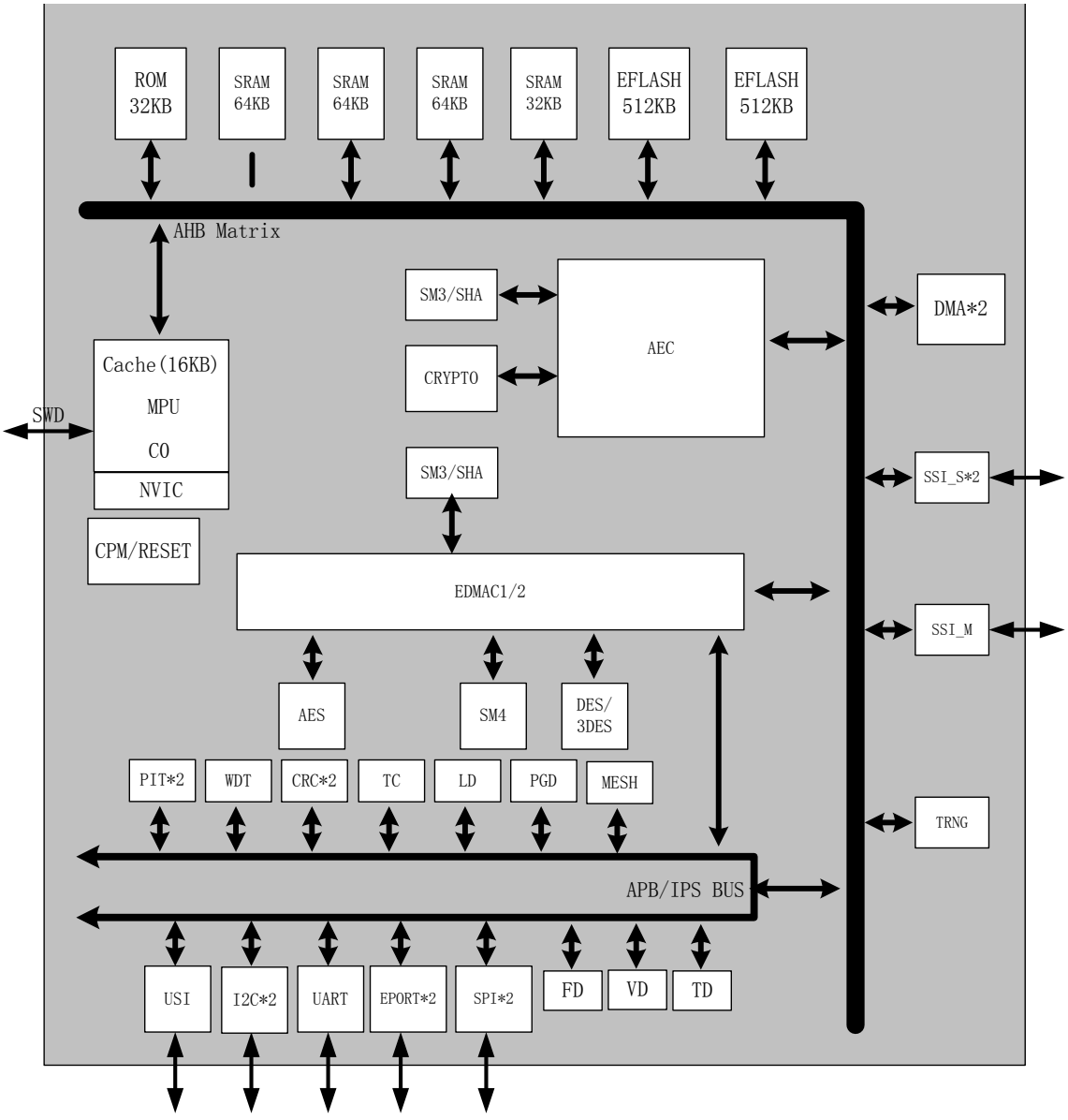
CCM3320S 车规算法安全芯片规格书

2020-10-10

1 简介

芯片采用国芯自主知识产权的 32 位高性能低功耗安全内核 CS0，片上集成了 224KB SRAM、32KB ROM 和 1MB EFlash。同时硬件算法协处理器需提供 SM4，AES，DES/3DES、CRYPTO（RSA、ECC、SM2）、SM3/SHA 安全算法和真随机数发生器。芯片拥有 SPI、SSI、ISO7816、I2C、UART、EPORT，同时支持 DMA 数据直接访问接口以及算法硬件调度模块。同时芯片应具备高安全防御设计，可抵御电压、温度、频率、光照异常检测以及电源毛刺检测，专门的功耗处理以防止功耗和电磁辐射分析，专门的版图设计以保护信号层不受攻击。

2 系统框图



3 关键特性

3.1 CPU内核（CS0）

- 32 位 load/store 结构
- 固定的 16 位指令长度
- 16 项，32 位通用寄存器文件
- 高效率 3 级执行流水线
- 大部分指令是单周期执行，3 周期跳转指令
- 支持字节/半字/字访问
- 内嵌中断控制器，支持嵌套中断和低功耗模式唤醒
- 32 位 x 32 位 硬件整数乘法单元（单周期）
- 可选的 32 位 / 32 位 硬件整数除法单元（3~13 周期）
- 内嵌 MPU 安全保护单元
- 片上仿真支持
- 全静态设计以减少功耗

3.2 片上存储单元

- 32KByte ROM，可进行字，半字和字节读访问
- 224KB SRAM，可进行字，半字和字节读写访问
- 1MB EFLASH
  - Main Block ：128KX39bit（7 个 ECC bit）
  - Info Block :1KX39bit（7 个 ECC bit）
  - 页大小：512X39bit（7 个 ECC bit）
  - 片擦除时间：100ms(最大值)
  - 页擦除时间：100K Endurance 部分：100ms(最大值)；
    10K Endurance 部分：20ms(最大值)
  - 39-bit 编程时间：15us (最大值)

- ◆ 数据最大可擦写次数：全部容量：10K；

  小于等于 2Mb 容量：100K
- ◆ 数据保存时间：10 年@125℃

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

3.4 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。

3.5 AES分组密码算法

- ■ 支持 AES 加密、解密算法
- ■ 支持密钥分组长度为 128/192/256 比特
- ■ 支持 ECB/CBC/OFB/CFB/CTR/CCM 工作模式
- ■ 支持 Key Wrap 密钥封装模式
- ■ 抗侧信道攻击设计

3.6 DES/3DES分组密码算法

- ■ 支持 DES/3DES 加密、解密算法
- ■ 支持密钥分组长度为 64 比特的 DES
- ■ 支持密钥分组长度为 128/192 比特的 3DES

- 支持 ECB/CBC/OFB/CFB 工作模式
- 抗侧信道攻击设计

3.7 SM4 分组密码算法

- 支持 SM4 加密、解密算法
- 支持密钥分组长度为 128 比特
- 支持 ECB/CBC/OFB/CFB/CCM 工作模式
- 支持 Key Wrap 密钥封装模式
- 抗侧信道攻击设计

3.8 CRYPTO 公钥密码算法协处理器

- 支持最高位宽为 2048 比特大数的模乘，模幂，蒙哥马利模乘等运算
- 支持最高位宽为 512 比特素域下的 ECC/SM2 算法的点加和倍点运算；
- 支持 RSA/SM2/ECC 等公钥密码算法
- 抗侧信道攻击设计

3.9 SHA杂凑算法

- 支持 SM3(256)杂凑算法
- 支持 SHA0/1(160) 杂凑算法
- 支持 SHA224/SHA256 杂凑算法
- 支持 SHA384/SHA512 杂凑算法

3.10 AEC（算法引擎控制器）

- 支持两路 SPI 接口并行调度
- 支持公钥算法独立自动调度
- 支持杂凑算法独立自动调度
- 支持指令的自动解析和执行

3.11 CRC校验单元

- 支持 CRC32、CRC16、CRC8

3.12 随机数发生器

- 可以串行输出真随机数序列，最快可达 20Mbps

3.13 两路PIT定时器（可编程定时器）

- 32 位定时器

3.14 异步定时器（Timer）

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

3.15 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

3.16 时钟电源控制器

- 可选系统时钟源
- 独立的分频器
- 支持低功耗模式
- 独立的时钟门控

3.17 复位控制器

- 内部上电复位
- 外部复位（POR 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

3.18 两路SPI接口

- 支持主、从模式（软件可配）
- 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

3.19 两路SSI从接口

- 串行从机，可以和串行主机通讯
- 支持摩托罗拉模式的串行帧格式
- 通过指令，地址，数据的自定义协议将端口 SPI 传输直接转换为内部 AHB 传输
- 单次指令最大支持传输 64 word 数据
- 支持单线、双线、四线模式

3.20 一路SSI主接口

- 串行主机，可以和串行从机通讯
- 支持摩托罗拉模式的串行帧格式
- 使用握手信号发起总线式 DMA 的数据传输请求
- 支持单线、双线、四线模式
- 支持 XIP(芯片内执行)模式

3.21 16 路具有边沿检测功能的EPORT接口（复用）

- 支持电平中断

- 支持边沿中断（上升沿、下降沿或两者可配置）
- 可复用成 GPIO

3.22 一路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

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 一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 安全防护

- 安全检测与防护单元
  - 光照异常检测单元
  - 电压异常检测单元
  - 温度异常检测单元
  - 频率异常检测单元
  - 电源毛刺检测单元
  - 主动防护层检测单元(MESH)；
- 存储器加密机制
- 唯一芯片序列号
  - 每颗芯片都具有唯一序列号

4 算法性能

算法	工作模式及条件	性能
SM2(256)	生成密钥对@(200MHZ,SRAM 运行程序，运行 Crypto/AEC 模块)	6000 次/s
	签名@(200MHZ, SRAM 运行程序，运行 Crypto/AEC 模块)	6500 次/s
	验证@(200MHZ, SRAM 运行程序，运行 Crypto/AEC 模块)	3400 次/s
SM3	加密@(200MHZ, SRAM 运行程序，运行 SHA/AEC 模块)	800Mbps
SM4	加解密@(100MHZ, SRAM 运行程序，运行 SM4/ENCR 模块)	100Mbps
AES	加解密@(100MHZ, SRAM 运行程序，运行 AES/ENCR 模块)	100Mbps
DES	加解密@(100MHZ, SRAM 运行程序，运行 DES/ENCR 模块)	100Mbps
SHA	加密@(200MHZ, SRAM 运行程序，运行 SHA/AEC 模块)	800Mbps

5 芯片工作条件及功耗

- 工作温度：-40~105 摄氏度
- 存储温度：-55~150 摄氏度
- 系统典型工作频率：200MHz
- 支持工作电源输入范围：1.8V/3.3V
- 工作模式功耗（常温）
  - hibernation 模式（poff2.0）：小于 0.3uA
  - lowpower 模式（sleep）：典型值 100uA（以实测为准）
  - 运行模式:小于 300mA

可靠性说明

- HBM：2KV
- CDM：500V
- Latch-Up：200mA

6 工艺

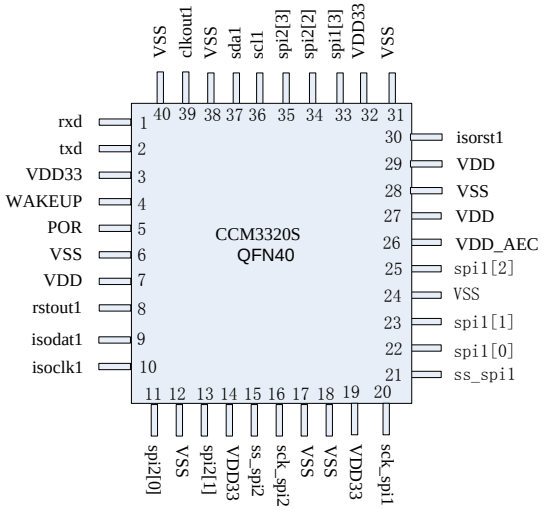
- TSMC 40nm ULP EFLASH

7 安全认证

- EAL4+
- 国密二级
- AEC-Q100（Grade 2）

8 封装说明

- QFN40



“

PIN No.	PIN Name	ALT1	ALT2	ALT3	Description
1	rxd	eport0[7]	eport2[7]		UART receiving data /GPIO
2	txd	eport0[6]	eport2[6]		UART transmitting data /GPIO
3	VDD33				3.3V power input for chip
4	WAKE UP				wake up pin
5	por				power on reset
6	VSS				ground
7	VDD				1.1V power output
8	rstout1	aec_rb	eport3[6]	gpio	reset output /AEC busy signal /GPIO
9	isodat1				ISO7816 DATA
10	isoclk1				ISO7816 CLOCK
11	spi2[0]	mosi2	eport0[2]		QSPI DATA0 /SPI master output/slave input data /GPIO
12	VSS				ground
13	spi2[1]	miso2	eport0[3]		QSPI DATA1 /SPI master input/slave output data /GPIO
14	VDD33				3.3V power input for chip
15	ss_spi2	ss2	eport0[0]		QSPI chip select /SPI chip select /GPIO
16	sck_spi2	sck2	eport0[1]		QSPI clock /SPI clock /GPIO
17	VSS				ground

18	VSS				ground
19	VDD33				3.3V power input for chip
20	sck_spi1	sck1	eport1[1]		QSPI clock /SPI clock /GPIO
21	ss_spi1	ss1	eport1[0]		QSPI chip select /SPI chip select /GPIO
22	spi1[0]	mosi1	eport1[2]		QSPI DATA0 /SPI master output/slave input data /GPIO
23	spi1[1]	miso1	eport1[3]		QSPI DATA1 /SPI master input/slave output data /GPIO
24	VSS				ground
25	spi1[2]	sda2	eport1[4]	tio	QSPI DATA2 /I2C2 DATA /GPIO /SWD DATA
26	VDD_AEC				1.1V AEC power output
27	VDD				1.1V power output
28	VSS				ground
29	VDD				1.1V power output
30	isorst1				ISO7816 RESET
31	VSS				ground
32	VDD33				3.3V power input for chip
33	spi1[3]	scl2	eport1[5]	tclk	QSPI DATA3 /I2C2 CLOCK /GPIO /SWD CLOCK
34	spi2[2]	isodata1	eport0[4]		QSPI DATA2 /ISO7816 DATA /GPIO

35	spi2[3]	isoclk1	eport0[5]		QSPI DATA3 /ISO7816 CLOCK /GPIO
36	scl1		eport1[6]		I2C CLOCK /GPIO
37	sda1	isorst1	eport1[7]		I2C DATA /ISO7816 RESET /GPIO
38	VSS				ground
39	clkout1	gpio	eport3[7]		clock output /GPIO
40	VSS				ground