方寸微电子
TIH Microelectronics

T620

存储安全芯片
技术手册

修改记录

版本号	描述	日期
v0.1	草稿版	2018/5/8
v0.2	增加 QFN64 封装定义	2019/4/12
v1.0	初版发布版本	2019/4/25
v1.1	增加 QSPI 接口描述	2019/6/4
v1.2	更新 Logo	2021/07/13
v1.3	增加 T620-N300C 相关信息	2021/10/28
v1.4	更新改图 2.2	2021/11/02

Table of Content

1 概述

1.1 产品简介

T620 是由方寸微电子自主开发的新一代 SoC 存储安全芯片，具有功能丰富、性能强劲、功耗低、安全性高等特点，可广泛适用于安全 U 盘、按键 U 盘、加密移动硬盘等众多安全存储产品，也可以应用于 USB3 转 SATA3、USB 转 SPI、USB 转 UART 等接口领域产品。

该芯片集成高性能 32 位国产 RISC CPU，可支持 USB3.0、SATA3.0、eMMC5.1 等多种超高速接口，并集成多种国密算法（如 SM2、SM3、SM4），可满足信息安全领域存储类产品需求；同时该芯片也支持国际标准 AES 加密算法及 ECC 算法，可应用于全球通用安全存储市场。

该芯片提供完整的 SDK 供客户进行定制化开发，尤其针对典型应用场景提供了源码级方案支撑，可帮助客户缩短产品开发周期、降低整体开发成本，提升产品市场竞争力。

1.2 芯片应用

图 1.1 芯片应用图

1.3 芯片架构

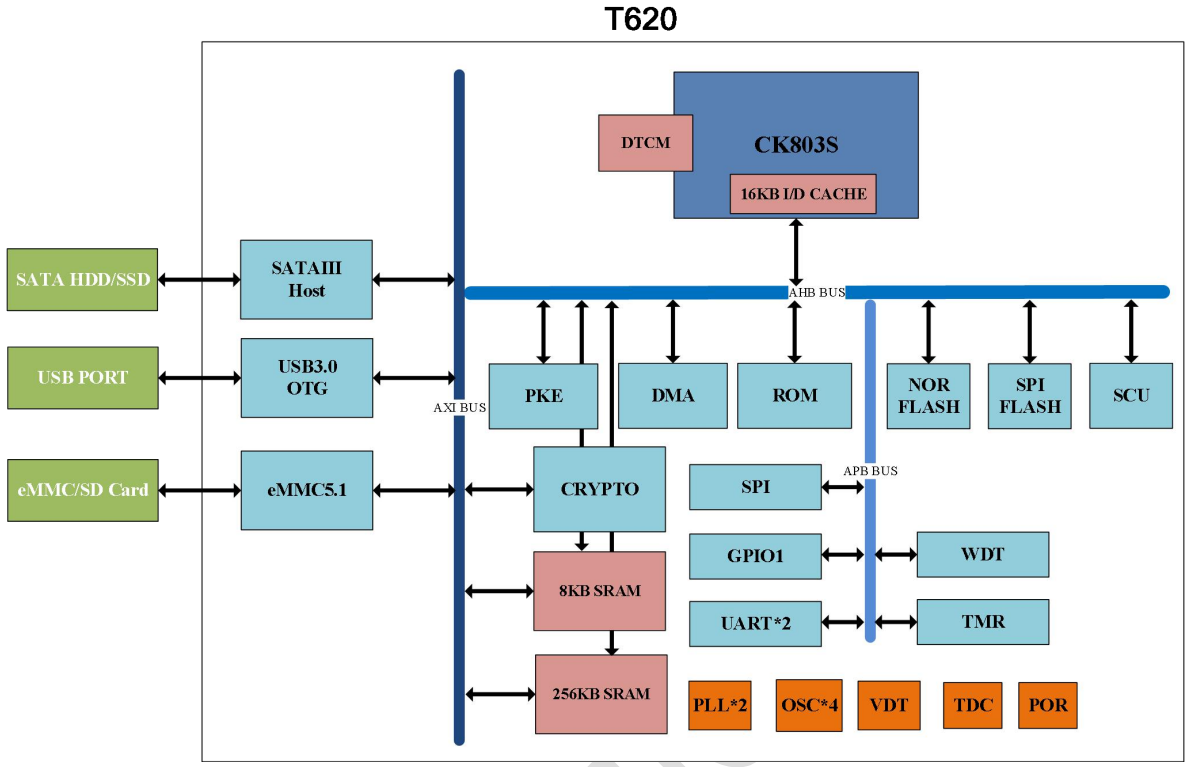


图 1.2 芯片系统架构框图

1.4 芯片特性

1.4.1 CPU 资源

- 主处理器集成 32 位国产 CPU CK803S
- 最高工作频率 260Mhz
- 内置 16KB I/D Cache
- 内置 32KB DTCM

1.4.2 USB3.0 OTG 接口

- 支持一路 USB3.0 OTG 接口速率 5Gbps，向下兼容 USB2.0/USB1.1
- 静态角色转换（主机/设备选择）
- 支持控制/批量/中断/等时传输类型
- 符合 Universal Serial Bus（USB） revision 3.0 标准协议

1.4.3 SATA3.0 主接口

- 支持一路 SATAIII host 接口速率 6Gbps，向下兼容 3Gbps/1.5Gbps
- 符合 Serial ATA Revision 3.0 标准协议
- 支持 NCQ 32 命令队列

1.4.4 eMMC 接口

- 支持 1 路 eMMC 接口
- 支持 eMMC5.1 协议标准
- 最高接口速率 HS400，向下兼容
- 支持 3.3V/1.8V IO 电压

1.4.5 安全引擎

- 支持 SM4、AES256 数据加密，加密性能 800MB/s@200Mhz
- 支持 ECB、CBC、OFB、CFB、CTR、XTS 6 种加密模式
- RSA（可选 CRT）：512~4096 比特
- ECC（素数域）：192、224、256、384 和 521 比特
- 支持大数模加、模减、模乘运算协处理
- SM2 密钥对生成速度 500 对/s
- 支持 SM2 签名验签，性能≥1200/600 次/s@200Mhz
- RSA1024 密钥对生成时间<0.1s
- 支持 RSA1024 签名验签，性能≥1200/12000 次/s@200Mhz
- RSA2048 密钥对生成时间<1s
- 支持 RSA2048 签名验签，性能≥200/4000 次/s@200Mhz
- 支持 SM3/SHA1/SHA224/SHA256 算法
- 支持一路 TRNG 发生器，生成速率≥30Mbps@50Mhz

*以上为硬件引擎性能，非最终产品性能

1.4.6 存储资源

- 32KB ROM
- 256KB SRAM
- 8KB SRAM（系统专用）
- 512KB/1MB 片内 flash

1.4.7 其他资源

- 内置硬件 DMA
- 内置 POR（Power on reset）电路
- 内置 8 个定时器
- 内置中断控制器
- 内置 1 个看门狗
- 支持 1 路 QSPI 主接口（仅用于连接 SPI Flash/SPI Ram 等）
- 支持 1 路 SPI 主接口
- 支持 2 路 UART 接口
- 支持 12 位 GPIO 接口

1.4.8 安全特性

- 支持电压检测
- 支持温度检测
- 支持物理探测防护
- 每颗芯片具备全球唯一 ID

1.4.9 物理规格

- Core 电压为 1.0V
- IO 电压为 3.3V
- 支持 QFN64 8mm x 8mm x 0.85mm 封装
- 工作温度 0~70℃，-40~85℃

1.5 地址映射

表 1.1 地址映射表

基地址	大小	模块名称	说明
0x0000_0000	1MB	ROM	
0x1010_0000	1MB	CRYPTO 寄存器端口	
0x1020_0000	1MB	DMA 寄存器端口	
0x1040_0000	1MB	QSPI 寄存器端口	
0x1050_0000	1MB	SCU 寄存器端口	
0x1060_0000	1MB	eMMC0 寄存器端口	
0x10C0_0000	1MB	TRNG 寄存器端口	
0x10D0_0000	1MB	PKE 寄存器端口	
0x1110_0000	1MB	8KB SRAM	8KB SRAM 在 AHB 总线地址
0x1120_0000	1MB	256KB SRAM	256KB SRAM 在 AHB 总线地址
0x1210_0000	1MB	SPI 寄存器端口	
0x1220_0000	1MB	UART0 寄存器端口	
0x1230_0000	1MB	UART1 寄存器端口	
0x1240_0000	1MB	TIMER 寄存器端口	
0x1250_0000	1MB	WDT 寄存器端口	
0x1280_0000	1MB	GPIO1 寄存器端口	
0x2200_0000	1MB	USB OTG 寄存器端口	
0x2210_0000	1MB	SATA Host 寄存器端口	
0x2220_0000	1MB	8KB SRAM	8KB SRAM 在 AXI 总线地址
0x2230_0000	1MB	256KB SRAM	256KB SRAM 在 AXI 总线地址
0x2240_0000	1MB	eMMC0_S 数据端口	
0x2300_0000	8MB	CRYPTO_S1 数据端口	
0x2380_0000	8MB	CRYPTO_S2 数据端口	

1.6 中断源

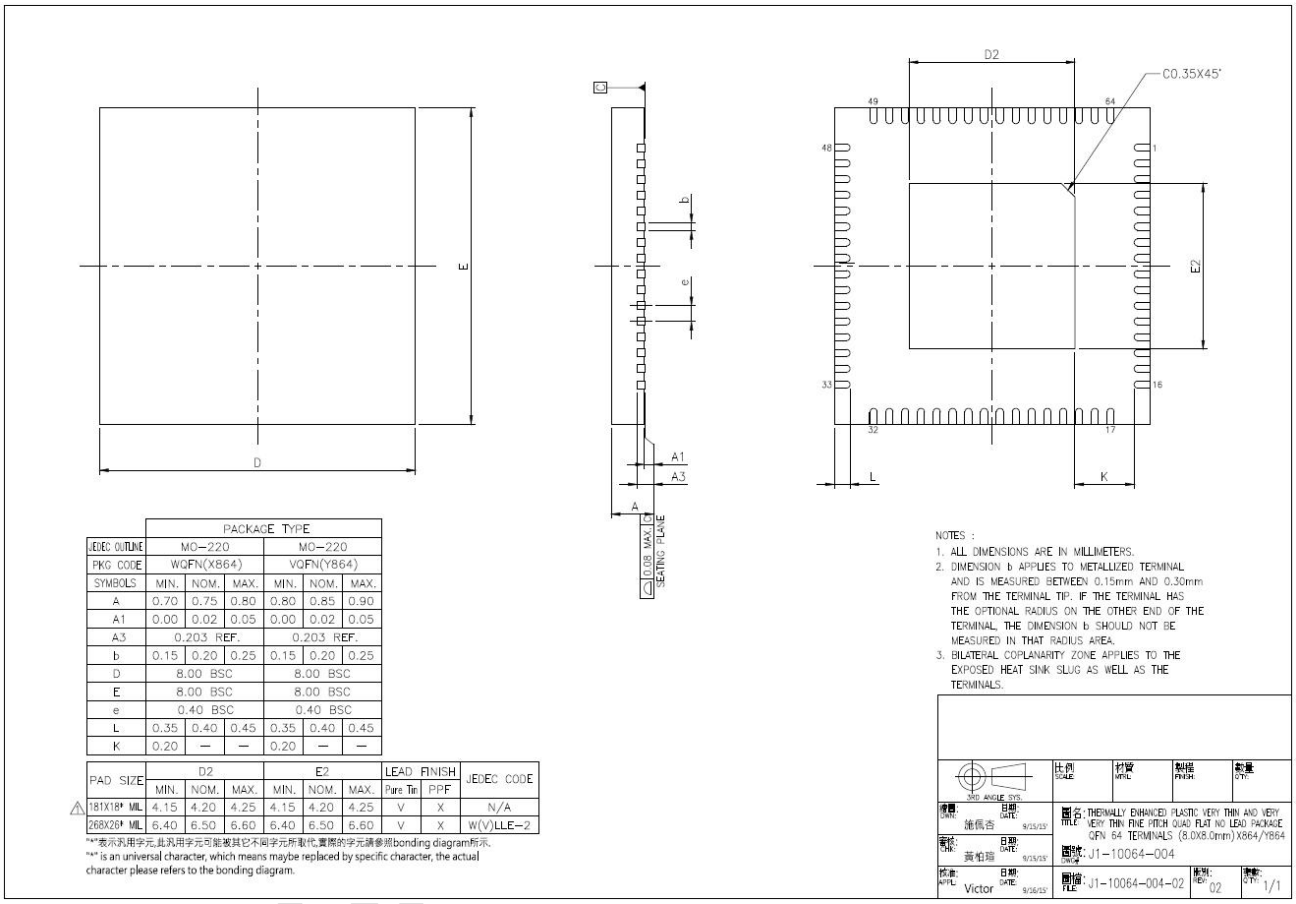
CK803S 的中断源映射如下：

表 1.2 CK803S 中断源

No.	中断源	说明
26	Core_Timer	
25	VDT	
24	Reserved	
23	TRNG	
22	PKE	
21	AXIC	
20	AHBC	
19	GPIO1	
18	Reserved	
17	WDT	
16	Reserved	
15	UART_1	
14	UART_0	
13	QSPI	
12	Reserved	
11	SPI	
10	TIMER	
9	DMA	
8	Reserved	
7	Reserved	
6	Reserved	
5	Reserved	
4	eMMC0	
3	CRYPTO	
2	SATA3_Host	
1	Reserved	
0	USB3_OTG	

2 硬件特性

2.1 芯片封装



JEDEC OUTLINE	PACKAGE TYPE					
	MO-220			MO-220		
PKG CODE	WQFN(X864)			VQFN(Y864)		
SYMBOLS	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	0.70	0.75	0.80	0.80	0.85	0.90
A1	0.00	0.02	0.05	0.00	0.02	0.05
A3	0.203 REF.			0.203 REF.		
b	0.15	0.20	0.25	0.15	0.20	0.25
D	8.00 BSC			8.00 BSC		
E	8.00 BSC			8.00 BSC		
e	0.40 BSC			0.40 BSC		
L	0.35	0.40	0.45	0.35	0.40	0.45
K	0.20	—	—	0.20	—	—

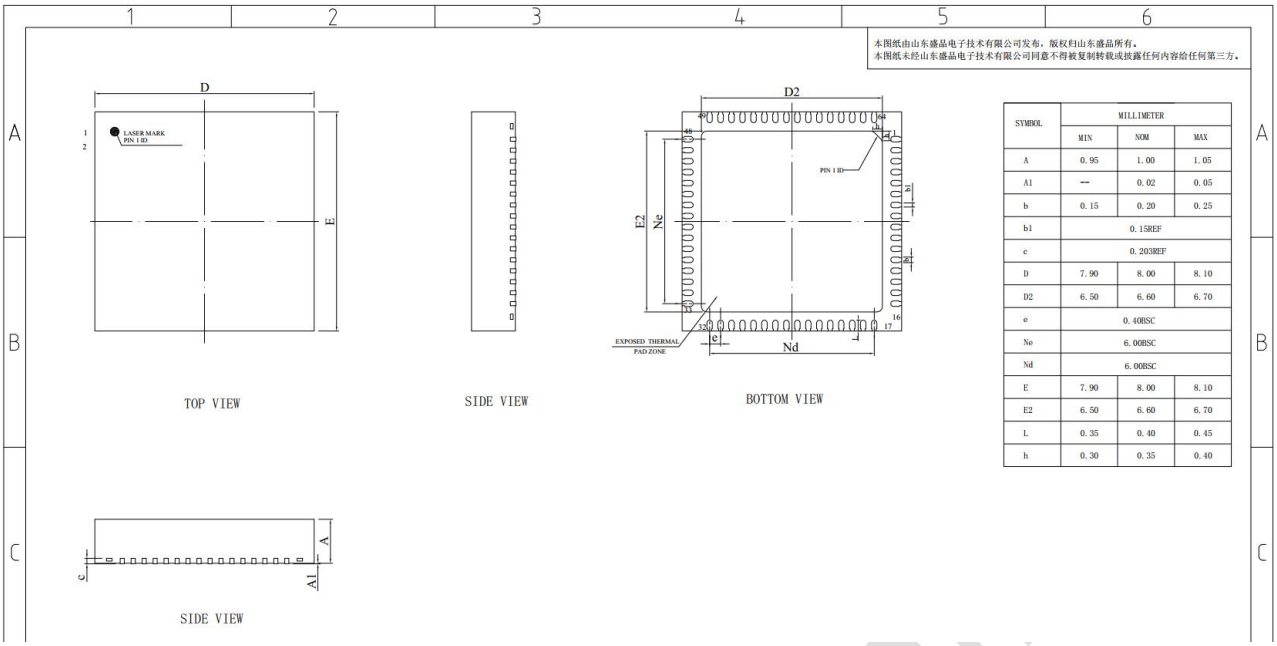
PAD SIZE	D2			E2			LEAD FINISH		JEDEC CODE
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.	Pure Tin	PPF	
⚠ 181X181* MIL	4.15	4.20	4.25	4.15	4.20	4.25	V	X	N/A
268X268* MIL	6.40	6.50	6.60	6.40	6.50	6.60	V	X	W(V)LLE-2

"*"表示泛用字元,此泛用字元可能被其它不同字元所取代,實際的字元請參照bonding diagram所示.
"*" is an universal character, which means maybe replaced by specific character, the actual character please refers to the bonding diagram.

3RD ANGLE SYS.	比例 SCALE	材質 MTRL	製程 FINISH	數量 QTY.
繪圖: 施佩吉 DRWN 9/15/15	圖名 TITLE: THERMALLY ENHANCED PLASTIC VERY THIN AND VERY VERY THIN FINE PITCH QUAD FLAT NO LEAD PACKAGE QFN 64 TERMINALS (8.0X8.0mm) X864/Y864		
審核: 黃旭瑞 CHK. 9/15/15	圖號 DWG#: J1-10064-004		
核准: Victor APPL. 9/16/15	檔名 FILE: J1-10064-004-02	版別 REV: 02	張數 QTY: 1/1

图 2.1 T620-N200C 芯片封装尺寸图

*注：D2=E2=6.5mm



SYMBOL	MILLIMETER		
	MIN	NOM	MAX
A	0.95	1.00	1.05
A1	--	0.02	0.05
b	0.15	0.20	0.25
b1	0.15REF		
c	0.203REF		
D	7.90	8.00	8.10
D2	6.50	6.60	6.70
e	0.40BSC		
Ne	6.00BSC		
Nd	6.00BSC		
E	7.90	8.00	8.10
E2	6.50	6.60	6.70
L	0.35	0.40	0.45
h	0.30	0.35	0.40

图 2.2 T620-N300C 芯片封装尺寸图

2.2 管脚分布

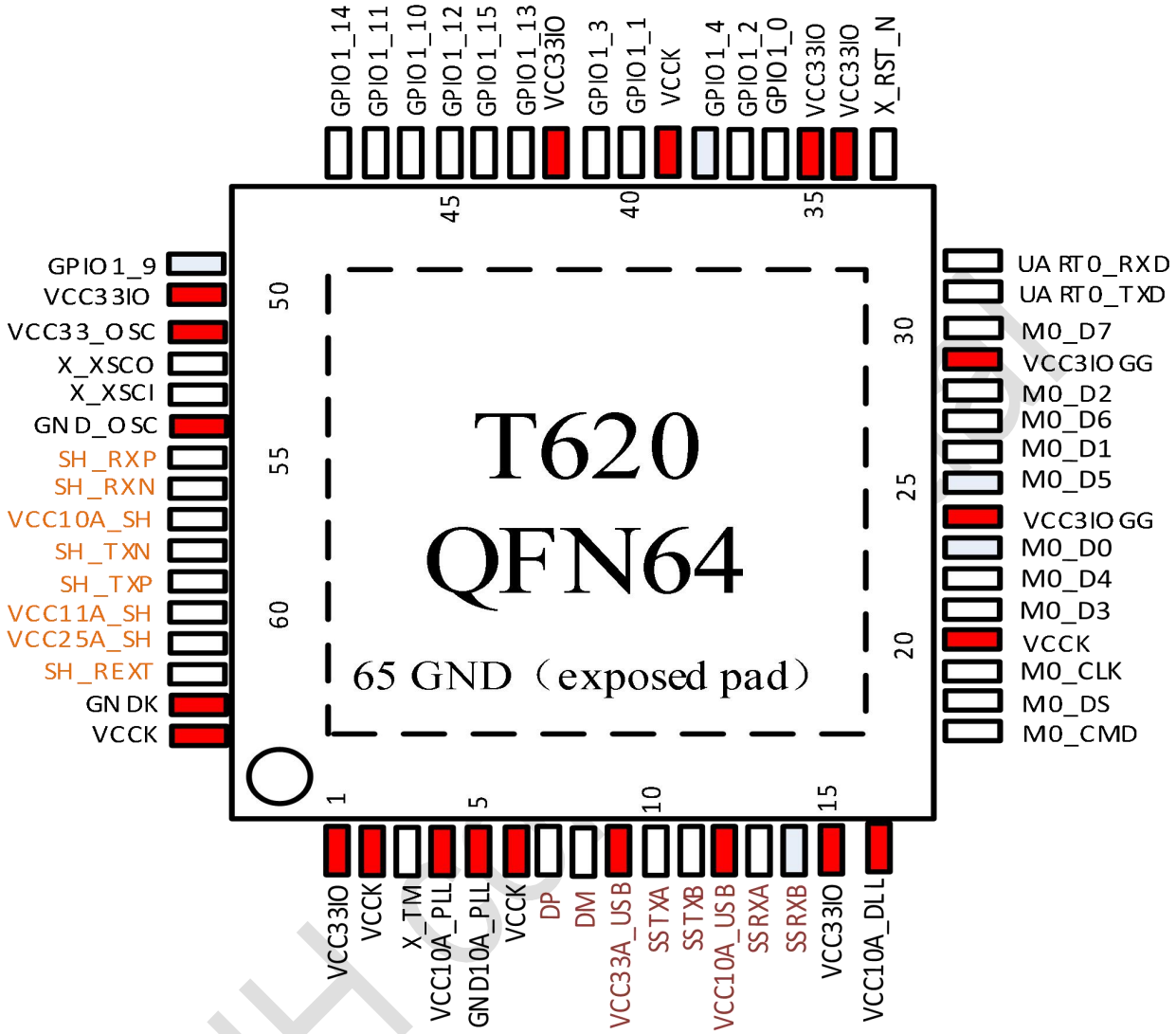


图 2.2 QFN64 封装图

2.3 管脚描述

表 2.1 管脚描述

位置	名称	I/O	功能描述
left			
1	VCC33IO		3.3V 数字电源
2	VCCK		1.0V 数字电源
3	X_TM	I	测试模式使能信号： 0：正常功能模式 1：测试模式 默认下拉
4	VCC10A_PLL		PLL 1.0V 模拟电源
5	GND10A_PLL		PLL 模拟地
6	VCCK		1.0V 数字电源
7	DP	IO	USB2.0 高速差分输入输出
8	DM	IO	USB2.0 高速差分输入输出
9	VCC33A_USB		USB 3.0 3.3V 模拟电源
10	SSTXA	O	USB 3.0 接口差分输出 A
11	SSTXB	O	USB 3.0 接口差分输出 B
12	VCC10A_USB		USB 3.0 1.0V 模拟电源
13	SSRXA	I	USB 3.0 接口差分输入 A
14	SSRXB	I	USB 3.0 接口差分输入 B
15	VCC33IO		3.3V 数字电源
16	VCC10A_DLL		eMMC DLL 1.0V 数字电源
down			
17	M0_CMD	IO	eMMC0 CMD 信号
18	M0_DS	I	eMMC0 DS 信号
19	M0_CLK	O	eMMC0 CLK 信号
20	VCCK		1.0V 数字电源
21	M0_D3	IO	eMMC0 DATA3 信号
22	M0_D4	IO	eMMC0 DATA4 信号
23	M0_D0	IO	eMMC0 DATA0 信号
24	VCC3IOGG		eMMC0 3.3V/1.8V 数字电源
25	M0_D5	IO	eMMC0 DATA5 信号
26	M0_D1	IO	eMMC0 DATA1 信号
27	M0_D6	IO	eMMC0 DATA6 信号
28	M0_D2	IO	eMMC0 DATA2 信号
29	VCC3IOGG		eMMC0 3.3V/1.8V 数字电源
30	M0_D7	IO	eMMC0 DATA7 信号
31	UART0_TXD	O	UART0 TXD 信号

32	UART0_RXD	I	UART0 RXD 信号
right			
33	X_RST_N	I	系统复位引脚，低电平有效
34	VCC33IO		3.3V 数字电源
35	VCC33IO		3.3V 数字电源
36	GPIO1_0	IO	GPIO1 通用输入输出端口 0，默认上拉
37	GPIO1_2	IO	GPIO1 通用输入输出端口 2
38	GPIO1_4	IO	GPIO1 通用输入输出端口 4
39	VCCK		1.0V 数字电源
40	GPIO1_1	IO	GPIO1 通用输入输出端口 1
41	GPIO1_3	IO	GPIO1 通用输入输出端口 3
42	VCC33IO		3.3V 数字电源
43	GPIO1_13	IO	GPIO1 通用输入输出端口 13
44	GPIO1_15	IO	GPIO1 通用输入输出端口 15
45	GPIO1_12	IO	GPIO1 通用输入输出端口 12
46	GPIO1_10	IO	GPIO1 通用输入输出端口 10
47	GPIO1_11	IO	GPIO1 通用输入输出端口 11
48	GPIO1_14	IO	GPIO1 通用输入输出端口 14
up			
49	GPIO1_9	IO	GPIO1 通用输入输出端口 9
50	VCC33IO		3.3V 数字电源
51	VCC33_OSC		OSC 3.3V 数字电源
52	X_XSCO	O	系统晶振输出，30Mhz
53	X_XSCI	I	系统输入时钟，30MHz
54	GND_OSC		OSC 数字地
55	SH_RXP	I	SATA Host 接口高速差分输入 P
56	SH_RXN	I	SATA Host 接口高速差分输入 N
57	VCC10A_SH		SATA Host 1.0V 模拟电源
58	SH_TXN	O	SATA Host 接口高速差分输出 N
59	SH_TXP	O	SATA Host 接口高速差分输出 P
60	VCC11A_SH	O	SATA Host 1.1V 模拟电源输出，需外挂 2.2uF 以上电容
61	VCC33A_SH		SATA Host 3.3V 模拟电源
62	SH_REXT	I	SATA Host 匹配电阻，需下拉 18K 欧姆至地信号
63	GNDK		数字地
64	VCCK		1.0V 数字电源
65	GND		芯片 bottom 面数字地引脚

2.4 管脚复用

在芯片内部，GPIO1、UART1、QSPI 等模块复用 12 根 IO 线，复用模式如下表 2.2 所示：
FUNC_MODE 通过 SCU 寄存器，可配置为 0、1 两种模式。
GPIO1[5:0]由 SCU 寄存器控制，在任何 FUNC_MODE 下均可进行模式选择。

表 2.2 管脚复用表

FUNC_MODE[1:0]	0	1
接口信号	功能模式 0	功能模式 1
GPIO1 [15]	GPIO1[15]	QSPI_SCK
GPIO1[14]	GPIO1[14]	QSPI_CS#
GPIO1[13]	GPIO1[13]	QSPI_TX（IO0）
GPIO1[12]	GPIO1[12]	QSPI_RX（IO1）
GPIO1[11]	GPIO1[11]	QSPI_WP#（IO2）
GPIO1[10]	GPIO1[10]	QSPI_HOLD#（IO3）
GPIO1[9]	GPIO1[9]	PWM0
GPIO1[4]	GPIO1[4]/SPI_CK	GPIO1[4]/SPI_CK
GPIO1[3]	GPIO1[3]/SPI_TXD	GPIO1[3]/SPI_TXD
GPIO1[2]	GPIO1[2]/SPI_RXD	GPIO1[2]/SPI_RXD
GPIO1[1]	GPIO1[1]/UART1_TXD	GPIO1[1]/UART1_TXD
GPIO1[0]	GPIO1[0]/UART1_RXD	GPIO1[0]/UART1_RXD

*备注：接口复用时 SPI 接口无 CS#，如果需要扩展可以用其他 GPIO 引脚控制。

2.5 上电时序

为确保芯片内部逻辑与外部器件通讯正常，VCCK（1.0V）电源和 VCCIO（3.3V）电源对上电时序有以下要求，如下图所示：

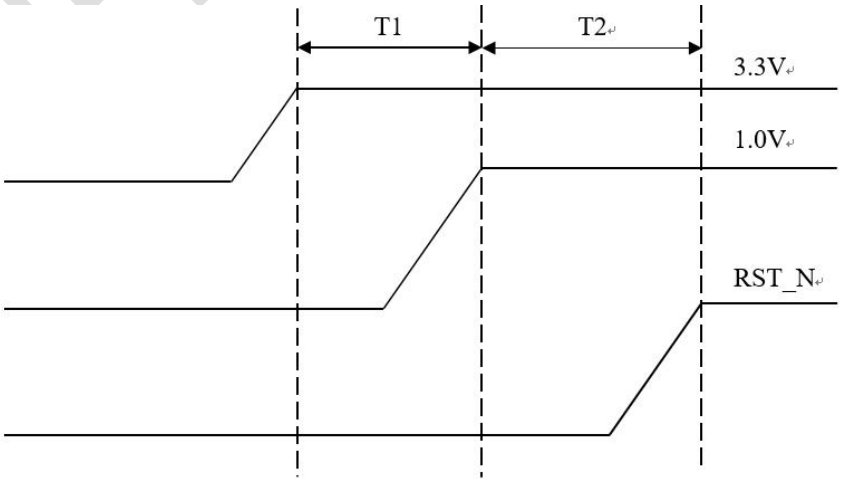


图 2.3 电源上电顺序 1 图

其中，0＜T1≤10ms。

T2 为系统复位要求，40ms≤T2

2.6 电性能参数

表 2.3 电气特性参数

符号	描述	Min	Typ	Max	单位
VCC33IO	普通 IO 口电源	3.0	3.3	3.6	V
VCCK	Core 电源	0.9	1.0	1.1	V
VCC10_PLL	PLL 模拟电源	0.9	1.0	1.1	V
VCC33A_USB	USB 接口 IO 模拟电源	3.0	3.3	3.6	V
VCC10A_USB	USB 接口 core 模拟电源	0.9	1.0	1.1	V
VCC10A_DLL	EMMC DLL 内核数字电源	0.9	1.0	1.1	V
VCC33_OSC	系统晶振数字电源	3.0	3.3	3.6	V
VCC10A_SH	SATA HOST PHY 内核模拟电源	0.9	1.0	1.1	V
VCC33A_SH	SATA HOST PHY IO 模拟电源	3.0	3.3	3.6	V
VCC11A_SH	SATA HOST PHY 内核模拟电源输出	1.0	1.1	1.2	V

2.7 功耗

- 静态功耗＜0.1W
- 动态功耗＜1.0W

2.8 PCB 设计建议

请参考《T6x0 硬件设计用户指南》

3 CPU 子系统

3.1 CK803S 处理器

3.1.1 简介

CK803S 是面向控制领域的 32 位高能效嵌入式 CPU 核，具有低成本、低功耗、高代码密度等多种特点。CK803S 采用 16/32 位混合编码指令系统，设计了精简高效的 3 级流水线。

CK803S 提供多总线接口，支持系统总线、指令总线、数据总线的灵活配置。CK803S 针对内存拷贝应用做了特殊优化，可以获得极致的内存拷贝性能。此外，CK803S 对中断响应做了特殊加速，中断响应延时仅需 13 个周期。

3.1.2 特性

- 精简指令集（RISC）处理器架构
- 32 位数据，16 位/32 位混合编码指令
- 16 个 32 位通用寄存器
- 3 级流水线
- 最高工作频率 260Mhz
- 单位性能 1.5DMIPS/MHz
- 按序发射、按序执行、按序退出
- 支持 AHB 系统总线和 AHB Databus 总线接口
- 内置 16KB 高速缓存
- 内置 32KB DTCM
- 内置 8 个内存保护单元
- 内置紧耦合矢量中断控制器与计时器
- 支持 1:1 和 2:1 处理器与系统时钟比
- 中断响应延时仅为 13 个处理器周期
- 静态分支预测
- 支持硬件乘除法
- 支持连续内存访问
- 仅支持 little endian

3.1.3 架构

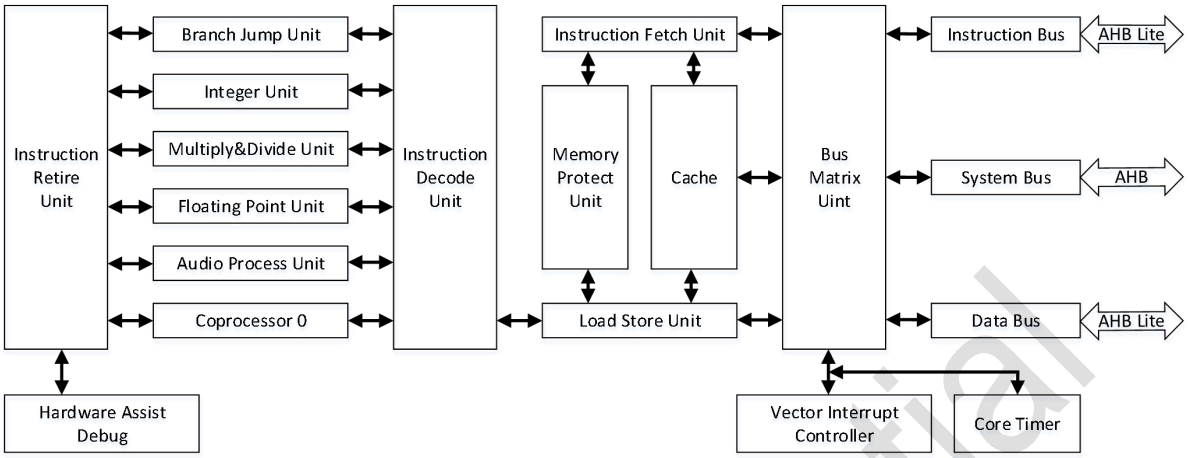


图 3.1 CK803S 系统架构图

*上图中，浮点处理单元、音频加速单元和指令总线模块本芯片中不支持。

3.1.4 矢量中断控制器

矢量中断控制器（VIC）是一个与 CK803S 紧耦合的 IP 单元，用于中断的高效处理。矢量中断控制器最大可支持 32 个中断源（IRQ[31:0]），每个中断源拥有软件可编程的中断优先级。矢量中断控制器收集来自不同中断源的中断请求，依据中断优先级对中断请求进行仲裁。最高优先级的中断将获得中断控制权并向处理器发出中断请求，当处理器响应中断请求，回中断请求响应信号给 VIC；当处理器退出中断服务程序（ISR），返回中断退出信号给 VIC。

矢量中断控制器支持中断嵌套。当处理器正在处理一个中断请求时来了一个更高优先级的中断请求，处理器将暂停当前中断服务程序，响应更高优先级的中断请求。在更高优先级的中断请求处理结束时，CPU 返回被暂停的中断服务程序继续执行。矢量中断控制器允许高优先级的中断请求抢占低优先级的中断请求，但不允许同级别或者低优先级的中断抢占，保证了中断响应的实时性。

矢量中断控制器的系统结构图如图所示。

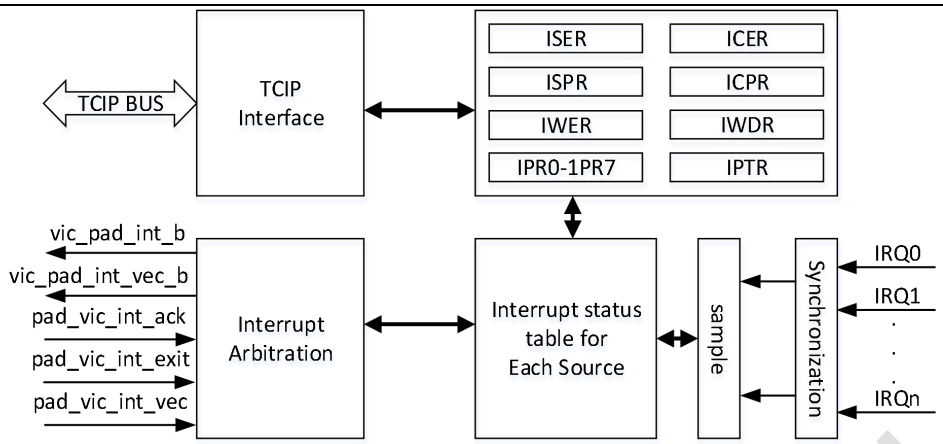


图 3.2 中断控制器结构框图

3.1.5 系统计时器

系统计时器Core Timer是CK803S内部集成的一个紧耦合模块，主要用于计时。Core Timer提供了一个简单易用的 24 位循环递减的计数器，当 Core Timer 使能时，计数器开始工作，当计数器递减到 0 时，会向矢量中断控制器发起中断请求，申请获得处理器响应并处理 Core Timer 的事务。

Core Timer 的结构框图如图所示：

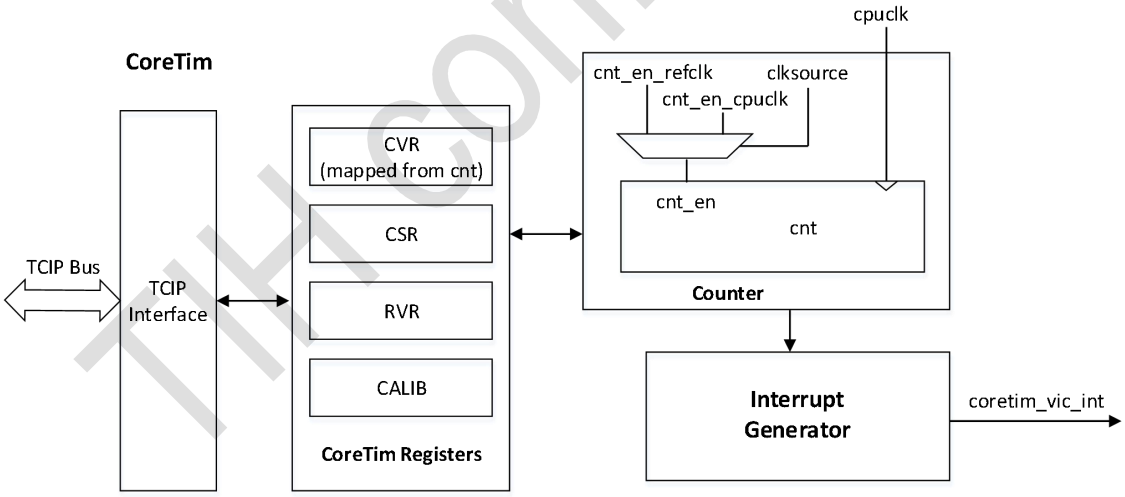


图 3.3 CoreTimer 结构框图

3.2 存储

芯片内部包含 4 块存储单元：ROM、Nor flash 和 2 块 SRAM。

内置 32KB ROM 固化了 Bootrom 程序，用于上电固件引导及固件下载，用户无法修改；

内置 512KB/1MB Nor flash，可用于存储固件代码及用户敏感信息；

Nor flash 主要参数如下：

- 页大小：512B
- 8/16/32bit 读、32bit 写
- 擦写次数：10 万次

内置 1 片 8KB SRAM 和 1 片 256KB SRAM，8KB SRAM 用于存储 SATA Host 模块的命令链表，用户不能使用该存储空间；256KB SRAM 可供用户使用，用于高速固件代码执行、临时数据存储和算法运算等。8KB SRAM 和 256KB SRAM 各自拥有独立 AHB 和 AXI 接口访问通道，可大大提升 AHB 和 AXI 间数据搬运效率。

3.3 DMA

3.3.1 模块概述

DMA (Direct Memory Access)是为了降低 CPU 负担专门用来进行数据搬运的模块。在 T620 中，单纯的 DMA 模块只在 AHB 总线上集成了一个，如果 AXI 总线上需要进行数据搬运，可以通过 CRYPTO 模块中的 DMA 实现。

DMA 模块架构如下：

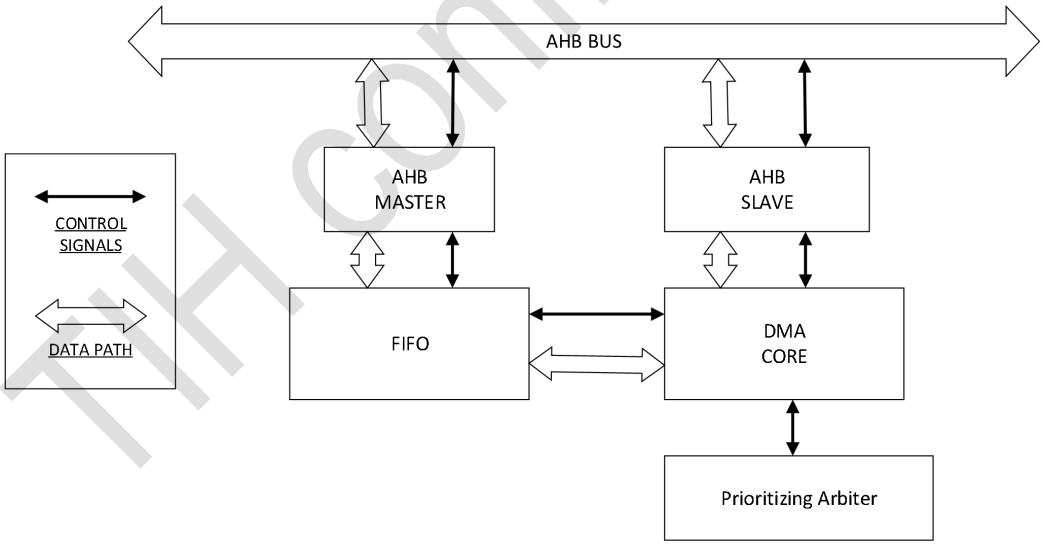


图 3.4 DMA 结构框图

3.3.2 模块特性

- 支持 8 路可配 DMA 通道
- 通道共享 16 个字节 buffer
- 支持链表模式传输

- 可在 AHB、AXI、APB bus 间进行数据搬运
- 支持 8/16/32 位数据传输
- 仅支持 little-endian 传输
- 支持 INCR 和 FIXED 地址传输模式

3.4 定时器

3.4.1 模块概述

定时器模块挂载于 APB 总线上，可提供 8 个独立的计数器，用于生成定时中断给 CPU 进行定时任务处理。同时定时器模块可生成并输出一路 PWM 信号，用于芯片外设时钟或者电机类设备的控制。

模块框图如下：

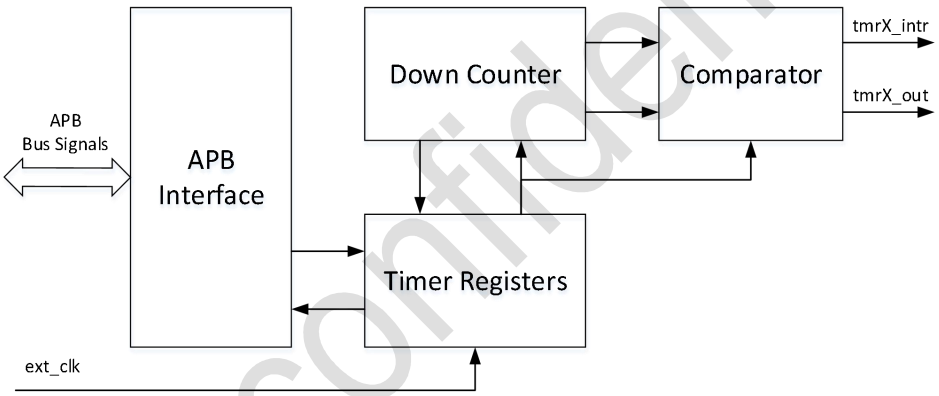


图 3.5 定时器结构框图

3.4.2 模块特性

- 支持 8 个独立的 32 位计数器
- 支持一路 PWM 输出，最高频率 20Mhz
- PWM 极性和占空比可配
- 支持自动加载模式

3.5 看门狗

3.5.1 模块概述

看门狗模块用于防止芯片固件跑飞或部分硬件造成的系统卡死情况，一旦发生上述情况，

看门狗可以产生硬件复位，让整个芯片重新复位启动。

看门狗模块结构如下：

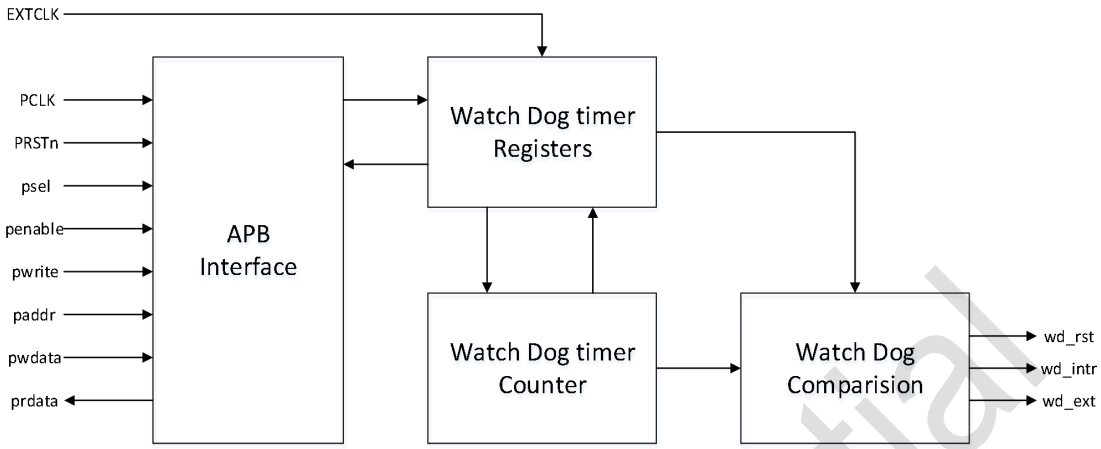


图 3.6 看门狗结构框图

3.5.2 模块特性

- 支持一路系统复位输出
- 复位输出时间可配置
- 支持一路 CPU 中断输出
- 内置 32 位递减计数器

3.6 SCU

3.6.1 模块概述

SCU 模块是系统控制单元，主要对芯片时钟、复位、功耗等芯片级配置进行控制。

SCU 模块架构如下：

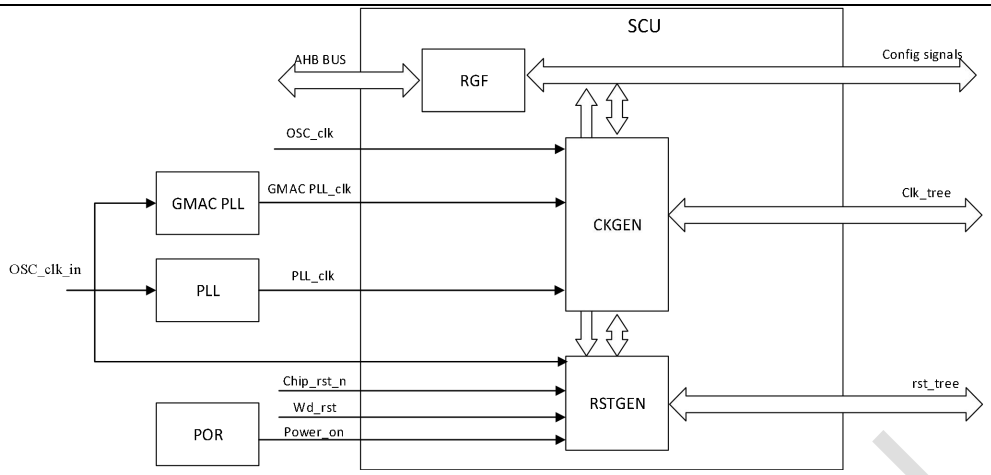


图 3.7 SCU 结构框图

3.6.2 模块特性

- 支持各模块时钟分频及门控
- 支持各模块复位控制
- 支持 PLL 输出频率可配
- 支持 PLL、OSC 时钟切换
- 支持管脚复用配置
- 内置看门狗复位状态寄存器

4 安全引擎

4.1 CRYPTO 引擎

4.1.1 模块概述

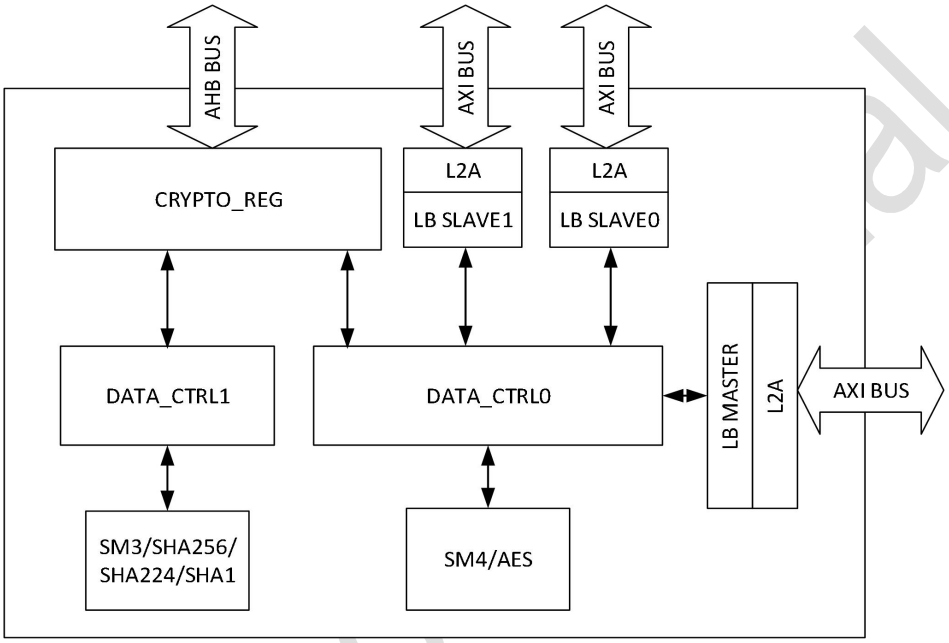


图 4.1 CRYPTO 引擎结构框图

CRYPTO 模块的作用主要是对进入模块的数据进行加解密操作。目前支持 SM4、AES 两种对称加密算法，同时支持 SM3、SHA1、SHA224、SHA256 四种 HASH 算法。两者之间相互独立，SM4、AES 数据走 AXI 总线，SM3、SHA1、SHA224、SHA256 数据走 AHB 总线。当数据从 AXI SLAVE 端口、AXI MASTER 端口或者 AHB SLAVE 端口进入 CRYPTO 模块之后，CPU 通过 AHB 总线配置 CRYPTO 模块寄存器，选择对应功能，直至加解密结束。

4.1.2 模块特性

- 支持一路 AHB SLAVE 配置端口
- 支持一路 AXI MASTER 端口
- 支持两路 AXI SLAVE 数据端口
- 支持 SM4 KEY 128 bit
- 支持 AES KEY 128/256 bit
- 支持 BYPASS 模式
- 支持数据填充和舍弃功能

- 对称加密模式支持数据输入输出端口选择
- 支持 ECB/CBC/CFB/OFB/CTR/XTS 六种操作模式（SM4/AES）
- 支持 SM4 and AES ≥800MB/s@200MHz（ECB/CTR/XTS）
- 支持 SM3/SHA1/SHA224/SHA256 ≥80MB/s@200MHz

4.1.3 工作方式

（1）BYPASS 模式

数据从 CRYPTO 模块流过，不做任何处理，输入输出相同。

①配置控制寄存器选择 bypass 模式
②配置中断使能寄存器（根据需求）
③配置数据流向寄存器选择输入输出端口
④配置数据长度寄存器
⑤配置开始寄存器开启数据传输
⑥等待数据传输完成

（2）FIFO 模式

将 CRYPTO 模块看成一个带有加解密功能的 FIFO，数据从一个 slave 端口写入，另一个 slave 端口取走（对应 FIFO 的读写端口）。上层 MASTER 将数据写入 CRYPTO 模块之后，对数据进行加解密操作，然后再由上层 MASTER 将已加解密完数据取走。

①配置控制寄存器选择密码算法、加/解密、算法模式、数据大小端、密钥类型，如果选择 CTR 模式还需配置步长寄存器
②配置中断使能寄存器（根据需求）
③配置密钥以及初始值寄存器
④配置数据流向寄存器，选择一个 AXI SLAVE 端口或两个 AXI SLAVE 端口（推荐使用两个，便于理解）
⑤配置数据长度寄存器
⑥配置开始寄存器，开始进行密钥扩展
⑦等待密钥扩展完成，配置开始寄存器开启数据传输
⑧等待数据传输完成

（3）BRIDGE 模式

由一个 MASTER 端口和一个 SLAVE 端口组成。可分为两种模式，一种是正常模式，另一种是 LLI 模式。正常模式下，只需要配置一次源地址或者目的地址，LLI 模式下可以将不同的源地址或者目的地址写入命令 FIFO 中，模块会自动根据 FIFO 中的命令去执行操作(MASTER 读是配置源地址，写配置目的地址)。两种模式下的数据长度寄存器是有区别的，正常模式下按照已配置好的数据长度操作，LLI 模式下按照写入 FIFO 中的命令数据长度操作（FIFO 中命令的数据总长度等于已配置的数据长度）。

①配置控制寄存器选择密码算法、加/解密、算法模式、数据大小端、密钥类型以及是否使用 LLI 模式，如果选择 CTR 模式，则还需配置步长寄存器

②配置中断使能寄存器（根据需求）
③配置密钥以及初始值寄存器
④如果配置了 LLI 模式，则需要向 LLI 寄存器中写入命令，如果没有则跳过
⑤配置数据流向寄存器，选择一个 AXI SLAVE 端口和一个 AXI MASTER 端口
⑥根据需求配置源地址或目的地址寄存器以及 MASTER 控制寄存器
⑦配置数据长度寄存器
⑧配置开始寄存器，开始进行密钥扩展
⑨等待密钥扩展完成，配置开始寄存器开启数据传输
⑩等待数据传输完成

（4）DMA 模式

由一个 MASTER 端口来完成读写操作。CRYPTO 模块会根据已配置的源地址及数据长度取数据进行加解密，然后将加解密后的数据写入对应目的地址。

①配置控制寄存器选择密码算法、加/解密、算法模式、数据大小端、密钥类型，如果选择 CTR 模式，则还需配置步长寄存器
②配置中断使能寄存器（根据需求）
③配置密钥以及初始值寄存器
④配置数据流向寄存器，选择一个 AXI MASTER 端口
⑤根据需求配置源地址或者目的地址寄存器以及 MASTER 控制寄存器
⑥配置数据长度寄存器
⑦配置开始寄存器，开始进行密钥扩展
⑧等待密钥扩展完成，配置开始寄存器开启数据传输
⑨等待数据传输完成

（5）哈希算法模式

①配置控制寄存器选择加密模式以及大小端
②配置中断使能寄存器（根据需求）
③CPU 向数据寄存器写入数据（512bit）
④检测加密核的状态是否处于忙状态
⑤如果检测到加密核的状态处于空闲状态，则继续向数据寄存器写入数据（如果是最后一笔则将控制寄存器的第 5 位使能，再继续向数据寄存器写入数据），重复该步骤直到数据输入完成
⑥等待传输结束，将最终结果从数据寄存器取走

4.2 PKE 引擎

4.2.1 模块概述

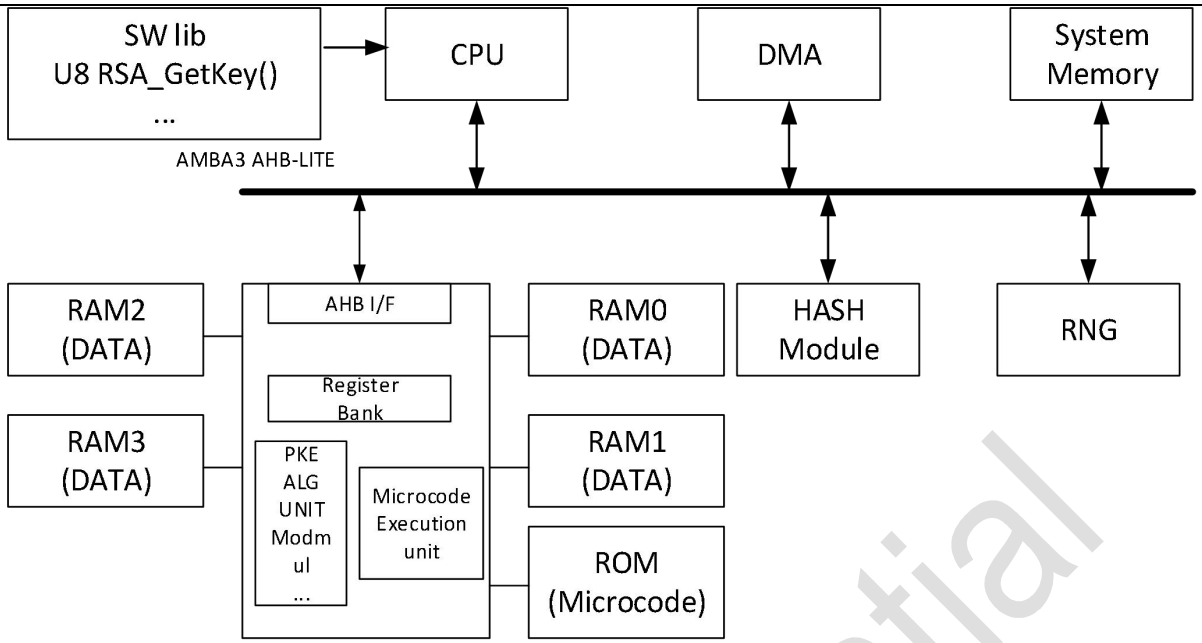


图 4.2 PKE 引擎结构框图

Public Key Engine（PKE）用来加速公钥密码运算中的大数模运算。公钥密钥的运算过程中，存在大量的大数模运算，对于普通的嵌入式 CPU 而言，完成这些大数模运算将会花费大量 CPU 指令，效率极低，因此在大多数支持公钥密码运算的芯片中都会加入公钥密码加速模块来完成公钥密码的运算。PKE 用来加速公钥密码中 RSA 和椭圆曲线（ECC）运算所涉及到的大数模运，RSA 和椭圆曲线密码是目前最为广泛使用的公钥密码。对于硬件而言，这两种加密算法都可以归结到操作数宽度分布在 32~4096 比特的模运算。其中，即使选用操作数位宽最小的 ECC-192，对于大多数 32 位的嵌入式设备而言，完成一次签名操作也会花费大量的 CPU 资源。PKE 模块将 CPU 从复杂的公钥密码运算中解放出来，CPU 只需要将输入参数配置好，PKE 会根据配置完成指定操作。目前，PKE 可以支持直接完成 RSA 中的模幂运算和 ECC 中的点乘运算。CPU 可以通过轮询或者中断方式来查询 PKE 的工作情况。

PKE 包含 AHB 接口模块（AHB I/F）、寄存器组模块、大数运算单元、微码运行单元（MEU）。另外，PKE 模块需要四块 RAM 和一块 ROM，可根据不同寄存器配置完成不同精度的运算。

4.2.2 模块特性

- RSA（可选 CRT）：512~4096 比特
- ECC（素数域）：192、224、256、384 和 521 比特
- 支持一路 AMBA 3 AHB-Lite 接口

4.2.3 工作方式

PKE 的运算通过微码（Microcode）形式完成，微码存储在程序存储单元中。因此通过向程序存储单元中灌入不同微码来实现不同要求的公钥密码运算。例如，在一个安全性要求较高的 SoC 中，可以向 PKE 模块中的程序存储单元灌入高安全性的公钥算法指令。在一些性能优先的设计中，可以向 PKE 模块中的程序存储单元灌入性能优化的公钥算法指令，实现性能优先的目的。在程序存储单元容量较大的设计中，可以将这些运算指令都写入 ROM，由 CPU 根据不同的使用场景进行实时调用，完整的微码大小大约为 2KB。

PKE 接口被映射到 7KB 地址空间内。这一块地址映射空间内主要包含 CPU 可以访问的所有操作数，这些操作数包含了模数、幂指数、部分中间变量等。除此之外，该地址映射空间内也包含控制和状态寄存器。CPU 可以通过控制寄存器和状态寄存器来配置、监控 PKE 模块。

PKE 支持的运算中，运算数最小为 192 比特，因此， CPU 或 DMA 将数据放入数据 RAM 中会遇到字间大小端问题。在 PKE 模块中，字与字之间都是按照小端进行排列的，下一个部分会给出具体的例子。

PKE 中，最小的操作数为 256 比特（4 个双字），因为目前 ALU 的输入位宽为 256 比特，如果操作数不是字对齐的，需要将高位补零。

PKE 接到开始命令后，开始进行运算，运算过程中，上位机可以通过状态寄存器查询目前的运行状态，也可以通过控制寄存器来中断目前的运行。另外，通过访问数据 RAM 地址可以获得部分中间运算结果。

上位机可以通过轮询或中断的方式来获取 PKE 是否完成目标运算的结果。数据 RAM 都是双字（64-bit）对齐，不支持字节对齐。

4.3 TRNG

4.3.1 模块概述

TRNG 模块通过物理随机源产生随机序列，后经 SM4 均衡处理，生成真随机数，为 SM2、RSA 等非对称算法提供密钥对。

4.3.2 模块特性

- 符合 GM/T 0005-2012《随机性检测规范》
- 符合 NIST SP800-90 a/b/c 的要求
- 集成 4 路物理随机源
- 具有在线健康检测功能
- 随机数生成速率≥30Mbps

5 USB OTG 接口

5.1 模块概述

USB OTG 接口是通用串行总线双功能设备控制器，支持 USB2.0/USB3.0 及可扩展主机控制器接口（XHCI）协议，可以通过寄存器配置选择来切换不同的功能。模块的功能框图如下：

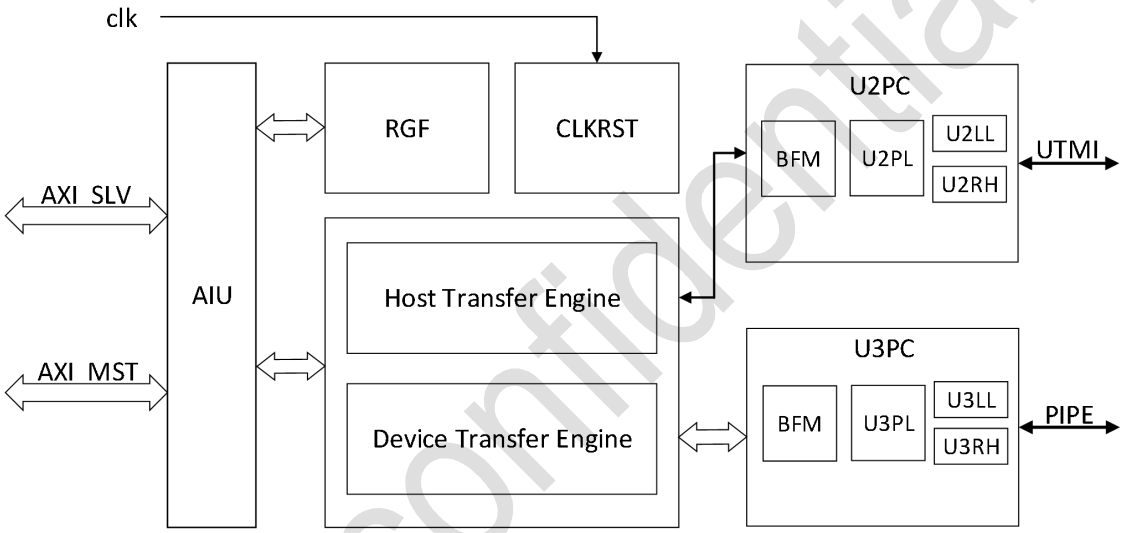


图 5.1 USB 内部结构框图

当 USB OTG 接口作为主机时，控制器根据系统软件准备的数据结构向 USB 设备发出传输请求，控制器支持 XHCI1.0 作为系统软件开发的标准接口。

当 USB OTG 接口作为设备时，控制器响应来自主机的传输请求，内置 9 个端点，端点使用数目可由控制器中的专用缓冲空间配置，端点缓冲空间与系统内存之间的数据传输可以通过内部 DMA 或外部 DMA 完成。

5.2 模块特性

- 支持可扩展主机控制器接口协议 1.0(XHCI1.0)
- 静态角色转换（主机/设备选择）
- 主机和设备模式下支持所有的 USB 传输类型，包括控制/批量/中断/等时传输
- 支持优异的功耗管理，USB3.0 模式下支持 U0/U1/U2/U3，USB2.0 模式下支持 LPM
- 主机和设备模式都支持 DMA 传输

- 主机模式下支持上下文缓存以减少等待时间
- 设备模式下支持 9 个端点
- 设备模式下每个端点的 FIFO 深度可配置
- 设备模式下支持大批量数据流协议

6 SATA 接口

6.1 SATA Host 控制器

6.1.1 模块概述

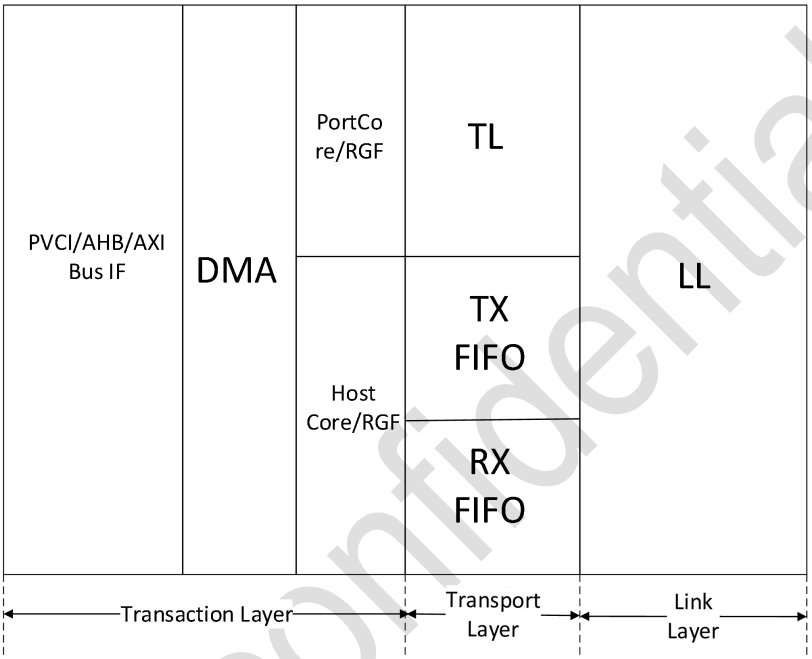


图 6.1 SATA Host 控制器结构框图

SATA host 控制器包含三个协议层：事务层，传输层和链路层。

事务层包含用户总线接口（AHB，AXI，PVCI），DMA 主控，端口/主机寄存器文件，以及端口/主机控制器：

1) DMA 控制器负责帧信息结构在系统内存和传输层 TXFIFO/RXFIFO 之间的发送和接收；
2) 主机核（Host core）负责全局复位，全局中断以及如 AHCI v1.1 协议中定义的每个端口命令完成合并，无论多少个端口被定义都只有一个主机核；
3) 主机寄存器文件（Host register file）是按照 AHCI v1.1 协议实现的，主机寄存器文件会提供实现的特性，比如对 HBA 的控制以及收集所有端口的状态反馈；
4) 端口核（Port core）负责处理 HBA 和已连接设备之间的事务。端口核请求 DMA 控制器从设备中获取一条命令或者数据 FIS 并将从设备中获取的 FIS 存储在系统内存中；
5) 端口寄存器文件（Port register file）与主机寄存器文件都是按照 AHCI v1.1 协议实现，端口控制器文件负责控制端口并反映端口上的事务和连接状态。

传输层负责构建需要发送的帧信息结构（FIS）并解析接收到的帧信息结构，传输层包含

三个主要的部分：FIS 发送器，FIS 接收器和 BIST 控制器模块。

链路层负责发送和接收帧，发送原语是基于传输层的控制信号，而接收原语来自物理层并且会转化成控制信号到传输层：

1) 数据的发送先经过 CRC 校验，加扰，8B/10B 转码，速度调整，然后发给物理层；
2) 数据的接收则经过数据调整，10B/8B 转码，解扰和 CRC 校验然后到传输层。

6.1.2 模块特性

- 符合 Serial ATA Revision 3.0 标准协议
- 符合 AHCI1.1 协议
- 支持数据传输速率 1.5Gbps，3.0Gbps 和 6.0Gbps
- 支持原生命令队列（NCQ）
- 支持命令列表覆盖特性
- 支持 PIO 针对多 DRQ 块
- 支持自动局部休眠功能
- 集成 TX FIFO 深度为 256 words
- 集成 RX FIFO 深度为 256 words
- 支持 PHY 数据位宽 20bit 或 40bit 可配

7 存储接口

7.1 eMMC0 控制器

7.1.1 模块概述

eMMC 控制器（以下简称 eMMC）是嵌入式多媒体设备的主机端控制器，去遵循 eMMC

标准协议，主要用于完成同 eMMC 器件命令及数据的交互，在固件的配合下，该模块可支持 eMMC5.1 协议相关特性，并向下兼容。eMMC 架构框图如下：

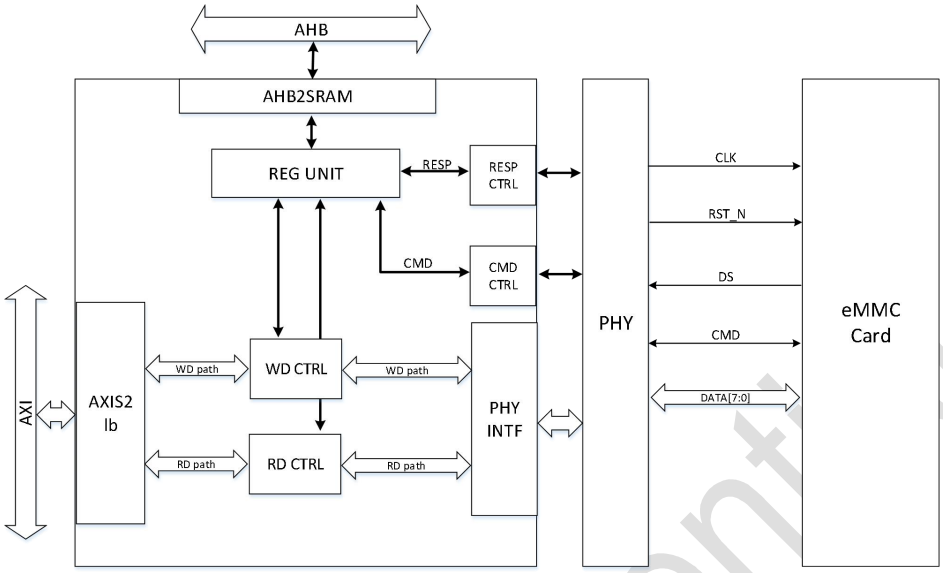


图 7.1 eMMC 控制器结构框图

7.1.2 模块特性

- 支持 1 路 AHB 从配置端口
- 支持 1 路 AXI 从数据传输端口
- 支持 eMMC 5.1 协议标准命令、响应及数据传输格式
- 硬件不支持 QE 操作，其功能由固件驱动实现
- 支持 1/4/8 线传输模式
- 支持 eMMC 协议规定的 HS400/HS200/SDR52/DDR52 模式
- 支持 1 路缓存命令通道
- 支持 1 路直接命令通道
- 支持基于块的数据传输模式，数据块长度为 512B
- 支持时钟流控管理功能
- 支持命令 CRC7 校验及数据 CRC16 校验
- 内置硬件 PHY，集成 DLL 数字锁相环
- 支持 timing 时序可调
- 支持查询和中断两种模式检查命令完成
- 支持超时及错误中断

7.1.3 工作方式

eMMC 寄存器控制模块包含两个命令通道，直接命令通道和缓存命令通道。

缓存命令通道作为一个命令缓存队列，可以缓存多组固定长度的读写命令，并实现响应（response）对比。每一个使用缓存命令通道的命令需要配置四个寄存器，缓存命令参数寄存器，缓存命令寄存器，响应寄存器和响应位使能寄存器。

直接命令通道需要配置两个寄存器，直接命令参数寄存器和直接命令寄存器，另外读写数据还需要配置直接命令字节计数寄存器。直接命令通道的优先级高于缓存命令通道，但无法进行硬件内部的响应对比。直接命令通道的数据传输以字节为单位，字节数由直接命令字节计数寄存器决定，缓存命令通道的数据传输以块（512 字节）为单位，传输长度由缓存命令寄存器高 16 位决定。直接命令通道每次只能发一个命令，需要等到命令（不带响应的）发送完成或响应返回后才能发下一个命令，缓存命令通道可以一次存入多条固定长度块传输的命令，然后 eMMC 控制器会依次执行并进行响应对比。

8 外围设备接口

8.1 QSPI 控制器

8.1.1 模块概述

QSPI 控制器主要用于外扩 SPI SRAM、SPI flash 外设等。

QSPI 控制器架构如下：

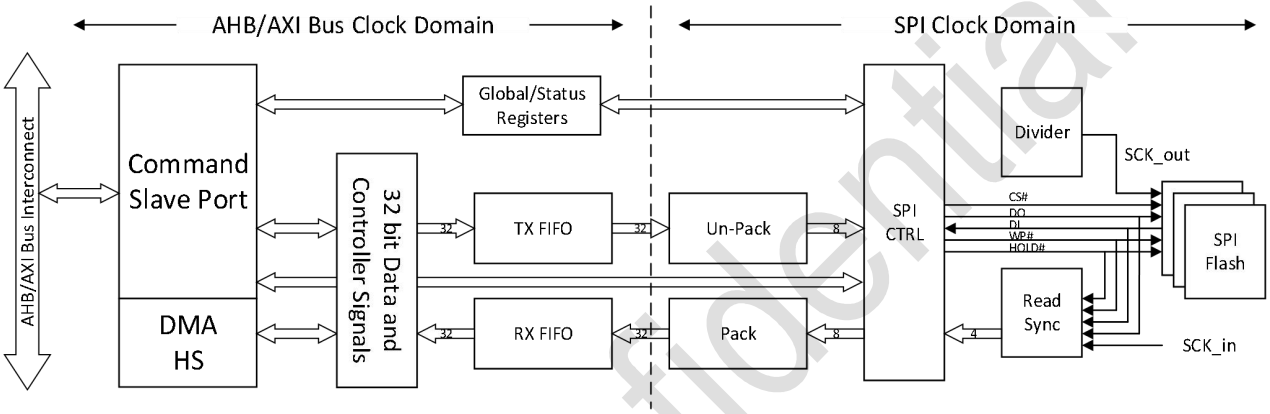


图 8.1 QSPI 控制器结构框图

8.1.2 模块特性

- 控制器时钟和接口时钟异步可调
- 支持 SPI 单线/双线/四线模式
- 最高接口工作频率 100 MHz

8.2 SPI 控制器

8.2.1 模块概述

SPI控制器挂载于APB总线上，符合Motorola总线协议，可作为SPI 主从设备进行外设扩展，操作简单、可扩展性强。

SPI模块结构如下：

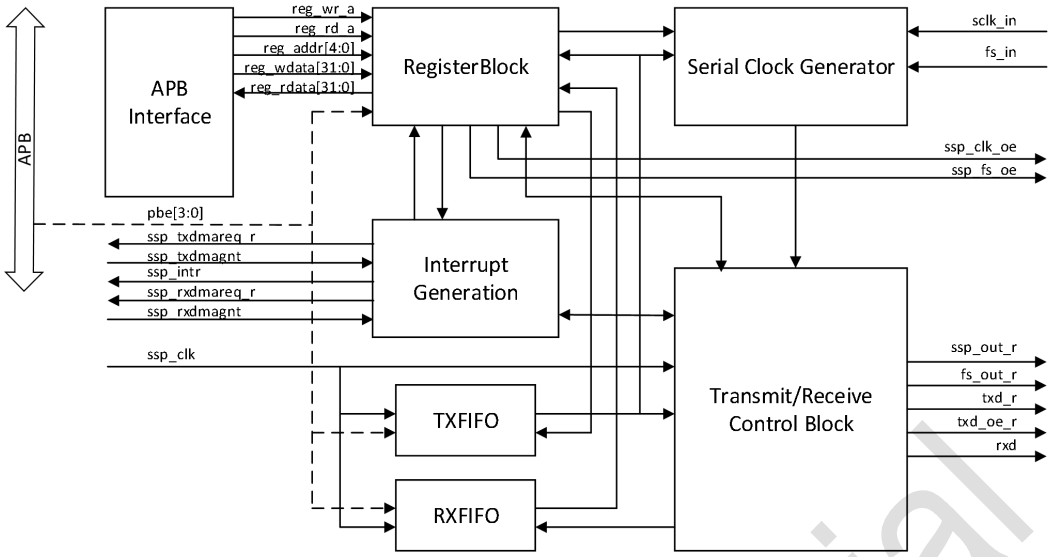


图 8.2 SPI 控制器结构框图

8.2.2 模块特性

- 支持 Motorola SPI 协议标准
- 最高接口工作频率 20 MHz
- 支持主从模式
- 输出时钟的极性、相位、频率可配
- 串行数据支持 MSB 或者 LSB first 模式
- 集成 32bytes TXFIFO
- 集成 32bytes RXFIFO
- TXFIFO/RXFIFO 阈值中断可配
- 支持中断和查询模式
- 独立的 SPI 工作时钟
- 独立可配置的中断使能

8.3 UART0 控制器

8.3.1 模块概述

UART0 控制器与通用的 16C550 UART 完全兼容。
UART0 控制器架构如下：

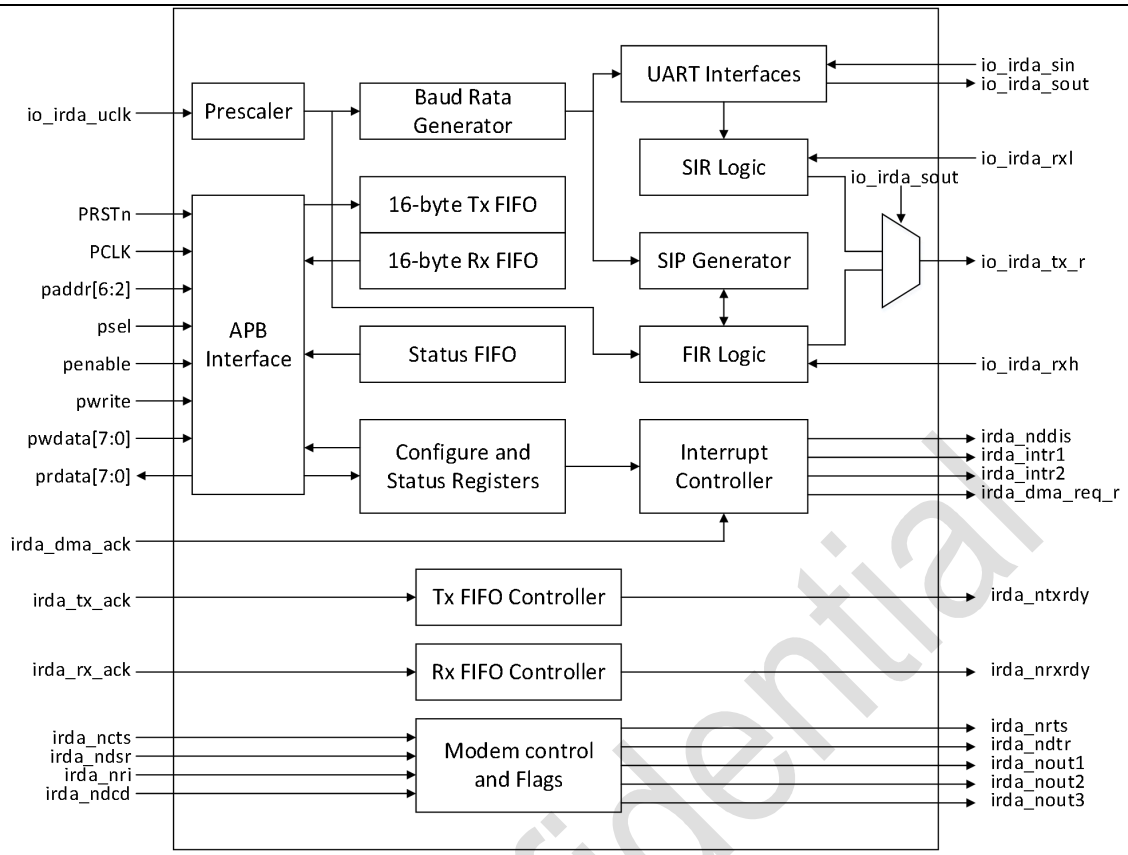


图 8.3 UART 控制器结构框图

*注：上图中 Irda 功能本芯片中未支持

8.3.2 模块特性

- 完全兼容高速 NS 16C550A UART
- 最高波特率为 3Mbit/s
- 集成 32bytes TX FIFO
- 集成 32bytes RX FIFO
- 支持奇偶校验方式或无校验
- 支持帧错误检测
- 支持 FIFO 溢出报警
- 波特率可配置
- 支持数据位和停止位的位宽配置，数据位宽可配置为 5/6/7/8bits，停止位可配置为 1/1.5/2bits.

8.4 UART1 控制器

UART1 控制器与 UART0 控制器内部结构及逻辑完全相同，只是基地址不同。

8.5 GPIO1 控制器

8.5.1 模块描述

GPIO1 提供 12 位可编程的输入输出管脚。每个管脚可配置为输入或输出。管脚用于生成特定应用的输出信号或采集特定应用的输入信号。输入管脚，GPIO 可作为中断源；输出管脚，每个 GPIO 都可以独立地清 0 或置 1。

GPIO1 的 12 个管脚输入状态下也可以根据电平或跳变值产生可屏蔽中断。

GPIO1 模块结构图如下：

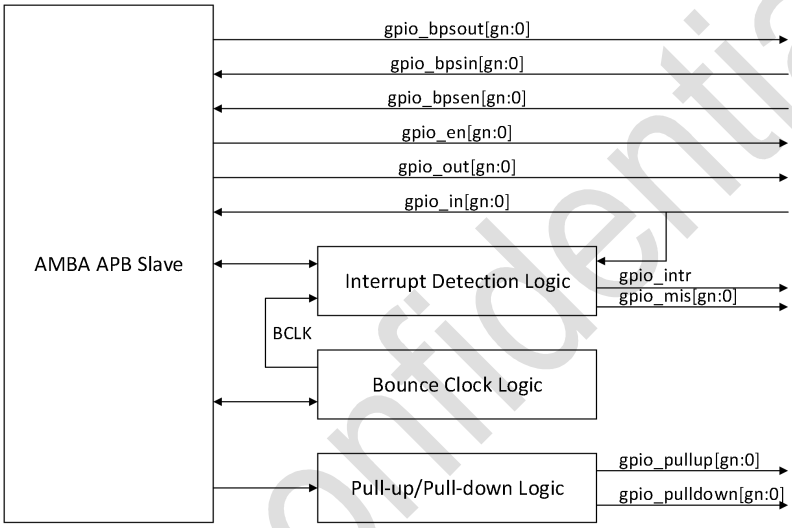


图 8.4 GPIO 控制器结构框图

8.5.2 模块特性

- 12 个管脚可独立设置为输入或输出
- 每个管脚均可以设置为 bypass 模式
- 每个管脚输入状态下可作为中断源
- 输入中断源可以设置为电平触发或边沿触发
- 每个端口可通过 SCU 配置为上拉或下拉
- 输出状态下每个 bit 都可单独设置 0 或 1
- 所有管脚上电复位后默认为输入

9 安全特性

9.1 电压检测

9.1.1 模块概述

电压检测模块 VDT 用于检测当前 IO 电压是否正常，当 IO 电压低于配置电压时，电压检测模块将触发 CPU 中断，可有效防止各种电压攻击手段。

电压检测模块结构如下图所示：

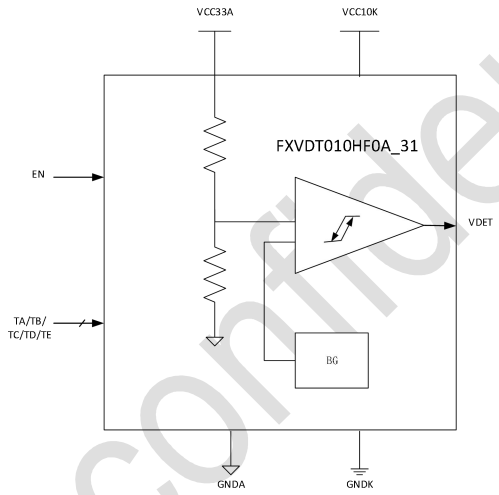


图 9.1 电压检测模块框图

9.1.2 模块特性

- 节点工作温度范围-40~125℃
- 支持低功耗模式
- 支持检测电压阈值微调

9.2 温度检测

9.2.1 模块概述

温度检测 TDC 是一个高速温度转数字信号模块，可以帮助 CPU 进行实时温度监控及报警，当芯片处于极端环境或者瞬时温差较大的情况下，CPU 可以调整各模块配置让芯片进入更加安全的工作模式，以保持芯片工作的稳定性，同时也可以防止外部温度环境的攻击。

TDC 模块结构如下：

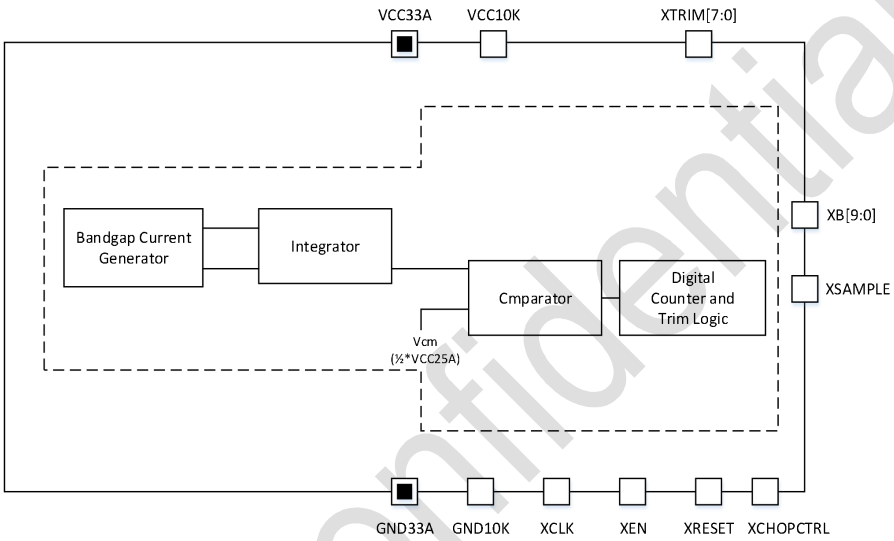


图 9.2 温度检测模块结构框图

9.2.2 模块特性

- 工作温度范围：-40~125℃
- 转换精度 10bit
- 转换速率 1.0KSPS
- 支持低功耗模式

9.2.3 模块时序

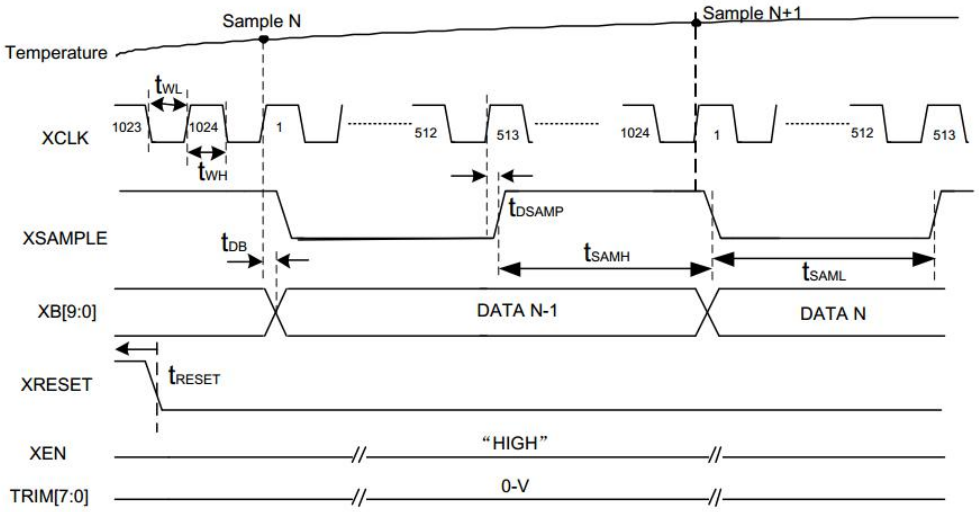


图 9.3 TDC 工作时序图

9.3 物理探测防护

9.3.1 金属屏蔽层

芯片采用 Power mesh 方法增加了金属屏蔽层，可有效防止芯片外部的电磁攻击。

9.3.2 后端设计防护

采用 Chip Level 层 Flatten 的方法，将接口电路、功能电路、密码算法电路和随机电路等完全进行混合布线，可有效防止后端电路反向分析等外部攻击。

9.4 芯片 ID

9.4.1 模块概述

芯片内置 OTP（One Time Programmable）电路，提供一次性编程机会，可作为芯片全球唯一识别号。

9.4.2 模块特性

- 有效数据位宽 64bits

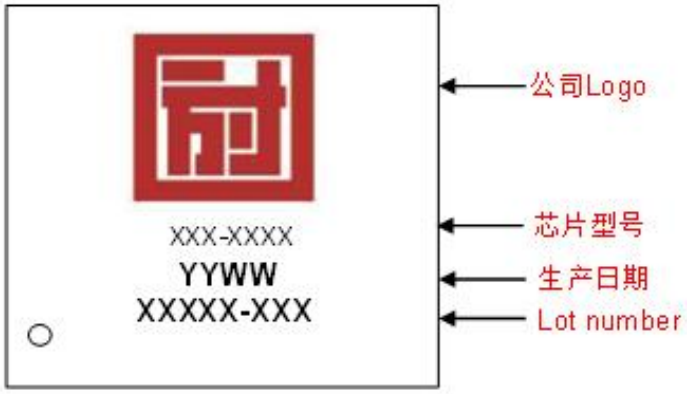
- 可支持出厂烧写和用户烧写 2 种模式
- 用户可自定义烧写内容
- 支持低功耗模式

订购信息

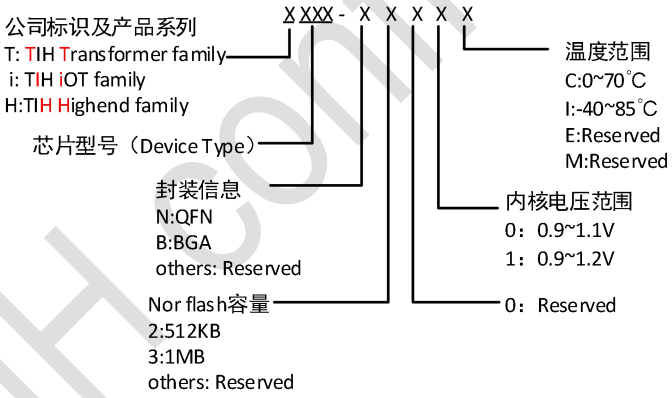
芯片名称	flash 容量	封装信息	温度范围	Package Qty
T620-N200C	512KB	QFN64	0~70℃	2600
T620-N300C	1MB	QFN64	0~70℃	2600

*注：Package Qty 表示单包芯片数量。

芯片外部丝印



芯片命名规则



举例