

A32DQ88D2

规格书



深圳市万物芯联科技有限公司
www.althico.com

版本号	文件修改描述	修订者	日期
V1.0	创建	Leo	2020-09-23
V2.0	补充系统框图	alex	2021-6-2

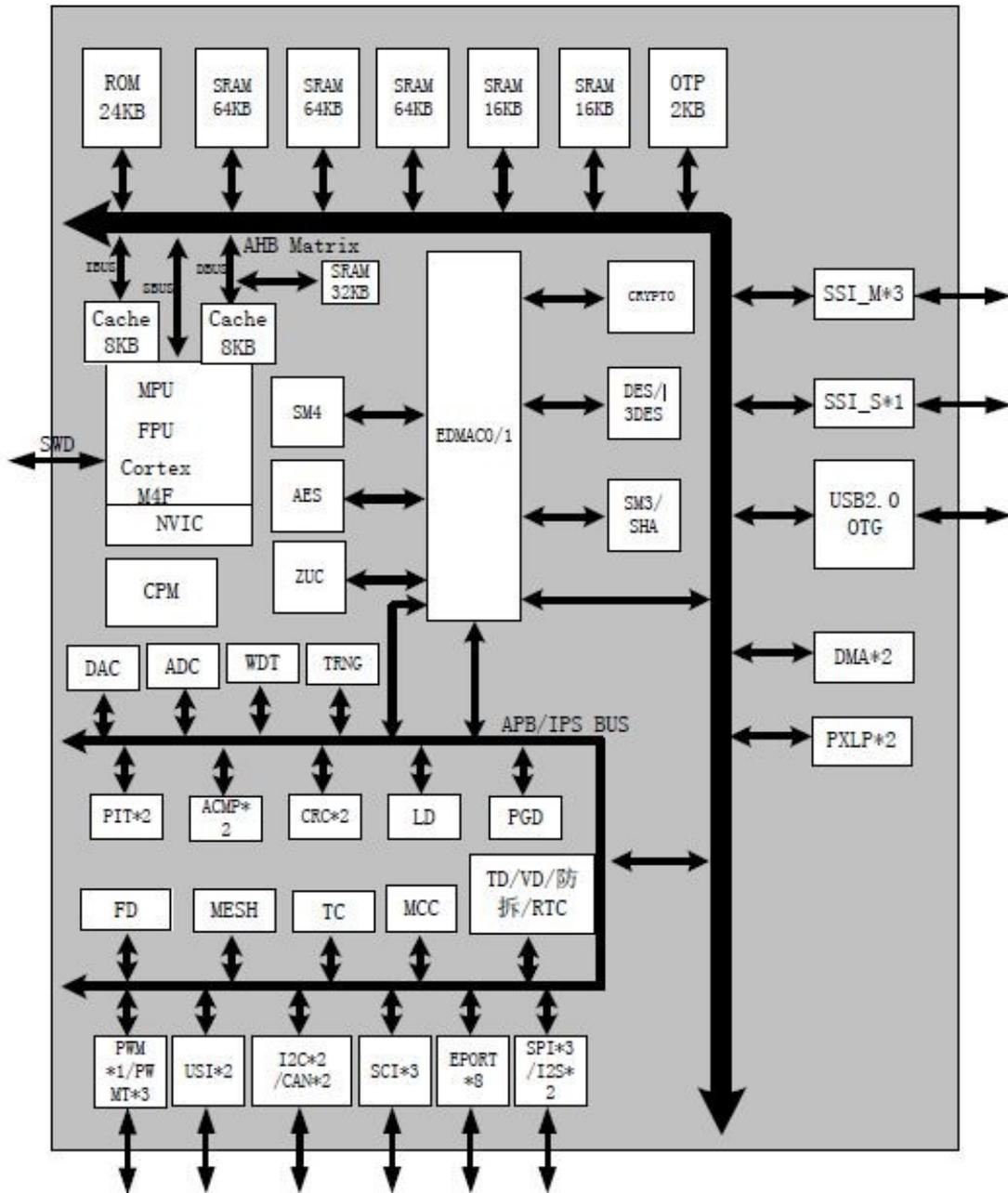
目录

1	简介	3
2	系统框图	4
3	关键特性	5
3.1	CPU内核	5
3.2	片上存储单元.....	5
3.3	两路DMA接口	5
3.1	两路EDMA接口.....	5
3.2	AES协处理器.....	6
3.3	DES协处理器.....	6
3.4	SM4 协处理器	6
3.5	Crypto 协处理器.....	6
3.6	SHA	6
3.7	ZUC	7
3.8	两路PXLP模块.....	7
3.9	两路CRC校验单元	7
3.10	一路随机数发生器.....	7
3.11	两路PIT定时器（可编程定时器）	7
3.12	一路定时计数器（Time Counter）	7
3.13	一路WDT定时器（看门狗）	8
3.14	时钟电源管理模块（CPM）.....	8
3.15	复位控制器.....	8
3.16	三路SPI接口	8
3.17	两路I2S接口.....	9
3.18	两路CAN接口	9
3.19	四路SSI接口	9
3.20	八路边沿检测功能的EPORT接口	9
3.21	一路USB2.0 OTG接口	9
3.22	两路ISO7816 接口	10
3.23	两路I2C接口.....	10
3.24	三路可编程串行通信接口SCI(UART)	10
3.25	一路普通PWM定时器.....	11
3.26	三路高级PWM定时器.....	11
3.27	一路ADC	11
3.28	一路DAC	11
3.29	两路ACMP（模拟比较器）	12
3.30	一路MCC.....	12
4	算法性能	12
5	芯片工作条件及功耗.....	14
6	可靠性说明	14
7	工艺	14
8	封装	14

1 简介

芯片采用 32 位高性能核 Cortex-M4F，片上集成了 256KB SRAM、24KB ROM、2KB OTP。同时硬件算法协处理器需提供 AES、DES/3DES、CRYPTO（RSA/ECC/SM2/SM9）、SM3/SM4、SHA-0/SHA-1/SHA-224/SHA-256/SHA-384/SHA-512、ZUC 安全算法、PXLp 算法、真随机数发生器以及 PCI 安全模块。芯片拥有 USB2.0 OTG、SPI、SSI_MASTER、SSI_SLAVE、ISO7816、I2C、UART、EPORT、ADC/DAC/ACMP、MCC（磁条解码接口）、PWM/PWMT、I2S、CAN 等通讯接口，同时支持 DMA 数据直接访问接口。同时芯片内部含有 27.12Mhz 时钟输出（需外接晶体，如供给蓝牙的时钟晶体）。

2 系统框图



3 关键特性

3.1 CPU内核

- 32 位 CPU 内核 Cortex-M4F
- 支持单精度浮点单元(FPU)
- 存储器保护单元 MPU
- 外部总线支持 8bit/16bit/32bit 访问
- 面向应用的存储分区
- 支持硬件安全访问控制外围组件访问受控
- 支持 SWD
- 嵌套矢量中断控制器(NVIC)：低延迟、低抖动中断响应
- 低功耗高性能

3.2 片上存储单元

- 24KB ROM，可进行字，半字和字节读访问
- 256KB SRAM，可配置 256K/128K/64K 可选
- 含有 2KB OTP 模块

3.3 两路DMA接口

- 支持传输长度可配置
- 支持读写地址可以配置
- 支持 Memory-to-Memory，Memory-to-Peripheral，Peripheral-to-Memory 以及 Peripheral-to-Peripheral 四种传输类型可配置
- 通过使用链表来支持Scatter or Gather

3.1 两路EDMA接口

- 支持双通道
- 可编程传输数据数量

- 可编程读缓存地址和写缓存地址
- 支持读、写、写后读传输。

3.2 AES协处理器

- 支持 128/192/256 bits key 算法引擎
- 支持 ECB 和 CTR 模式的加密和解密
- 抗攻击设计

3.3 DES协处理器

- DES/3DES 引擎
- 支持 DES、3DES、2 KEY 和 3 KEY 算法的加密解密
- 支持 EBC 模式和 CBC 模式的加密和解密
- 抗攻击设计

3.4 SM4 协处理器

- 支持 128bit KEY
- 支持 EBC、CBC、CFB、OFB 模式的加密和解密
- 抗攻击设计

3.5 Crypto 协处理器

- 支持大数（1024/2048 比特）模乘/模幂运算
- 支持最高 521 比特 ECC/SM2 算法的点加，点倍，点乘运算；
- 抗攻击设计

3.6 SHA

- 支持 SM3(256)
- 支持 SHA0(160)
- 支持 SHA1(160)

- 支持 SHA224
- 支持 SHA256
- 支持 SHA384
- 支持 SHA512
- 抗攻击设计

3.7 ZUC

- 支持 ZUC 标准加密和解密算法
- 支持密钥分组长度为 128 比特加解密运算
- 支持抗侧信道攻击设计

3.8 两路PXL模块

- 支持卷积 ABS 算法

3.9 两路CRC校验单元

- 支持 CRC32、CRC16、CRC8

3.10 一路随机数发生器

- 可以串行输出真随机数序列，最快可达 20Mbps

3.11 两路PIT定时器（可编程定时器）

- 32 位定时器

3.12 一路定时计数器（Time Counter）

- 128KHZ 独立时钟源
- 16 位计数器
- 预分频支持 0.125~16mS

3.13 一路WDT定时器（看门狗）

- 提供跳出软件死循环或系统锁死的功能

3.14 时钟电源管理模块（CPM）

时钟和电源管理模块特性包括：

- 两个系统时钟源
 - ◆ 内部高速振荡器，频率为 320MHz
 - ◆ 内部低速振荡器，频率为 8MHz
- 支持低功耗模式
- 独立的时钟分频设置
- 独立的模块时钟开关

3.15 复位控制器

- 内部上电复位 (POR)
- 外部复位 (RESET 管脚)
- 软件复位
- 看门狗定时器复位
- 高低电平检测复位 (HVD/LVD)
- 高低频率检测复位 (HFD/LFD)
- 软件可读状态标志表明上次复位的中断源

3.16 三路SPI接口

- 支持主、从模式；
- 支持极性和相位可编程的串行通信时钟
- 支持从模式选择输出
- 支持中断请求
- 接口可复用 GPIO

3.17 两路I2S接口

- 支持主、从模式；
- 半双工通讯
- 可编程预分频器
- 支持 I2S 飞利浦标准

3.18 两路CAN接口

- 支持 CAN2.0B
- 64 个可灵活配置数据大小（0-8 个）的 Buffer
- 16 bit 的计时器
- 可屏蔽中断

3.19 四路SSI接口

- 串行主机，可以和串行从机通讯
- 可配置的串行帧格式：1）摩托罗拉模式 2）TI 模式 3）MicroWire 模式
- 使用握手信号发起总线式 DMA 的数据传输请求
- 支持 2 线/4 线模式
- 一路主合封四线 Norflash，一路主合封四线 PSRAM，一路从接两线摄像头，一路主接两线 SPI LCD

3.20 八路边沿检测功能的EPORT接口

- 支持低电平中断
- 支持边沿中断（上升沿、下降沿或两者可配置）
- 可复用成 GPIO（每路 EPORT 模块包含 8 个 GPIO）

3.21 一路USB2.0 OTG接口

- 兼容 USB2.0 OTG 协议
- 最高速率 480Mbps 工作模式

3.22 两路ISO7816 接口

- 支持 ISO7816-3 协议
- 支持主从模式
- 支持卡及读卡器模式
- 支持 T=0 和 T=1 协议
- 支持 F/D 因子：8, 12, 16, 31, 32, 31, 23.25, 46.5, 93, 186, 372, 744, 64, 128, 256, 512
- 9-bit guard time counter (GTCNT)
- 24 bits waiting time counter (WTCNT)
- 支持 8 字节接收 FIFO
- 接口可以复用成 GPIO
- USI1 接口支持低功耗唤醒
- USI2 做读卡器有独立 LDO 供电

3.23 两路I2C接口

- 支持主从模式
- 兼容 I2C 2.1 总线标准
- 支持 7 位以及 10 位地址模式

3.24 三路可编程串行通信接口SCI(UART)

- 全双工操作；
- 波特率可灵活配置；
- 可编程 8 位或 9 位数据格式；
- 发送和接收可独立控制；
- 支持帧接收错误检测；
- 硬件奇偶检测；
- 支持灵活的标志位中断请求（如传输数据寄存器空、传输完成、接收数据寄存器满等）
- 接口可复用 GPIO

3.25 一路普通PWM定时器

- 可编程周期和占空比
- 支持捕获功能
- 2 个 Dead-Zone 发生器
- 8 路可独立配置引脚

3.26 三路高级PWM定时器

- 16 位计数器
- 16 位可编程预分频器
- 最大 4 个独立通道
 - ◆ 输入捕捉
 - ◆ 输出比较
 - ◆ PWM 产生
 - ◆ 单脉冲模式输出
- 带可编程 dead-time 的互补输出
- 带紧急刹车控制
- 用于外部信号同步或者多个 Timer 串联同步的同步控制逻辑
- 灵活的中断或者 DMA 请求

3.27 一路ADC

- 支持 6bit、8bit、10bit、12bit 分辨率
- 可编程采样周期
- 12 个普通 Channel

3.28 一路DAC

- 12 位精度
- 支持数据左对齐、右对齐格式

- 支持 DMA
- 支持外部触发源启动转换
- 支持 FIFO 操作

3.29 两路ACMP（模拟比较器）

- 8 对差分比较输入（VIP，VIN）
- 比较电压输出
- 过滤毛刺功能
- 可配置建立时间

3.30 一路MCC

- 支持 ISO/IEC 7811-2
- 支持 F2F 编码
- 支持不同的 char width, 7bit(track0)/5bit(track0)
- 支持 3 轨磁头解码

4 算法性能

算法	工作模式及条件	性能
SM2(256)	生成密钥对@(80MHZ,SRAM 运行程序, 运行 Crypto/ENCR 模块)	250 次/s
	签名@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	230 次/s
	验证@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	115 次/s
SM3	加密@(80MHZ, SRAM 运行程序, 运行 SHA/ENCR 模块)	420Mbps
SM4	加解密@(80MHZ, SRAM 运行程序, 运行 SM4/ENCR 模块)	215Mbps
AES(256)	加解密@(80MHZ, SRAM 运行程序, 运行 AES/ENCR 模块)	225Mbps
DES	加解密@(80MHZ, SRAM 运行程序, 运行 DES/ENCR 模块)	151.4Mbps
RSA (1024)	生成密钥对@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	5 次/s
	解密/签名@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	220 次/s
	加密/验签@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	4000 次/s
	生成密钥对@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	0.55 次/s

RSA (2048)	解密/签名@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	35 次/s
	加密/验签@(80MHZ, SRAM 运行程序, 运行 Crypto/ENCR 模块)	1050 次/s

5 芯片工作条件及功耗

- 工作温度：-40~85 摄氏度
- 存储温度：-40~125 摄氏度
- 系统典型工作频率：160MHz
- 支持工作电源输入范围：3.3V
- 工作模式功耗（常温）
 - ◆ 深度睡眠模式（poff2）：小于 1 uA
 - ◆ 睡眠模式（sleep）：小于：100uA

6 可靠性说明

- HBM: 2KV
- MM: 200V
- CDM: 500V
- Latch-Up: 200mA

7 工艺

- TSMC 40nm ULP Logic

8 封装

- QFN88