69-EVK

ARM KEIL Microcontroller Tools

IAR SYSTEMS

SEGGER

易于开发安全功能的嵌入式开发平台

帮助客户将产品快速投放市场

LPC5500系列MCU

NXP

LPC5500 系列MCU

Cortex-M33 支持 TrustZone

特色介绍

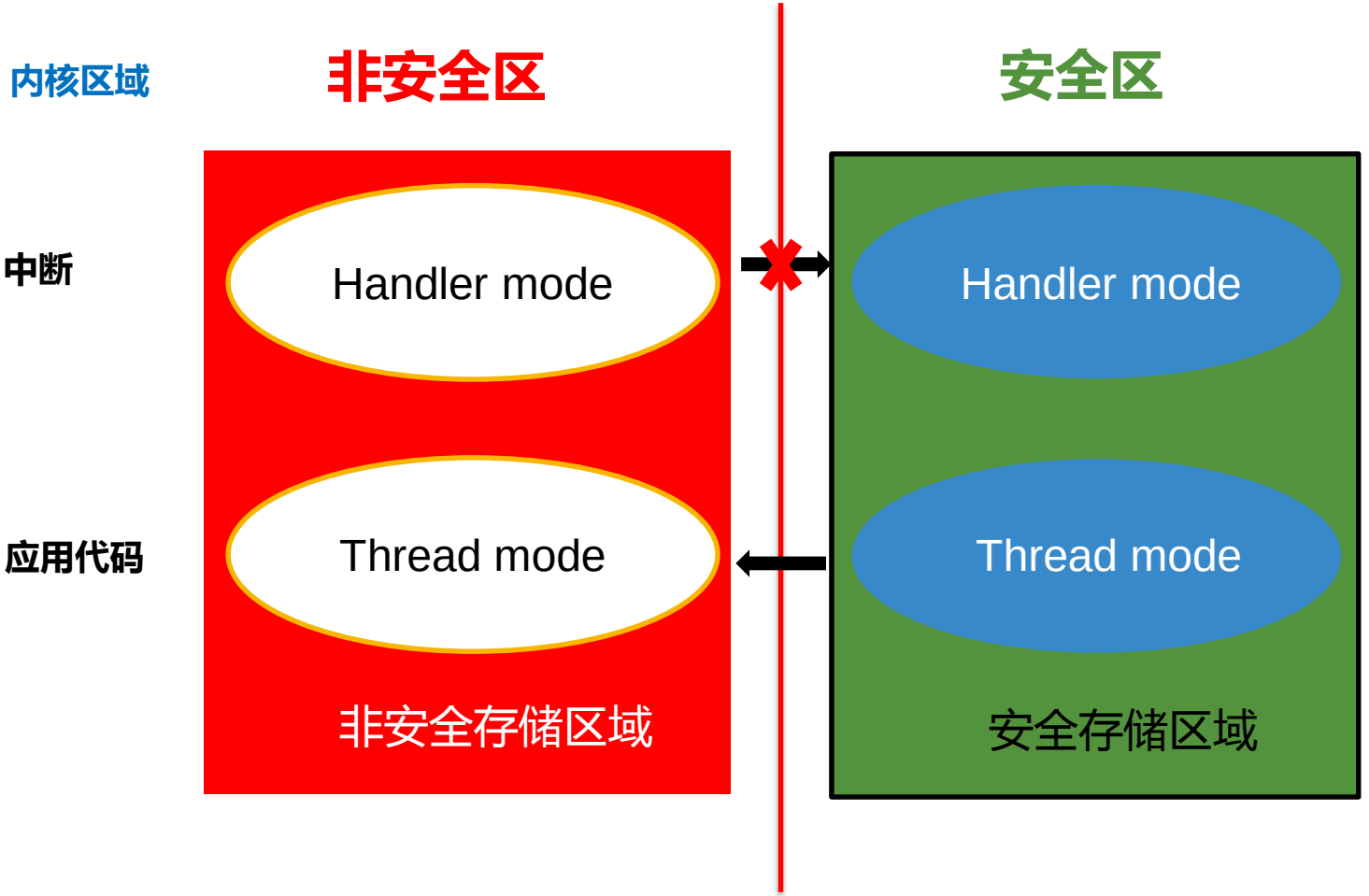
增强工业产品和IOT节点的安全特性

Delivering major breakthrough **signal processing**, **performance efficiency** and **embedded security**

NXP

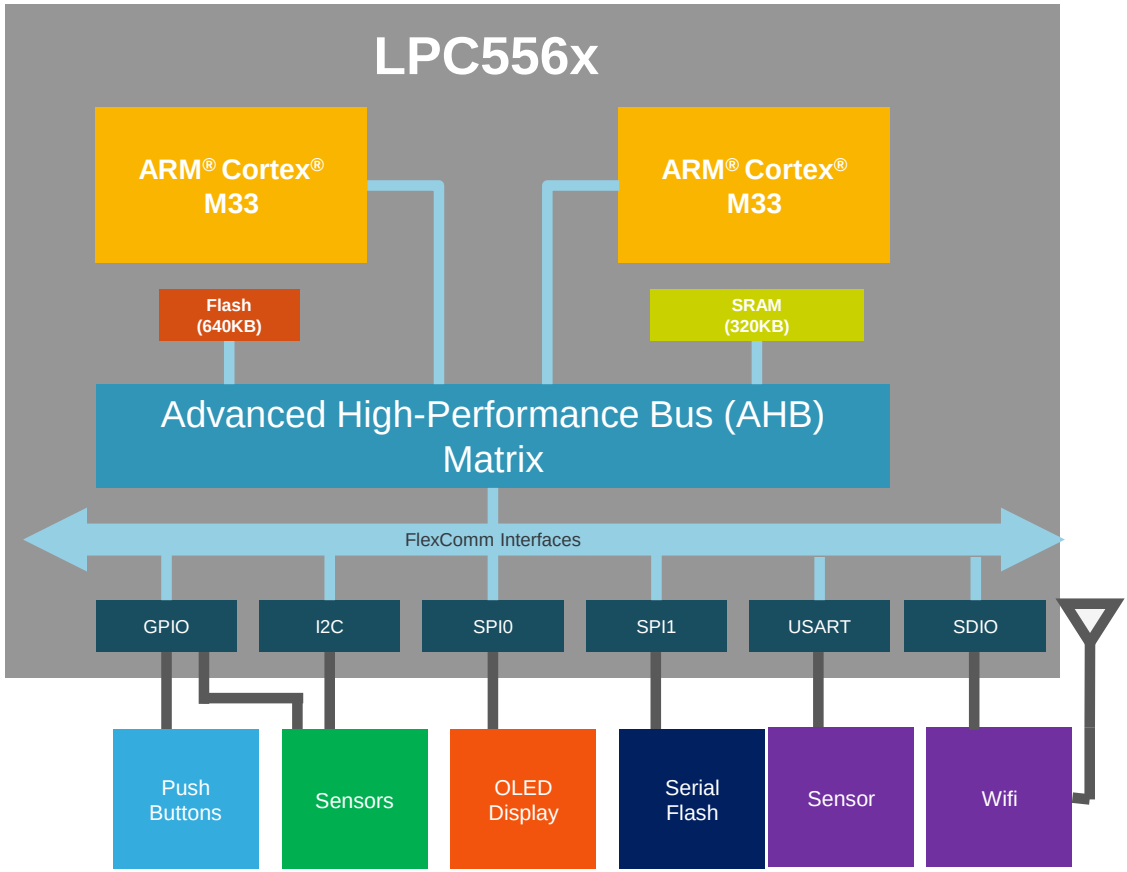
TRUSTZONE – CORTEX-M33内核特色

- **可选配的安全扩展,针对MCU应用优化了功耗**
- **通过SAU和IDAU将系统资源隔离为安全和非安全两种状态**
  - 安全区域： 安全代码+数据(安全任务，安全堆栈, 其他安全数据)
  - 非安全调用(NSC) 区域： 非安全代码访问完全功能的函数入口
- **根据存储器设定划分安全和非安全状态**
- **高可信度的代码**
  - 拥有更高的系统访问权限
  - 防止非可信代码访问
- **安全区的代码可以访问安全区域和非安全区域的内容**
- **非安全区域的代码不能直接访问安全区的内容非安全区的代码可以通过NSC来调用安全区的功能**

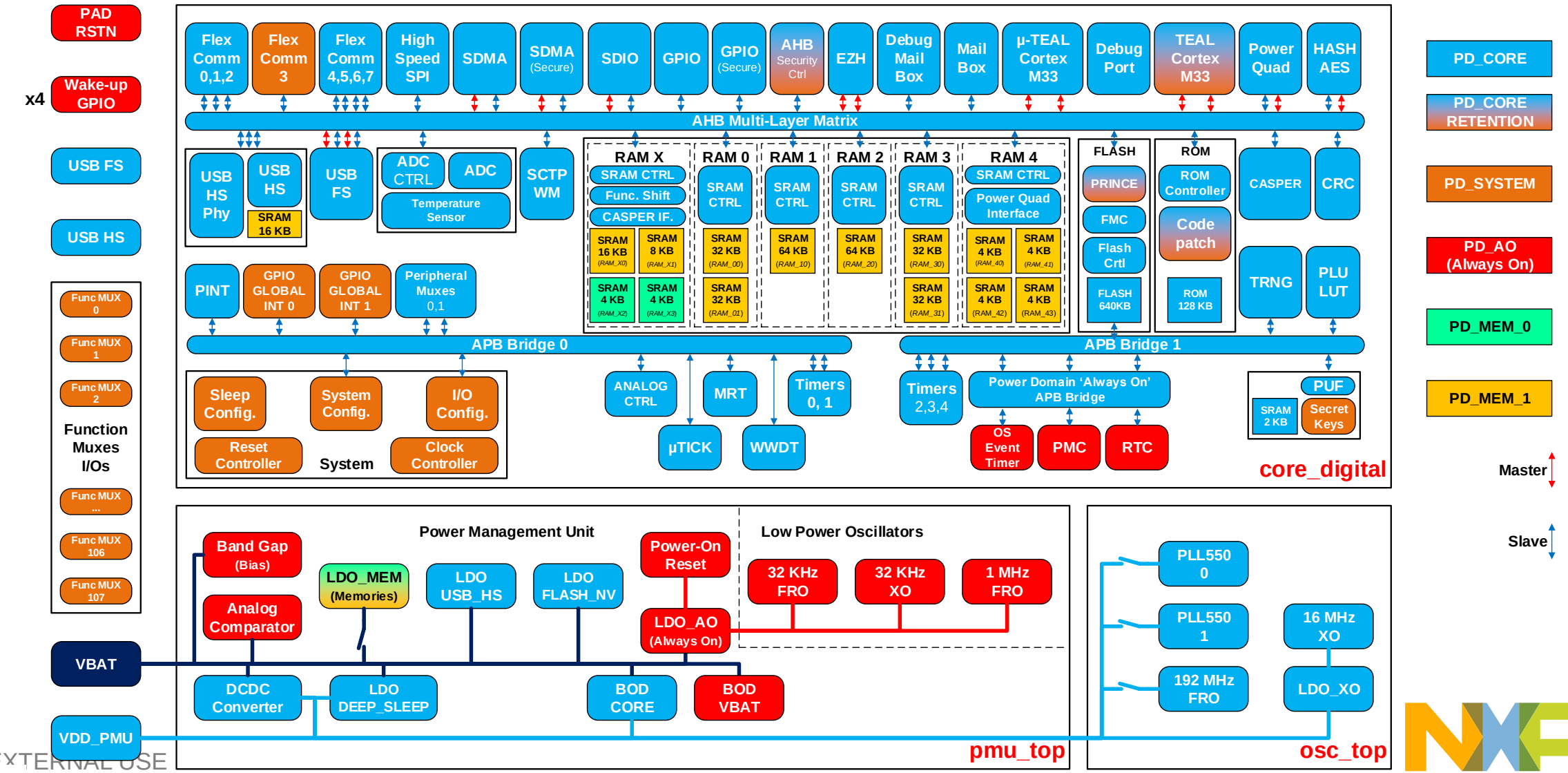


非对称双核架构设计

- **双核架构**
  - CPU0
    - Cortex-M33 带有 NVIC, FPU, MPU, DSP, ITM, SAU和TrustZone安全扩展功能
    - 被配置为主CPU
  - CPU1
    - Cortex-M33 带有 NVIC
    - 处于复位状态直到CPU0将它使能
  - 应用划分
    - CPU1可用于运行系统级任务，CPU0可以被唤醒以利用协处理器处理计算任务
  - 邮箱机制 用于处理多核之间的通信和同步

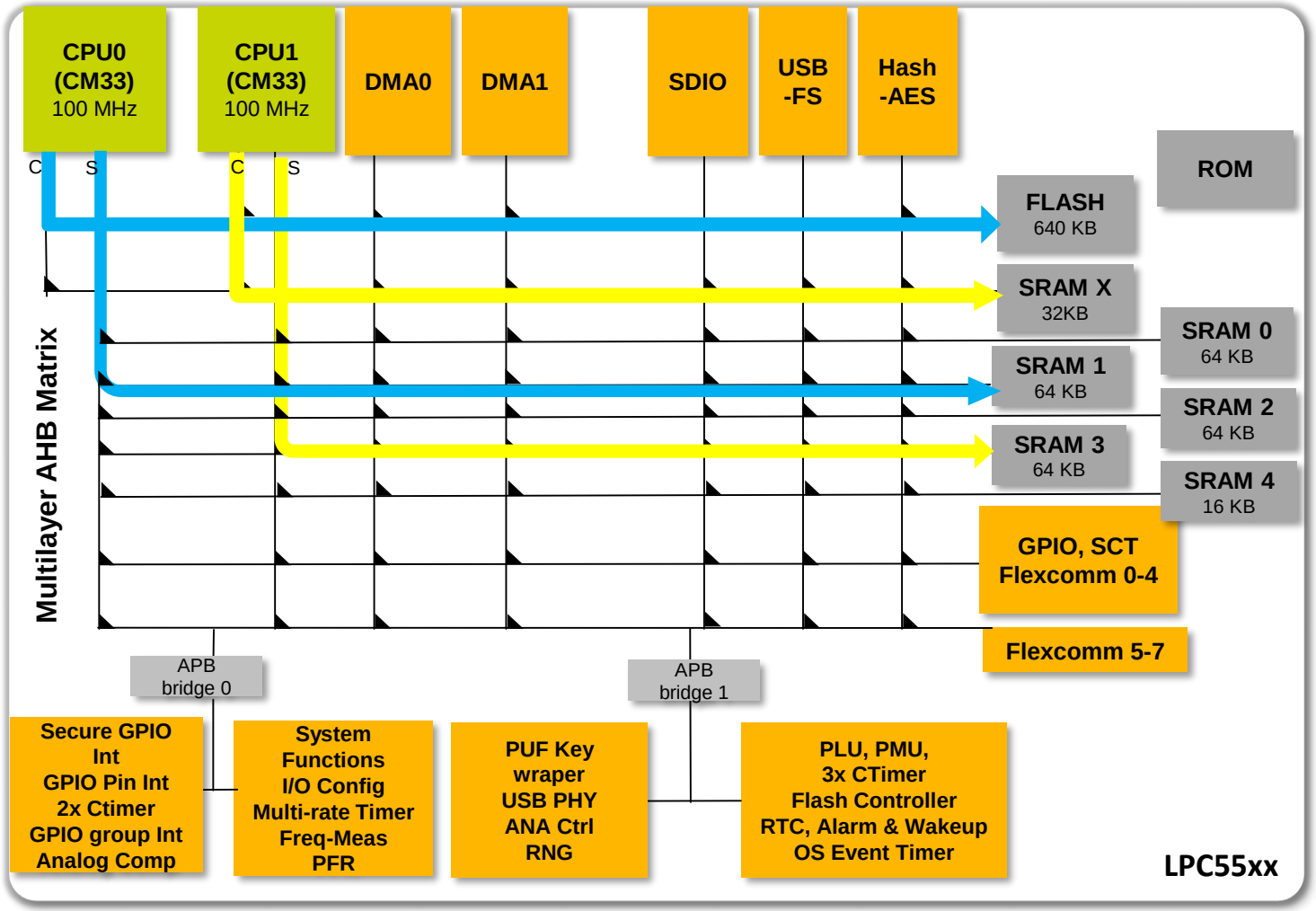


电源域



矩阵总线设计 – 提高性能

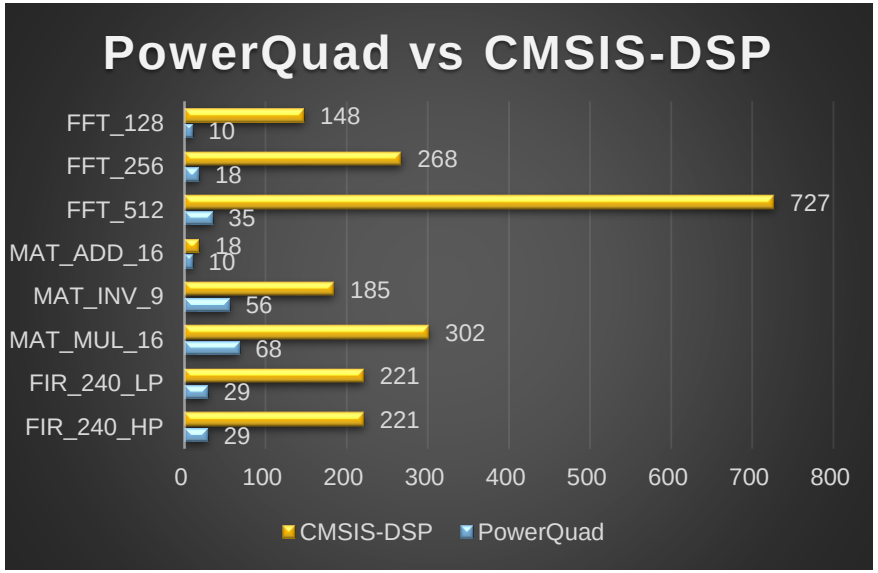
- **高效分区**
  - 允许内核和DMA并行不悖
  - 存储器和外设通过多个从端与APB桥接，总线可以轻松访问各个独立的从端
  - RAM区域地址是连续的
  - **双核: 755 CoreMark**
- **外设访问优先级可配置**
- **系统同步时钟**
  - 同步时钟供给给所有的总线控制器和AHB从机以及APB上的寄存器
  - 独立的异步外设接口时钟
  - 定时器具有独立的异步时钟

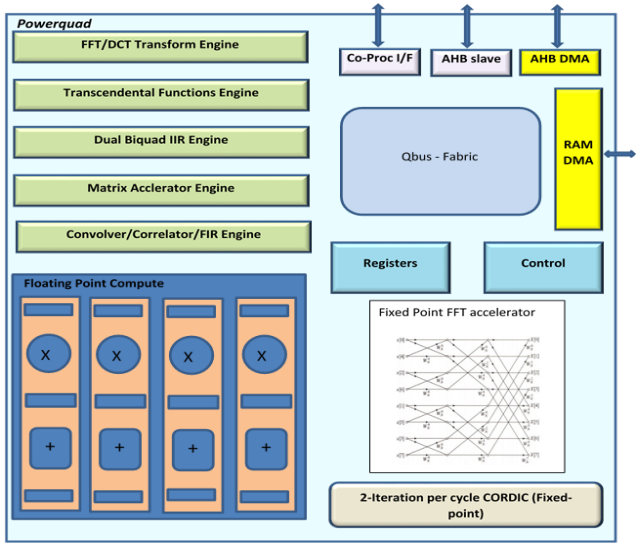


协处理器 – POWERQUAD DSP加速器

- 高性能DSP加速器

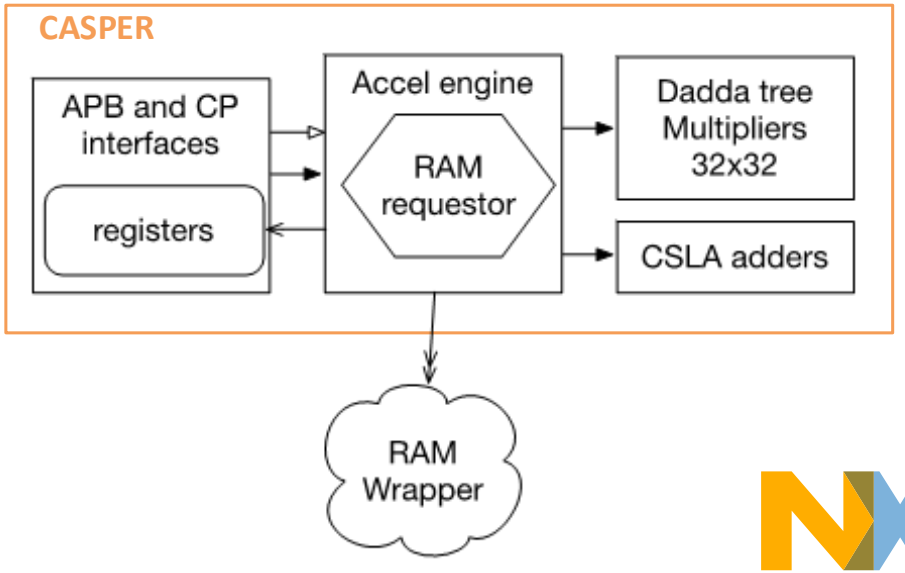
- 4个单精度浮点MAC
- 支持AHB DMA – 读/写数据 输入数据/设置过程/获取结果
- 支持RAM DMA – 128位宽RAM 用于数据输入计算和保存结果
- 基于Cortex-M33协处理器功能，紧耦合操作码(支持两个**MACs并行算**)
- 加速数学运算的过程/DSP
  - **FFT**/iFFT/DCT/iDCT machine
  - Matrix (add, sub, dot, prod, mult, inverse, transpose, scale)
  - Convolution/Correlation/**FIR, biquad(x)**
  - sin(x), cos(x), ln(x), e^(x), e^(-x),1/(x),1/sqrt(x), sqrt(x)
  - Arctan / Arctanh (适用于优化任何CORDI计算)
- **兼容CMSIS-DSP API，** 简化用户移植代码的过程





协处理器 – CASPER 非对称密码学加速器

- 提供基于mbed TLS优化后的库
- 使用ARMv8-M Cortex-M33协处理器总线结构
- 64bit 数据总线
- 脱离CPU ： 一次写入启动加速器并启动序列
- 快速访问共享的RAM区
- 为CASPER RAM接口分配2x 32b RAM，允许64位并行访问
- RAM与系统内存共享（低成本）
- 一组加法器和寄存器允许MAC（乘法和累加）
- 两个32x32乘法器
- 旁路攻击保护
- 使用随机屏蔽
- 执行高效
- 功耗更好



DC/DC电路设计

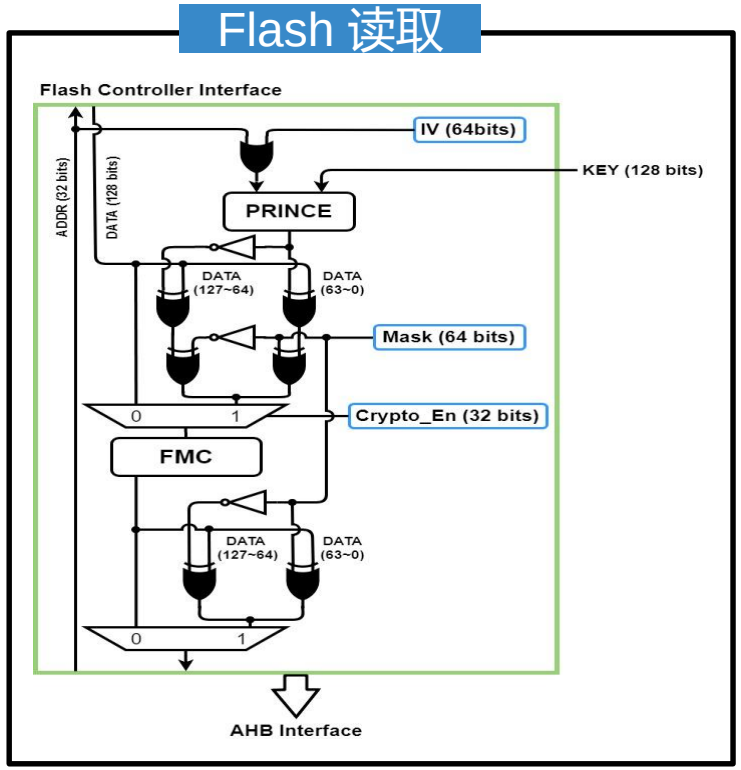
- 进一步降低系统功耗
- 系统为单电源供电
- 可以通过给VDD_PMU一路电源(0.950V – 1.200V)即可屏蔽DC/DC
- 启动时间: ~100us (典型)
- 效率: >80% @负载=50mA,
  >70% @负载=4mA
- 设计请参考AN12275

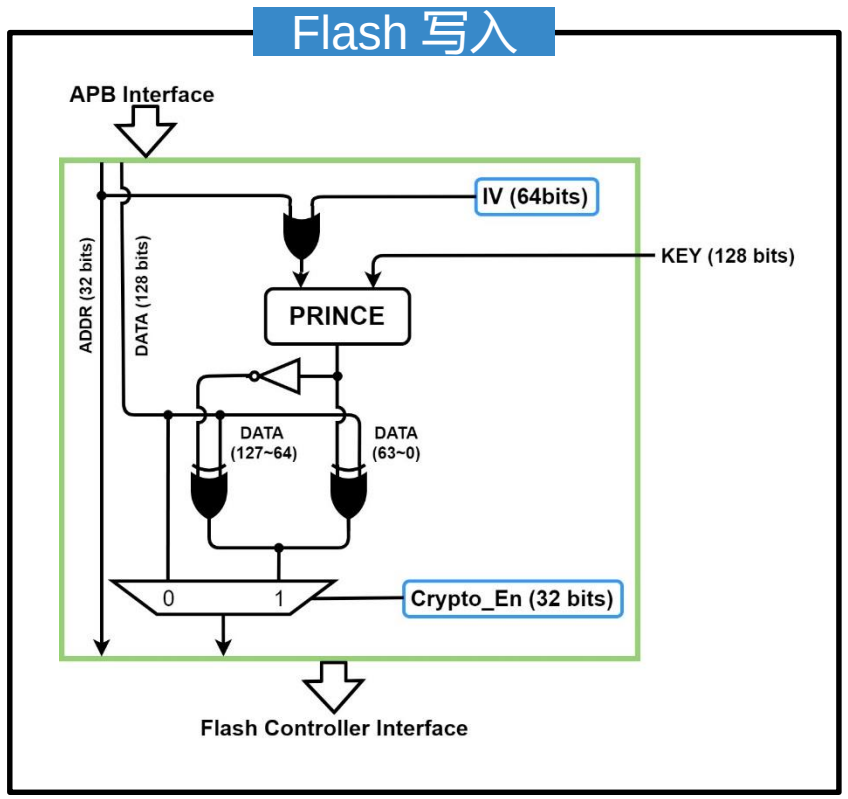
Part	Min	Typ	Max	Unit
C1	10	22 (X5R or X7R)	47	µF
C2	10	22 (X5R or X7R)	47	µF
C3	80	100 (X5R or X7R)	120	nF
C4	38.7	47 (COG)	56.2	pF
C5	80	100 (X5R or X7R)	120	nF
L1	3.87	4.7	10	µH

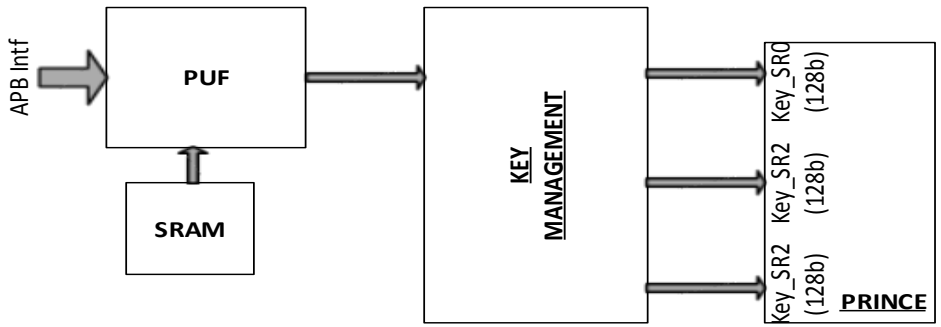
Pin Name	Pin number	
	HLQFP100	VBGA100
VBAT_DCDC	49	45
VBAT_DCDC_CORE	50	45
VBAT_PMU	51	46
VSS_DCDC	47	43
VSS_DCDC_CORE	46	42
VSS_PMU	-	47
LX	48	44
FB_VDD_PMU	45	41

PRINCE – FLASH加密技术

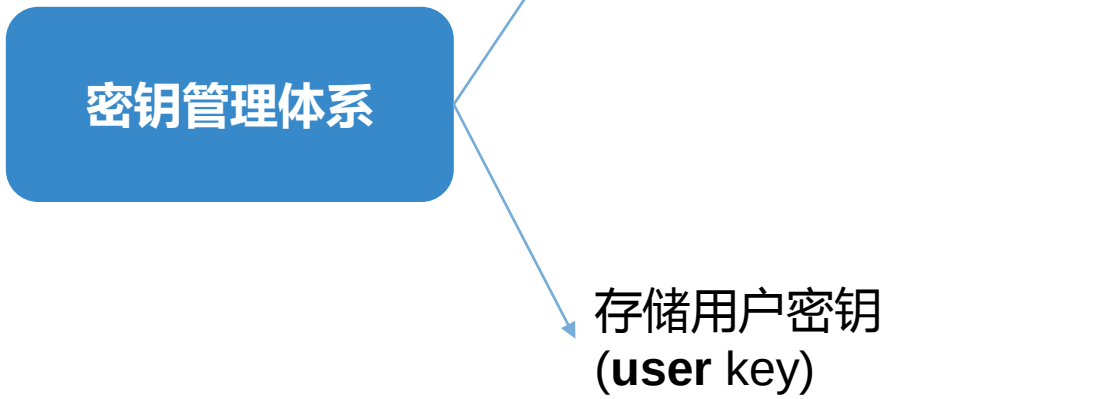
- **NXP和2家大学共同开发加密算法**
- **轻量级分组对称加密算法**
  - 64bit分组密码 支持128bit密钥
  - 使用PUF保护初始矢量 (IV)
  - 密钥和IV保存在PFR 中(Protected Flash Region), 不可读
  - 支持加密和解密
- **实时**
  - 解密低延迟，读取内容无需额外时钟周期(对比AES，AES一般需要 10-14 时钟周期)
  - 无初始化时间
  - 组合逻辑
- **效率**
  - 低成本
  - 低能耗
  - 无需额外的RAM空间







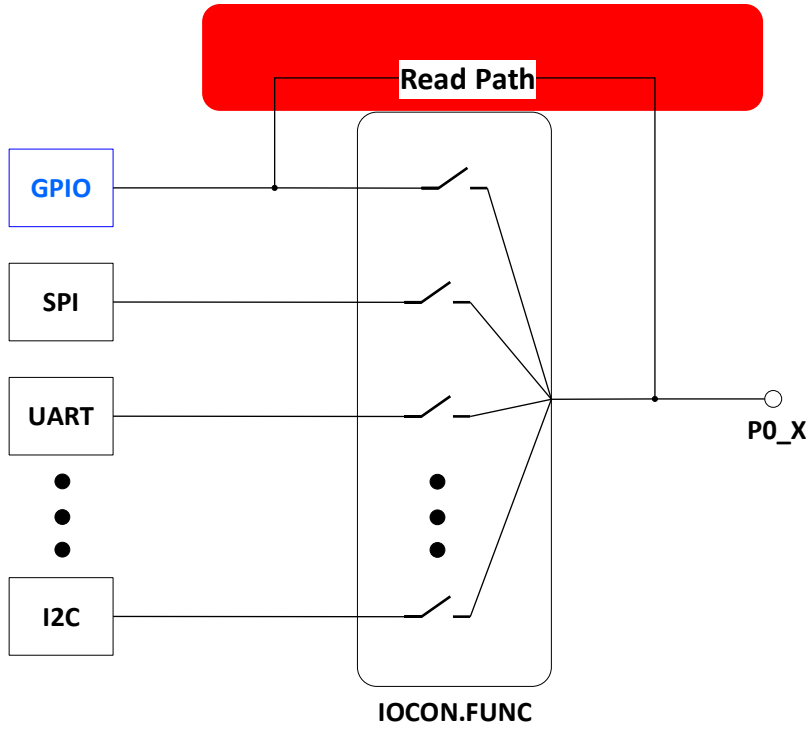
PUF – 物理防克隆技术

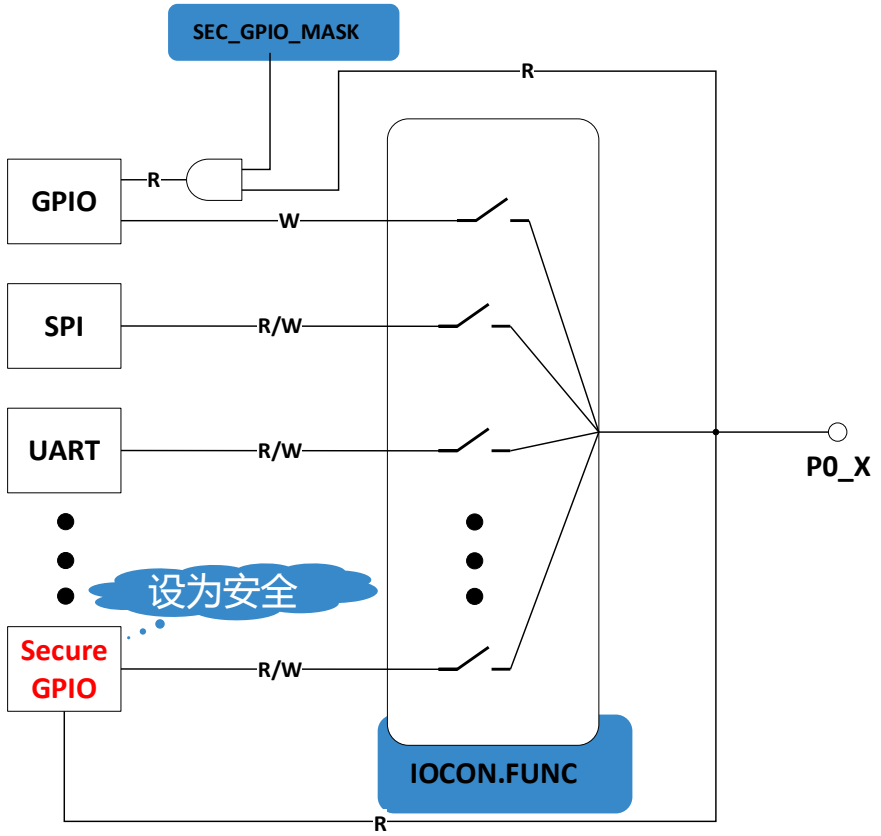


- PUF提供安全的密钥存储，而无需提前注入或配置设备唯一的PUF根密钥。
- 不以明文形式存储密钥，而是生成密钥代码(**Key Code**)。重建密钥时(Get Key)，向PUF提供密钥代码(**Key Code**)，PUF将其与自身的**数字指纹**(**Digital fingerprint**)结合完成密钥重建。密钥可供软件使用或路由到某些IP（例如AES引擎，PRINCE）。

芯片自己的指纹

SECURE GPIO – 安全GPIO





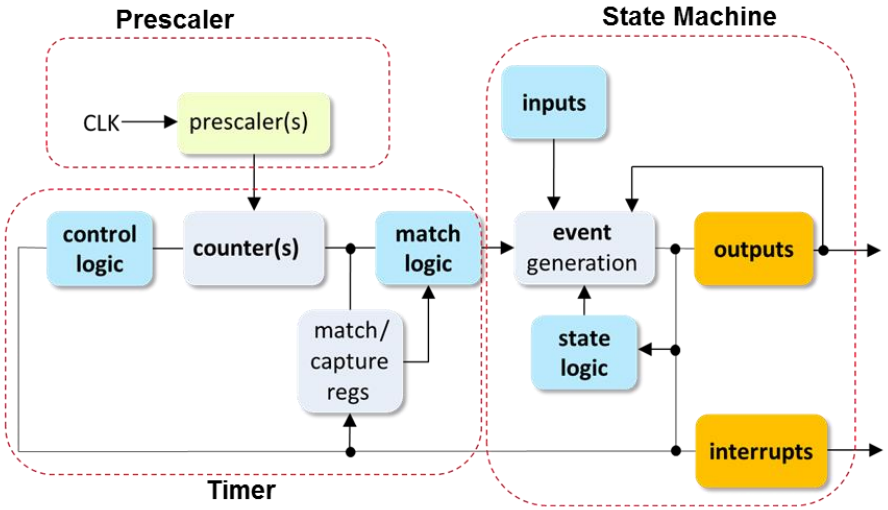
*R： Read Path
*W: Write Path
*R/W: Read and Write Path

SCT – 状态可配置定时器

基本的定时器timer
- 输入捕捉
- 输出比较
- PWM

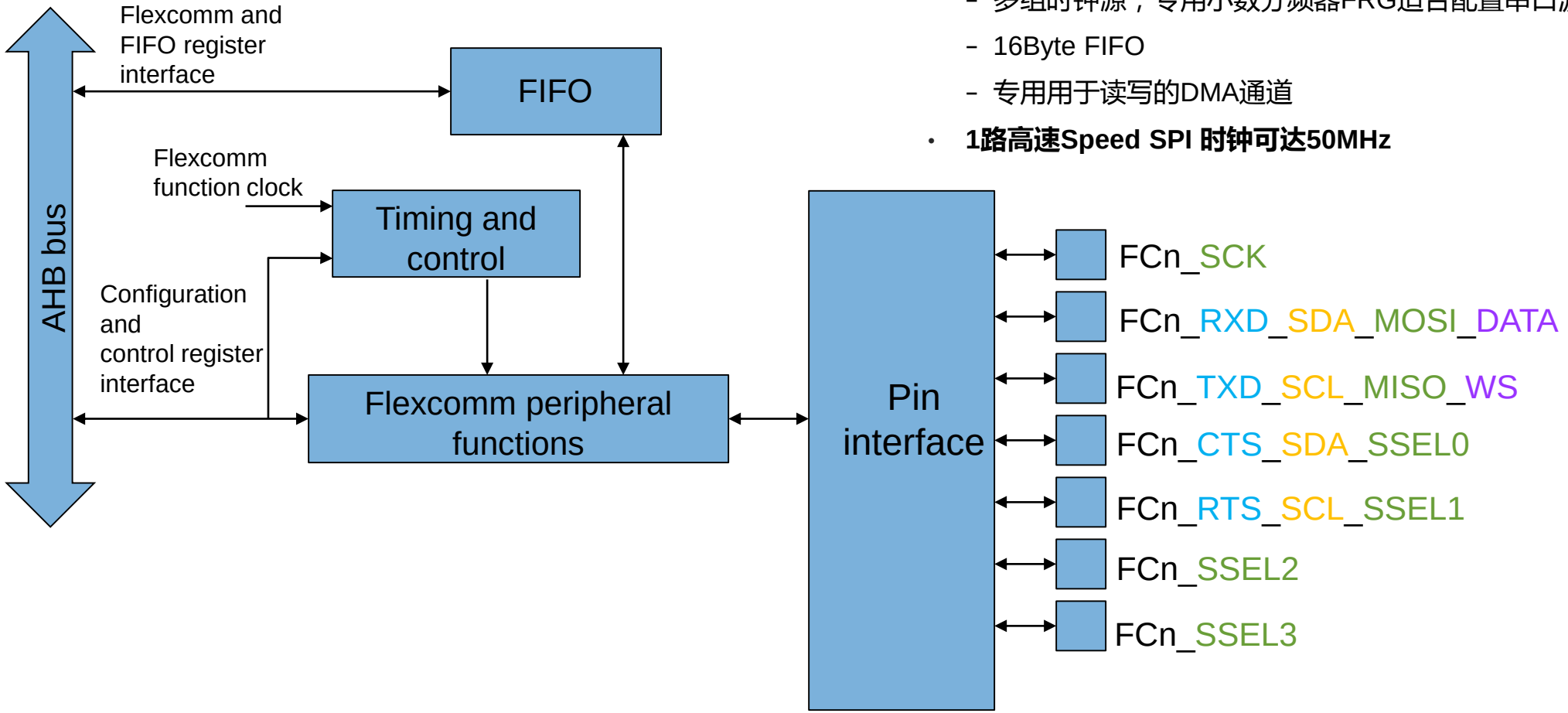
…**带有状态机**

- 相较于通用定时器，SCT可编程的特性使其使用更灵活
- 可配置为 单32bit计数器 或者 双16位计数器
- 在定时器的基础上，增强了
  - 事件的输入捕捉
  - 信号输出功能
  - 中断和DMA事件
  - 状态机，在计数周期中可以灵活的定义计数值、输出、中断和DMA的行为
  - 如上功能可以实现多种内联
- **LPC55S6x配置**
  - 8 个输入源
  - 10 个输出
  - 16 个匹配/捕捉 寄存器
  - 16 个事件
  - 32 个状态



FLEXCOMM – 灵活可配置串行接口单元

- 8组FlexComm接口
  - 软件可以将其配置为：USART, I2C, SPI或者I2S
  - 多组时钟源，专用小数分频器FRG适合配置串口波特率或者I2S时钟信号
  - 16Byte FIFO
  - 专用用于读写的DMA通道
- **1路高速Speed SPI 时钟可达50MHz**



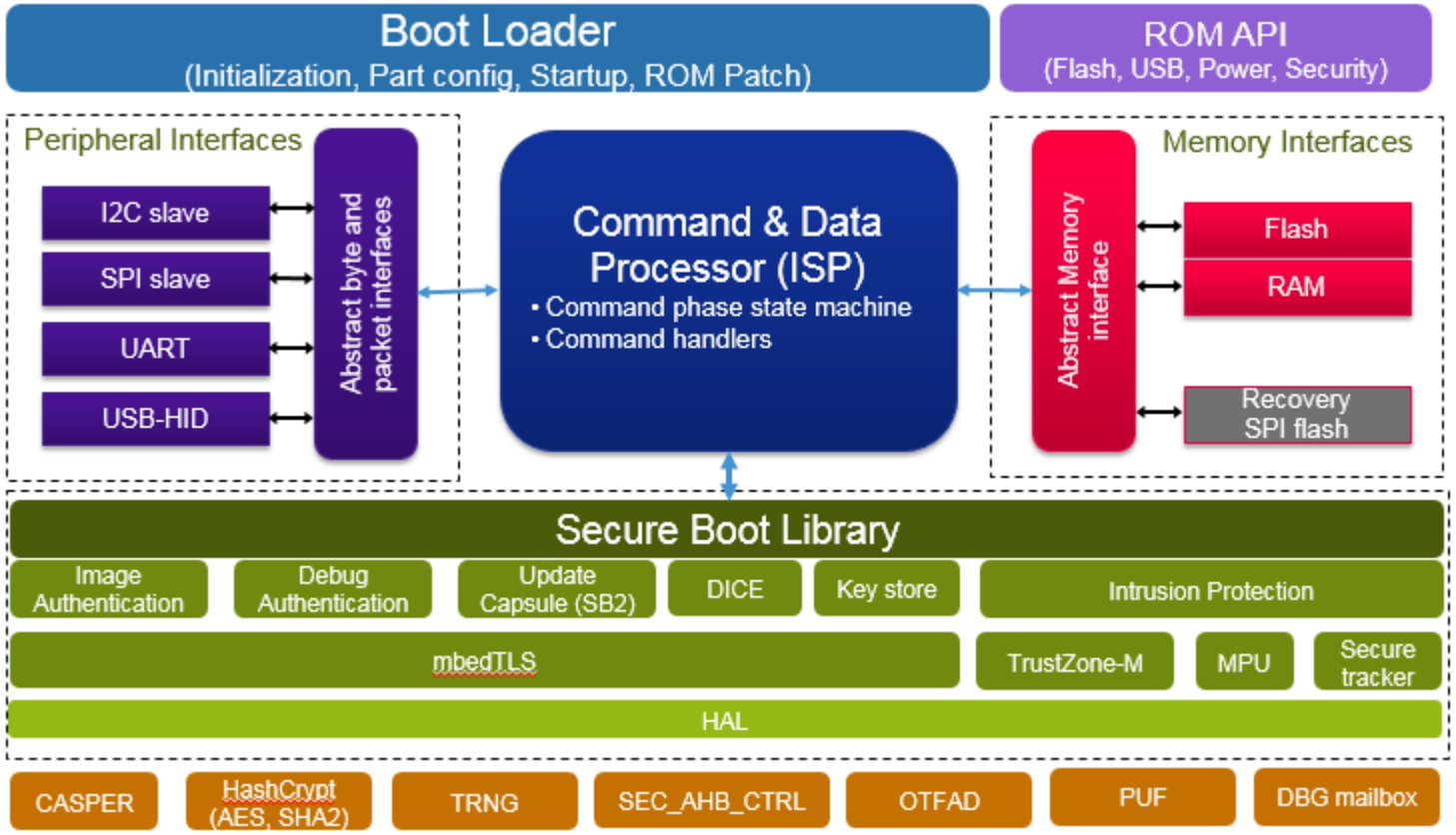
*LPC553x/1x 系列仅有4路FlexComm

ROM - 简化开发 降低FLASH消耗

- 片上集成128KB ROM 支持一下功能 ：
  - 引导flash中的固件并执行
  - 支持CRC32可用于检查固件完整性
  - 支持Flash在应用中编程IAP和在系统中编程ISP
  - 通过ISP烧录Flash支持以下接口:
    - USB接口，通过HID设备类
    - UART接口，支持自适应波特率
    - SPI从机接口
    - I2C从机接口
  - ROM API 功能

ROM – 支持安全启动

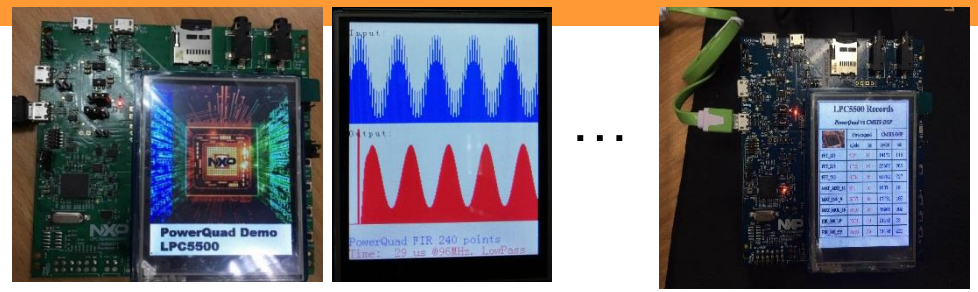
- 支持安全启动
  - 启动使用公钥签名的固件
- 支持从PRINCE加密的区域引导执行程序
- 支持公钥和防止固件版本回滚
  - 支持4 RoT 密钥
  - 支持16固件认证密钥
- 支持TrustZone区域预设定




WHAT WILL YOU CREATE THAT CAN CHANGE THE WORLD?
参考例程
LPC5500 系列 MCU
NXP

DEMO – 参考例程

- LPC5500利用PowerQuad加速器增强DSP运算性能
  - 单周期4x32位单精度浮点MAC
  - 硬件加速 trigonometry/ Hypobolics/Matrix/Transform/Signal Processing/ 等数学运算
  - 比CMSIS-DSP提高几倍亦或十几倍
- LPC5500 PRINCE实时加解密例程
  - Flash实时加解密
  - 与片上其他安全技术为内核/晶元/系统 提供安全防护
- CMSIS-NN 机器学习例程
  - 通过 CIFAR-10 模型和CMSIS-NN实现识别图片的功能
  - 使用单核Coretex-M33比Cortex-M4F提升15%以上的效率



PowerQuad demo

PRINCE demo

CMSIS-NN demo

DEMO – 参考设计

- 指纹识别
  - 相对于Cortex-M4F具有更快的响应速度
    - LPC55S6x： 正确识别可在200ms内完成
    - LPC541xx： 正确识别可在300ms内完成

AN – 应用笔记

编号	文档名称	简介
	LPC55xx/LPC55Sxx Dual Core Communication	LPC5500 双核应用笔记
	LPC55S6x Secure GPIO and Usage	LPC5500 安全GPIO应用笔记
AN12282	Digital Signal Processing for NXP LPC5500 Using PowerQuad	LPC5500 PowerQuad加速DSP计算应用笔记
	Firmware update using SBL with Trust Zone	LPC5500 使用TrustZone实现安全固件升级
AN12283	LPC55Sxx Secure boot	LPC5500 安全启动应用笔记
AN12284	LPC55Sxx CoreMark Cortex-M33 Porting Guide	LPC5500 CoreMark衡量内核性能应用笔记
AN12278	LPC55Sxx Security Solutions for IoT	LPC5500 基于AWS IOT开发应用笔记
AN12275	Using the DC-DC feature	LPC5500 DC-DC电源设计应用笔记
AN12324	Secure Storage with SRAM PUF	LPC5500 PUF应用笔记
	LPC55S6x Dual-DMA Usage	LPC5500 双DMA使用笔记

关注微信公众号获取更多技术细节

恩智浦 MCU加油站 微信公众号

- **恩智浦工程师原创技术分享**
- **欢迎关注，欢迎投稿**

SECURE CONNECTIONS
FOR A SMARTER WORLD