

MH1902T

芯片简介

兆讯恒达科技股份有限公司

目 录

1	芯片概述.....	1
1.1	芯片描述	1
1.2	芯片主要功能特性	1
1.3	芯片应用场合	2
1.4	芯片基本结构描述	2
2	芯片特性说明.....	3
2.1	电气特性	3
2.2	管脚定义	5
2.2.1	QFN68.....	5
2.2.2	QFN88.....	7
2.3	封装信息	10
2.3.1	QFN68.....	10
2.3.2	QFN88.....	11
2.4	料号信息	12
3	芯片功能模块详述.....	13
3.1	外设描述	13
3.1.1	SPI.....	13
3.1.2	HSPI.....	14
3.1.3	UART外设.....	15
3.1.4	SCI	15
3.1.5	USB	15
3.1.6	BPU & Sensor	16
3.1.7	GPIO.....	17
3.1.8	真随机数.....	17
3.2	CPU资源描述.....	17
3.2.1	MPU.....	17
3.2.2	NVIC.....	17

图索引

图 1-1 系统主要模块3

图 2-1 MH1902T QFN68 8MM*8MM封装尺寸10

图 2-2 MH1902T QFN88 10MM*10MM封装尺寸11

图 3-1 SPI时序 1(CPHA=0)14

图 3-2 SPI时序 2(CPHA=1)14

表索引

表 2-1 极限参数.....3

表 2-2 电气特性.....4

表 2-3 安全相关特性4

表 2-4 功耗列表.....4

表 2-5 充电模块相关参数.....5

表 2-6 MH1902T QFN68 8MM×8MM封装引脚定义.....5

表 2-7 MH1902T QFN88 10MM×10MM封装引脚定义.....7

表 7 MH1902T 料号信息12

1 芯片概述

1.1 芯片描述

MH1902T 芯片使用 SC300 安全核处理器。充分利用其卓越的架构特性、高性能和超低的成本，在提供高性能的同时，还提供安全、节能的解决方案。

芯片内置硬件安全加密模块，支持多种加密安全算法，包括 DES、TDES、AES、RSA、ECC、SHA 等主流加密算法。芯片硬件还支持多种攻击检测功能，符合金融安全设备标准。

芯片内部包含安全 BOOT 程序，支持下载、启动时对固件签名校验。芯片集成了丰富的外设资源，所有外设驱动软件兼容目前主流安全芯片软件接口并符合 ARM CMSIS 规范，用户可在现有方案基础上进行快速开发和移植。

采用先进的制造工艺，使本款芯片可以提供更高的主频和更低的功耗。

1.2 芯片主要功能特性

- ARM SecurCore™ SC300™核心
 - 32-bit RISC Core (ARMv7-M)
 - MPU 内存保护单元
 - 144/120/108/72/60/54MHz 主频 (1、2、4 分频可调)
 - 1 个受控 JTAG-DP 调试端口
- 128KB/64KB 随机加扰 SRAM
- 系统控制模块 (控制所有外设模块时钟及系统相关配置)
- 安全加密算法加速引擎
 - 对称算法: DES、TDES、AES-128/192/256
 - 非对称算法: RSA-1024/2048、ECC
 - HASH 校验算法: SHA-1/224/256/384/512
- 1 个 SmartCard 接口 (支持 EMV Level-1 规范、ISO7816-3 标准)，集成 7816 电平转换功能，可通过寄存器配置输出 3V 和 1.8V
- 3 个 UART 接口 (均支持 4 线)
- 3 个 SPI 接口 (1 个主从可配，2 个仅主)
- 1 个高速 SPI 接口 SPI3(主/从可配)
- 1 个 I2C 接口
- 6 个 32 位 TIMER(带有 PWM 功能)
- 1 个真随机数发生器
- 1 个 DMA 控制器 (支持 4 通道 DMA 传输)
- 1 个 CRC 模块 (支持 16Bit/32Bit、多种常用多项式计算)

- 最多支持 8 个静态 Tamper 或 4 组动态 Tamper(2 输出, 2 输入), 动/静态可配
- 1 组内部 Sensor (支持高低电压、高低温、Mesh、时钟和 voltage glitch 等传感器)
- 1 块密钥存储区 (支持硬件快速擦除)
- 1 个 USB (OTG-FS)
 - 支持 USB2.0 和 OTG1.0a
 - 内置 USB PHY 模块
 - 专用 DMA 通道和专有的中断向量, 加快数据通信速度
- 集成内部看门狗
- 1 个支持最高 1MHz 采样率的 7 通道 10bit ADC, 通道 0 采集电压范围是 0~5V(内部分压 1.7M/425K), 通道 6 内部固定采集 CHARGE_VBAT 管脚电压; 其余通道采集电压范围 0~1.2V
- 1 个 10bit DAC 接口
- 芯片集成磁条卡解码模块, 支持 ISO/ABA、AAMVA、IBM 和 JIS II 等标准卡
- 芯片集成 USB 充电管理模块, 支持最大 200mA 充电电流
- 芯片集成开关机功能
- 支持输出 27.12M

1.3 芯片应用场合

金融安全设备、移动安全设备及其他对功耗和成本敏感的安全设备。

1.4 芯片基本结构描述

芯片包括安全核、128KB/64KB SRAM、系统控制模块、安全加密模块、真随机数模块、1 个 QSPI 控制器、1 个 4 通道 DMA 控制器、1 个 USB 接口、1 个 GPIO 模块、1 个 WDT 模块、1 个 BPU 模块、6 个 32bit Timer、3 个 SPI 接口、1 个高速 SPI 接口、1 个 I2C 接口、1 个 CRC 模块、1 个 SCI 接口、3 个 UART 接口、1 个 7 通道 ADC、1 个 DAC、1 个 TRNG 模块, 系统框图如下:

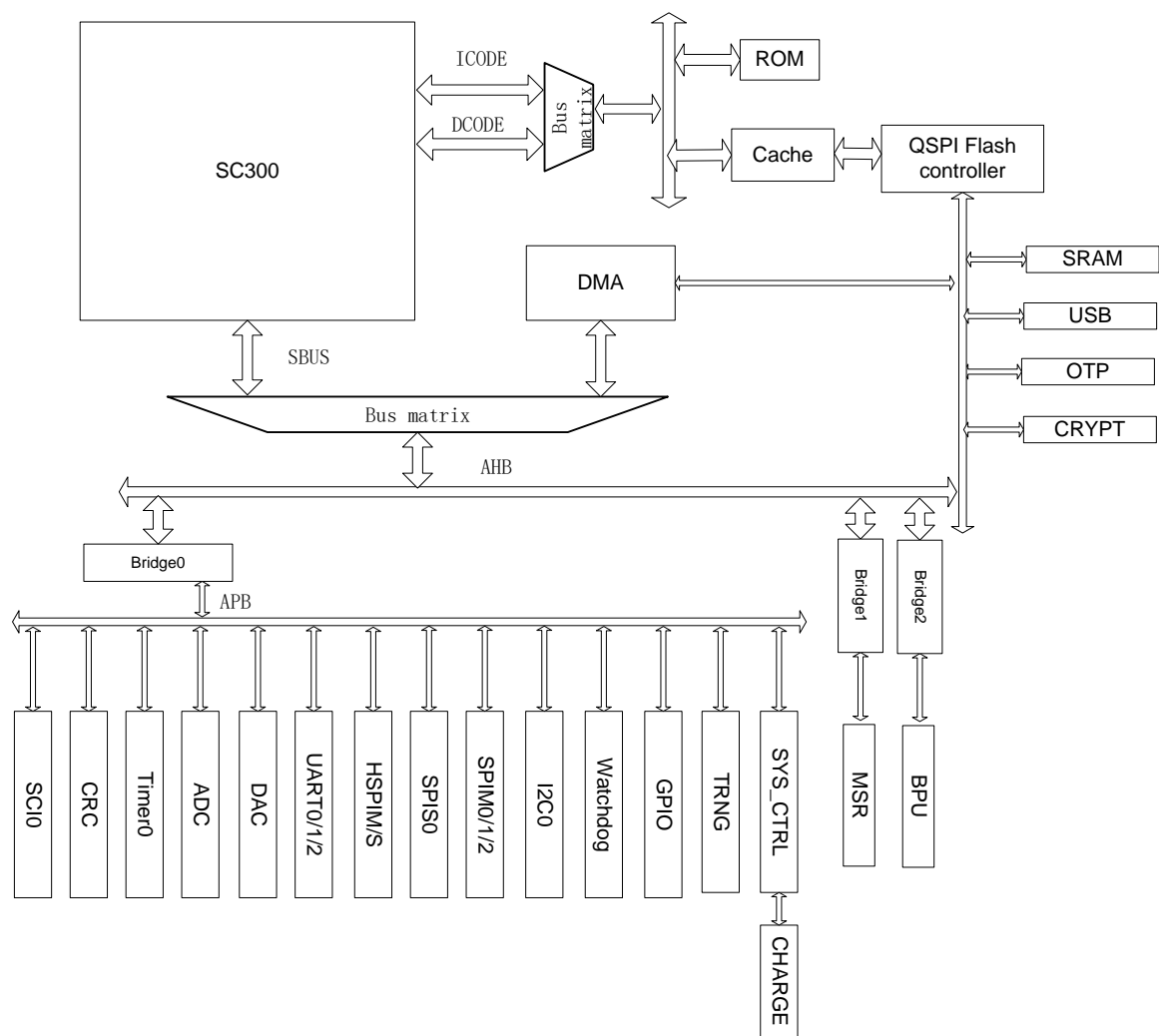


图 1-1 系统主要模块

2 芯片特性说明

2.1 电气特性

表 2-1 极限参数

参数	说明	范围	单位
VDD	稳态电源电压	-0.3 to 3.6	V
Iddpd	关机电流	--	nA
Tamb	工作温度	-40~+80	°C
Tstg	储藏温度	-40~+125	°C
Ground	地	-0.3~0.3	V
Voh	数字输出高电平	VDD -0.3 ~ VDD+0.3	V
Vol	数字输出低电平	<0.4	V

参数	说明	范围	单位
Ioh	拉电流	20	mA
Iol	灌电流	20	mA
Vih	数字输入高电平	$\geq 0.7 \times VDD$	V
ViL	数字输入低电平	$\leq 0.3 \times VDD$	V

表 2-2 电气特性

参数	条件 (-40°C to +85°C)	值		单位
		最小	最大	
AVD33		2.7	3.6	V
VDD33		2.7	3.6	V
VBAT33		1.9	3.6	V
CHARGE_VCC		4.6	5.5	V
Vol	VDD=3.3V	-	0.4	V
Voh	VDD=3.3V	VDD - 0.3	-	V
VIH	VDD=3.3V	$0.7 \times VDD$	-	V
VIL	VDD=3.3V	-	$0.3 \times VDD$	V

表 2-3 安全相关特性

传感器	说明	范围	单位
温度传感器	高温检测范围	90~120	°C
	低温检测范围	-30 ~ -50	°C
电压传感器	主电源电压高压检测范围	4.2 ± 0.1	V
	主电源电压低压检测范围	2.7~2.9	V
	电池电压高压检测范围	4.2 ± 0.1	V
	电池电压低压检测范围	2.1 ± 0.1	V
时钟频率传感器	12M 时钟频率检测范围	$12 \pm 50\%$	MHz
	32K 时钟频率检测范围	$32 \pm 50\%$	KHz
Tamper 拉电阻	Tamper 管脚上的拉电阻阻值	$3.8M \pm 10\%$	Ω

表 2-4 功耗列表

工作模式	说明	功耗	单位
RUN	<ul style="list-style-type: none"> ● 所有外设全开 ■ @144MHz 	42	mA
	<ul style="list-style-type: none"> ● 所有外设全关 ■ @144MHz 	22	
CPU Sleep	所有外设全关 @144MHz	7.2	mA
DeepSleep	● 支持 IO 低电平、RTC、攻击、充电和刷卡唤醒	200	uA
PowerDown	● 支持 IO 低电平、RTC、攻击、充电和刷卡唤醒	20	uA

VBAT	测试时所有 Tamper 管脚悬空，内部拉电阻使能 ■ 内部传感器全开 ■ 内部传感器全关	1.8	uA
		1.6	

表 2-5 充电模块相关参数

编程电阻值	涓流充电电流(mA)	涓流阈值(V)	恒流充电电流(mA)	充电电压(V)
1K	20±1	2.87±0.01	193±5	4.15±0.05
2K	10±1	2.88±0.01	96±2	4.15±0.05
4.02K	5±1	2.90±0.01	46.5±1.5	4.15±0.05

2.2 管脚定义

2.2.1 QFN68

表 2-6 MH1902T QFN68 8mm×8mm 封装引脚定义

PIN No.	PIN name	ALT0	ALT1 (default)	ALT2	ALT3	备注
1	PA4		PA[4]	PWM4	XTAL32K	
2	PA5		PA[5]	PWM5	27.12M	可配置输出 27.12M
3	PA8	SCI0_CLK	PA[8]			复用为 IO 时必须先打开 IC 卡电源, 且输出信号的高电平为 IC 卡输出电平
4	PA9	SCI0_RSTN	PA[9]			
5	PA10	SCI0_IO	PA[10]			
6	CVCC					IC 卡电源
7	VDD33					
8	POWER_KEY					开关机按键
9	EN_LDO5V					外部 LDO 使能
10	VSS					芯片地
11	PA6	SCI0_DET	PA[6]			
12	PA13		PA[13]	CLK_27P12	UART0_RTS	可配置输出 27.12M
13	PA15		PA[15]	UART2_TX	UART0_TX	
14	PA0	UART0_RX/IrDA_IN	PA[0]	PWM0		
15	PA1	UART0_TX/IrDA_OUT	PA[1]	PWM1		
16	PA2	UART0_CTS	PA[2]	PWM2		
17	PA3	UART0_RTS	PA[3]	PWM3		
18	PB0	I2C0_SCL	PB[0]	PWM0	XTAL32K	
19	PB1	I2C0_SDA	PB[1]	PWM1	CLK_27P12	
20	PD4	UART1_RX/IrDA_IN	PD[4]			
21	PD5	UART1_TX/IrDA_OUT	PD[5]			
22	PB2	SPI0_SCK	PB[2]	PWM2	SPI3_CLK	
23	PB3	SPI0_CSN0	PB[3]	PWM3	SPI3_CSN0	
24	PB4	SPI0_MOSI	PB[4]	PWM4	SPI3_MOSI	
25	PB5	SPI0_MISO	PB[5]	PWM5	SPI3_MISO	
26	VDD33					IO 电源

27	PB12	SPI2_CLK	PB[12]	SPI3_CLK	UART1_RX/I rDA_IN	
28	PB13	SPI2_CSN	PB[13]	SPI3_CSN0	UART1_TX/I rDA_OUT	
29	PB14	SPI2_MOSI	PB[14]	SPI3_MOSI	UART1_CTS	
30	PB15	SPI2_MISO	PB[15]	SPI3_MISO	UART1_RTS	
31	VDD12					外接 1uF 滤波电容
32	RST_N					
33	PC9	UART2_CTS	PC[9]		SPI1_MOSI	
34	PC10	UART2_RX/Ir DA_IN	PC[10]		SPI1_CLK	
35	PC15	SPI1_MISO	PC[15]	SPI3_MISO	UART2_TX/I rDA_OUT	
36	PC14	SPI1_MOSI	PC[14]	SPI3_MOSI	UART2_RTS	
37	PC13	SPI1_CLK	PC[13]	SPI3_CLK	UART2_RX/I rDA_IN	
38	PC12	SPI1_CSN	PC[12]	SPI3_CSN	UART2_CTS	
39	CHARGE_VPR OG					CHARGE 充电电流 控制管脚
40	CHARGE_VCC					CHARGE 电源输入
41	CHARGE_VBA T					CHARGE 电源输出， 接电池
42	MSR_IN1	UART1_CTS	PD[6]	MSR_IN1	I2C0_SCL	磁条卡 T1+
43	MSR_IN2	UART1_RTS	PD[7]	MSR_IN2	I2C0_SDA	磁条卡 T1-
44	MSR_IN3	SPI1_SCK	PD[8]	MSR_IN3		磁条卡 T2+
45	MSR_IN4	SPI1_CSN	PD[9]	MSR_IN4		磁条卡 T2-
46	MSR_IN5	SPI1_MOSI	PD[10]	MSR_IN5		磁条卡 T3+
47	MSR_IN6	SPI1_MISO	PD[11]	MSR_IN6		磁条卡 T3-
48	PC5		PC[5]	ADC_IN5		
49	PC4	TCK	PC[4]	ADC_IN4		
50	PC3	TMS	PC[3]	ADC_IN3	UART1_RTS	
51	PC2	TDO	PC[2]	ADC_IN2	UART1_CTS	
52	PC1	TDI	PC[1]	ADC_IN1/D AC	UART1_TX/I rDA_OUT	
53	PC0	TRST	PC[0]	ADC_IN0	UART1_RX/I rDA_IN	
54	DN					USB DN
55	DP					USB DP
56	VBUS					USB VBUS
57	ID					USB ID
58	XI12M					XTAL 12MHz Input
59	XO12M					XTAL 12MHz Output
60	VDD33					IO 电源
61	AVD33					模拟电源
62	XO32					XTAL 32KHz Output
63	XI32					XTAL 32KHz Input
64	EXTS3					外部 Tamper3
65	EXTS1					外部 Tamper1
66	EXTS2					外部 Tamper2
67	EXTS0					外部 Tamper0
68	VBAT33					电池供电电源

2.2.2 QFN88

表 2-7 MH1902T QFN88 10mm×10mm 封装引脚定义

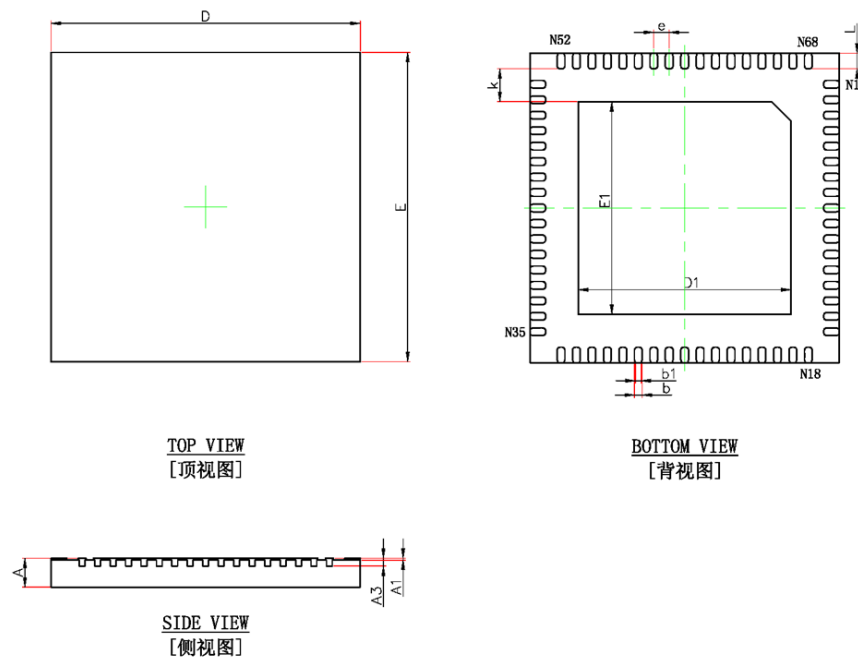
PIN No.	PIN name	ALT0	ALT1 (default)	ALT2	ALT3	备注
1	PA4		PA[4]	PWM4	XTAL32K	
2	PA5		PA[5]	PWM5	CLK_27P12	可配置输出 27.12M
3	PA8	SCI0_CLK	PA[8]			复用为 IO 时必须先打开 IC 卡电源，且输出信号的高电平为 IC 卡输出电平
4	PA9	SCI0_RSTN	PA[9]			
5	PA10	SCI0_IO	PA[10]			
6	CVCC					IC 卡电源
7	VDD33					
8	POWER_KEY					开关机按键
9	EN_LDO5V					外部 LDO 使能
10	VSS					芯片地
11	PA6	SCI0_DET	PA[6]			
12	PA7		PA[7]	CLK_27P12		可配置输出 27.12M
13	PA11		PA[11]			
14	PA12		PA[12]		UART0_CTS	
15	PA13		PA[13]	CLK_27P12	UART0_RTS	可配置输出 27.12M
16	PA14	SCI0_VCCEN	PA[14]	UART2_RX	UART0_RX	
17	PA15		PA[15]	UART2_TX	UART0_TX	
18	PA0	UART0_RX/IrD A_IN	PA[0]	PWM0		串口下载管脚
19	PA1	UART0_TX/IrDA_OUT	PA[1]	PWM1		
20	PA2	UART0_CTS	PA[2]	PWM2		
21	PA3	UART0_RTS	PA[3]	PWM3		
22	PB0	I2C0_SCL	PB[0]	PWM0	XTAL32K	
23	PB1	I2C0_SDA	PB[1]	PWM1	CLK_27P12	
24	PD4	UART1_RX/IrD A_IN	PD[4]			
25	PD5	UART1_TX/IrDA_OUT	PD[5]			
26	PB2	SPI0_SCK	PB[2]	PWM2	SPI3_CLK	
27	PB3	SPI0_CSN0	PB[3]	PWM3	SPI3_CSN0	
28	PB4	SPI0_MOSI	PB[4]	PWM4	SPI3_MOSI	
29	PB5	SPI0_MISO	PB[5]	PWM5	SPI3_MISO	
30	IO_VCC					PB2~PB5 电源输入
31	PB12	SPI2_CLK	PB[12]	SPI3_CLK	UART1_RX/IrDA_IN	
32	PB13	SPI2_CSN	PB[13]	SPI3_CSN0	UART1_TX/IrDA_OUT	
33	PB14	SPI2_MOSI	PB[14]	SPI3_MOSI	UART1_CTS	
34	PB15	SPI2_MISO	PB[15]	SPI3_MISO	UART1_RTS	

35	PB10		PB[10]			
36	PB11		PB[11]			
37	PC6		PC[6]		CLK_27P12	
38	PC7		PC[7]			
39	PC8	UART2_TX/IrDA_OUT	PC[8]		SPI1_MISO	
40	VDD12					外接 1uF 滤波电容
41	RST_N					
42	PC9	UART2_CTS	PC[9]		SPI1_MOSI	
43	PC10	UART2_RX/IrDA_A_IN	PC[10]		SPI1_SCK	
44	PB6	SPI1_SCK	PB[6]	SPI3_SCK		
45	PB7	SPI1_CSN0	PB[7]	SPI3_CSN0		
46	PB8	SPI1_MOSI	PB[8]	SPI3_MOSI		
47	PB9	SPI1_MISO	PB[9]	SPI3_MISO		
48	PC15	SPI1_MISO	PC[15]	SPI3_MISO	UART2_TX/IrDA_OUT	
49	PC14	SPI1_MOSI	PC[14]	SPI3_MOSI	UART2_RTS	
50	PC13	SPI1_CLK	PC[13]	SPI3_CLK	UART2_RX/IrDA_IN	
51	PC12	SPI1_CSN	PC[12]	SPI3_CSN	UART2_CTS	
52	PC11	UART2_RTS	PC[11]		SPI1_CSN0	
53	CHARGE_VPROG					CHARGE 充电电流控制管脚
54	CHARGE_VCC					CHARGE 电源输入
55	CHARGE_VBAT					CHARGE 电源输出，接电池
56	PD6	UART1_CTS	PD[6]	MSR_IN1	I2C0_SCL	磁条卡 T1+
57	PD7	UART1_RTS	PD[7]	MSR_IN2	I2C0_SDA	磁条卡 T1-
58	PD8	SPI1_SCK	PD[8]	MSR_IN3		磁条卡 T2+
59	PD9	SPI1_CSN	PD[9]	MSR_IN4		磁条卡 T2-
60	PD10	SPI1_MOSI	PD[10]	MSR_IN5		磁条卡 T3+
61	PD11	SPI1_MISO	PD[11]	MSR_IN6		磁条卡 T3-
62	PC5		PC[5]	ADC_IN5		
63	PC4	TCK	PC[4]	ADC_IN4		
64	PC3	TMS	PC[3]	ADC_IN3	UART1_RTS	
65	PC2	TDO	PC[2]	ADC_IN2	UART1_CTS	
66	PC1	TDI	PC[1]	ADC_IN1/DAC	UART1_TX/IrDA_OUT	
67	PC0	TRST	PC[0]	ADC_IN0	UART1_RX/IrDA_IN	
68	VDD33					IO 电源
69	PD0	DRV_VBUS	PD[0]			
70	VSS					芯片地
71	DN					USB DN
72	DP					USB DP
73	VBUS					USB VBUS

74	ID					USB ID
75	XI12M					XTAL 12MHz Input
76	XO12M					XTAL12MHz Output
77	VDD33					
78	EXTS7					外部 Tamper7
79	EXTS5					外部 Tamper5
80	XO32					XTAL 32KHz Output
81	XI32					XTAL 32KHz Input
82	EXTS6					外部 Tamper6
83	EXTS4					外部 Tamper4
84	EXTS3					外部 Tamper3
85	EXTS1					外部 Tamper1
86	EXTS2					外部 Tamper2
87	EXTS0					外部 Tamper0
88	VBAT33					电池供电电源

2.3 封装信息

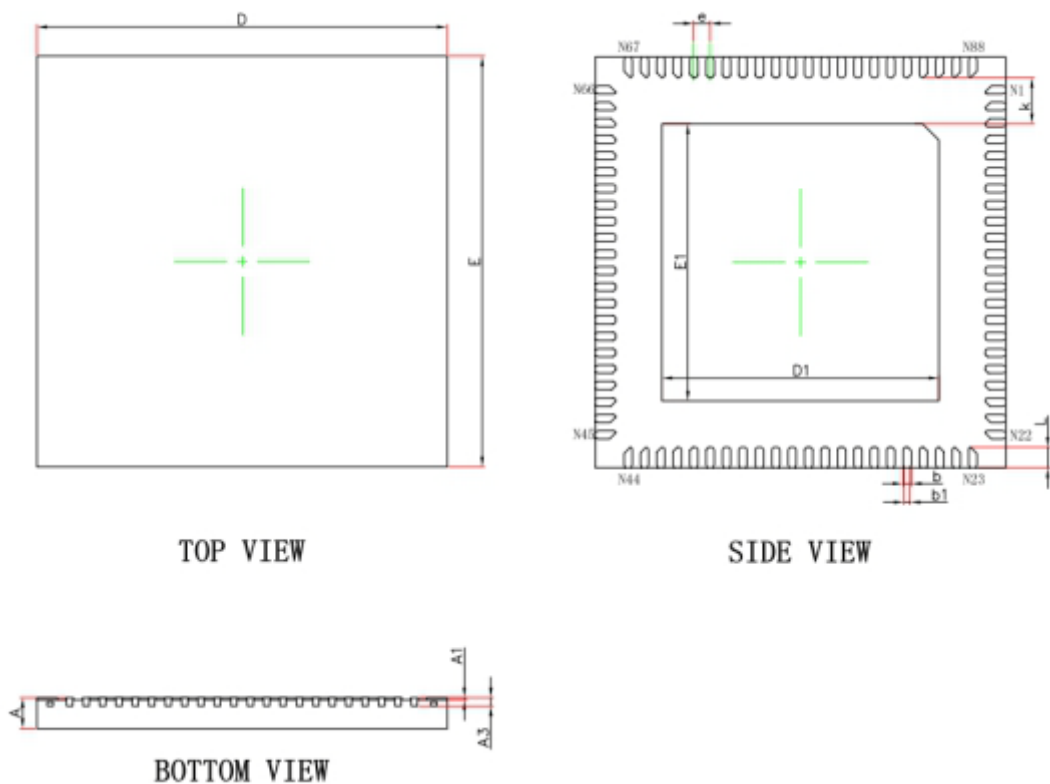
2.3.1 QFN68



Symbol	Dimensions In Millimeters		Dimensions In Inches	
	Min.	Max.	Min.	Max.
A	0.700	0.800	0.028	0.031
A1	0.000	0.050	0.000	0.002
A3	0.203REF.		0.008REF.	
D	7.900	8.100	0.311	0.319
E	7.900	8.100	0.311	0.319
D1	5.400	5.600	0.213	0.220
E1	5.400	5.600	0.213	0.220
k	0.200MIN.		0.008MIN.	
b	0.150	0.250	0.006	0.010
b1	0.100	0.200	0.004	0.008
e	0.400TYP.		0.016TYP.	
L	0.324	0.476	0.013	0.019

图 2-1 MH1902T QFN68 8mm*8mm 封装尺寸

2.3.2 QFN88



Symbol	Dimensions In Millimeters		Dimensions In Inches	
	MIN.	MAX.	MIN.	MAX.
A	0.700	0.800	0.028	0.031
A1	0.000	0.050	0.000	0.002
A3	0.203REF.		0.008REF.	
D	9.900	10.100	0.390	0.398
E	9.900	10.100	0.390	0.398
D1	6.650	6.850	0.262	0.270
E1	6.650	6.850	0.262	0.270
k	1.125REF.		0.044REF.	
b	0.150	0.250	0.006	0.010
b1	0.150REF.		0.006REF.	
e	0.400BSC.		0.016BSC.	
L	0.400	0.600	0.016	0.024

图 2-2 MH1902T QFN88 10mm*10mm 封装尺寸

注释:

- A. 所有线性尺寸单位均为毫米;
- B. 该图若有变化, 恕不另行通知。

2.4 料号信息

表 8 MH1902T 料号信息

参数 料号	SRAM	Flash	扫码算法	管脚定义
MH1902TQ66FH00	64KB	512KB	无	QFN68
MH1902TQ67MH0S	128KB	1MB	通用版	QFN68
MH1902TQ67NH0S	128KB	4MB	通用版	QFN68
MH1902TQ87MH0S	128KB	1MB	通用版	QFN88
MH1902TQ87NH0S	128KB	4MB	通用版	QFN88

3 芯片功能模块详述

3.1 外设描述

3.1.1 SPI

芯片提供 1 个 SPI 主从，2 个 SPI 主设备接口，作为主设备接口时可以支持与多个从设备通信。

SPI 外设特性：

- Master 模式与 Slave 模式独立地址操作
- Master 模式支持全双工、单工收、单工发、EEPROM 模式
- 多个 Master 冲突探测
- 支持 Motorola SPI、Texas Instruments SPI、National Semiconductor Microwire 三种通讯模式
- 独立的接收和发送 FIFO，接收和发送 FIFO 深度均为 16，宽度固定为 16bits
- 帧长度可配，范围 4-16bits
- DMA 接口

常用 Motorola SPI 通讯协议支持的四种通讯模式，能够实现全双工通讯。系统上电默认采用模式 0 工作方式。

SPI 协议规定的 4 中通讯格式说明如下：

- 模式0：时钟极性（CPOL）=0，时钟相位（CPHA）=0，该模式下串行同步时钟的空闲状态为低电平，芯片将在串行同步时钟的第一个跳变沿（上升沿）采样，芯片默认为该模式；
- 模式1：时钟极性（CPOL）=0，时钟相位（CPHA）=1，该模式下串行同步时钟的空闲状态为低电平，芯片将在串行同步时钟的第二个跳变沿（下降沿）采样；
- 模式2：时钟极性（CPOL）=1，时钟相位（CPHA）=0，该模式下串行同步时钟的空闲状态为高电平，芯片将在串行同步时钟的第一个跳变沿（下降沿）采样；
- 模式3：时钟极性（CPOL）=1，时钟相位（CPHA）=1，该模式下串行同步时钟的空闲状态为高电平，芯片将在串行同步时钟的第二个跳变沿（上升沿）采样。

注意：为保证芯片 SPI 正常工作，在进行模式切换时保证 CSN 信号线保持为高电平。同时在通讯过程中主机认为从机发生错误时，均可以通过将 CSN 拉高使从机恢复正常。

SPI 接口说明如下：

- SCK：SPI 的时钟输入管脚，当采用 200K 的通信速率时，字节之间需要有至少 20us 的延时；

- CSN: SPI的片选信号，为芯片的输入管脚，低有效；
- MOSI: SPI的数据输入管脚；
- MISO: SPI的数据输出管脚。

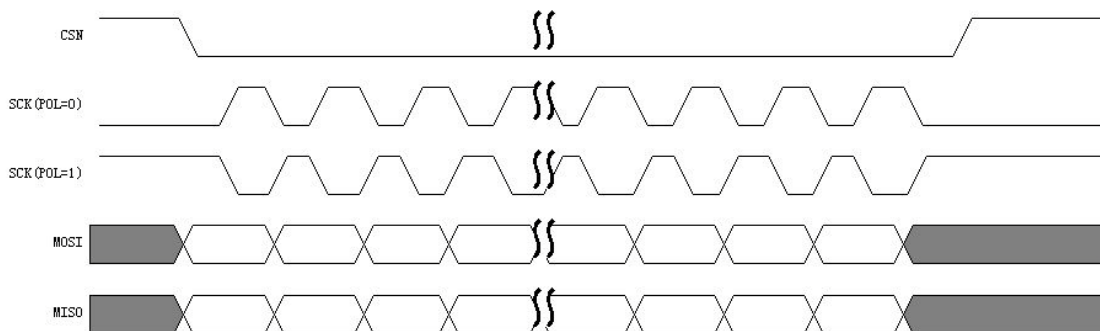


图 3-1 SPI 时序 1(CPHA=0)

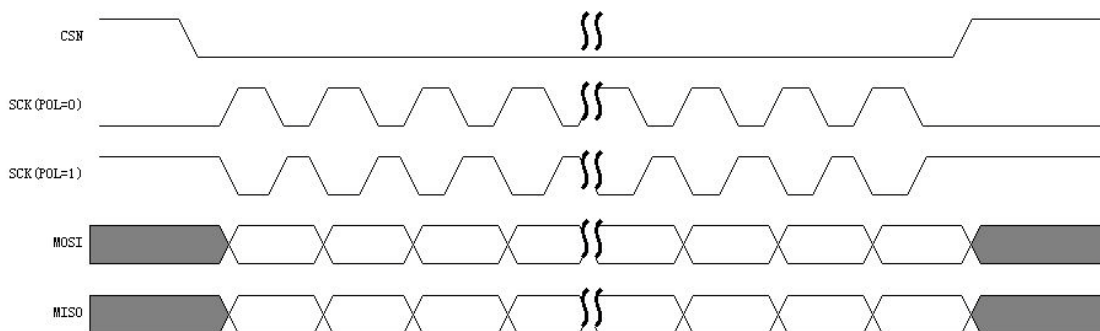


图 3-2 SPI 时序 2(CPHA=1)

3.1.2 HSPI

芯片提供 1 个高速 SPI 主从接口，作为主设备接口时可以支持与多个从设备通信。

SPI 外设特性：

- Master 模式与 Slave 模式独立地址操作
- Master 模式支持全双工模式
- 独立硬件收发 FIFO，可配收发 FIFO 中断阈值
- 接收和发送 FIFO 深度均为 64
- DMA 接口

常用 Motorola SPI 通讯协议支持的四种通讯模式，能够实现全双工通讯。系统上电默认采用模式 0 工作方式。

3.1.3 UART外设

芯片带有 3 个全双工的 UART 串行通信接口，均支持 4 线模式

UART 外设特性：

- 独立接收发送 FIFO，接收发送 FIFO 深度均为 16 字节
- FIFO 使能控制
- 数据位设定，支持 5-8bit
- 强制 9bit 校验位输出
- 帧错误、校验错误、break 中断探测
- IrDA 1.0 红外协议支持
- DMA 接收

UART 外设支持独立的接收发送 FIFO，FIFO 功能可通过使能位配置其是否使用。

UART 接收和发送 FIFO 分别支持接收 FIFO 满和发送 FIFO 空中断，其触发值可配。发送 FIFO 中断源与非 FIFO 模式中发送保持寄存器空（THRE）共用同一中断源，通过软件进行设定。

3.1.4 SCI

芯片包含 1 个智能卡接口（Smart Card Interface），该接口支持 ISO7816-3 标准和 EMV Level-1 规范。

- 支持异步 T=0 和 T=1 传输协议
- 协议时序、时间参数可配
- 8 字符深度接收、发送缓冲
- 接收、发送 FIFO 监测中断
- 中断状态寄存器
- 检测卡移除时，自动触发硬件去激活时序
- 可软件配置的去激活时序
- 对同步卡的有限支持（通过寄存器控制输入、输出）

SCI 模块对外提供的时钟 $F = PCLK/2(SCICKICC + 1)$ ，SCICKICC 位宽为 8bit，范围 0 到 255。

3.1.5 USB

OTG_FS 控制器接口，符合 USB 2.0 标准和 OTG 1.0a 规范

- 支持 USB2.0

- 支持 OTG1.0a
 - 对插入的 A-B 类设备的辨认(ID)
 - 支持主机协商协议(HNP)和会话请求协议(SRP)
 - 在 OTG 应用中, 允许主机关闭 VBUS 以节省耗电
- 支持 SRP 协议的 USB 全速/低速设备(B 类设备)
 - 支持 SRP 协议的 USB 全速/低速设备(A 类设备)
 - USB OTG 全速/低速双重角色设备
- 提供 512 字节的专用 RAM 和高级的 FIFO 管理
 - 通过软件为不同的 FIFO 配置不同的 RAM 区域, 以便灵活有效的使用 RAM
 - 每个 FIFO 可以存储多个数据包
 - 允许动态的分配存储区
 - 不限定 FIFO 的长度 (不强制 2 的幂次长度, 可以连续的使用存储区)
 - 允许相同端点号 (IN/OUT 端点共用同一个 FIFO, 更加有效的使用存储区)
- 无需要系统的介入就可以保证一个帧(1ms)的最大数据流量
- 拥有一个专用的 DMA 通道和专有的中断向量, 可以加快数据通信速度
- 主机模式
 - 支持最多 4 个主机通道, 每个通道都可以动态的配置为任意一种传输类型
 - 在周期性硬件传输请求队列中支持多达 4 个中断和同步传输请求
 - 在非周期行硬件传输请求队列中支持多达 4 个控制和大容量传输的传输请求

3.1.6 BPU & Sensor

芯片内置 BPU 模块提供 BPK 单元、Sensor 单元及 RTC 单元。

BPK 密钥寄存器, 可以由电池电源域供电, 外部电源掉电不丢失。当 Sensor 单元探测到攻击时清除 BPK 寄存器。

Sensor 特性:

- 可编程外部攻击, 支持外部静态和外部动态两种模式, 外部静态最多可编程 8 个检测源, 外部动态最多可编程 4 对检测源。
- 内部攻击检测包括 32K 时钟频率检测、高低温攻击检测、高低电压攻击检测。
- Active shelding。
- 电池电压毛刺 (glitch) 检测。

3.1.7 GPIO

每个IO都与外设复用管脚。每个GPIO均可配置为输入、输出、中断模式，当做为输出时，每个IO输出值都可单独配置。IO支持强推挽输出/开漏输出模式。

3.1.8 真随机数

芯片内置真随机数发生器，用户一次可最多取 128bit 的真随机数。

3.2 CPU资源描述

3.2.1 MPU

详情请参考 ARMv7 Protected Memory System Architecture 文档。

3.2.2 NVIC

详情请参考 Cortex-M3 NVIC 控制器。