目　录

图索引

表索引

1 芯片概述

1.1 芯片描述

ID812 芯片使用 ARM 32-bit 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、SHA、ECC 等主流加密算法，芯片硬件还支持多种攻击检测功能。

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 32-bit 安全核
  - 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 随机加扰 SRAM
- 1MB Flash
- 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
- 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 个 USB（OTG-FS）
  - 支持 USB2.0 和 OTG1.0a
  - 内置 USB PHY 模块
- 芯片集成内部看门狗
- 1 个支持 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)，其余通道采集电压范围 0~1.2V
- 芯片集成 USB 充电管理模块，支持高达 200mA 的充电电流
- 芯片集成开关机功能

1.3 芯片应用场合

物联网安全设备、指纹模块

1.4 芯片基本结构描述

芯片包括安全核、128KB SRAM、系统控制模块、安全加密模块、真随机数模块、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、1 个 I2C 接口，3 个 SPI 接口、1 个高速 SPI 接口、1 个 CRC 模块、3 个 UART 接口、1 个 7 通道 ADC，1 个 TRNG 模块，系统框图如下：

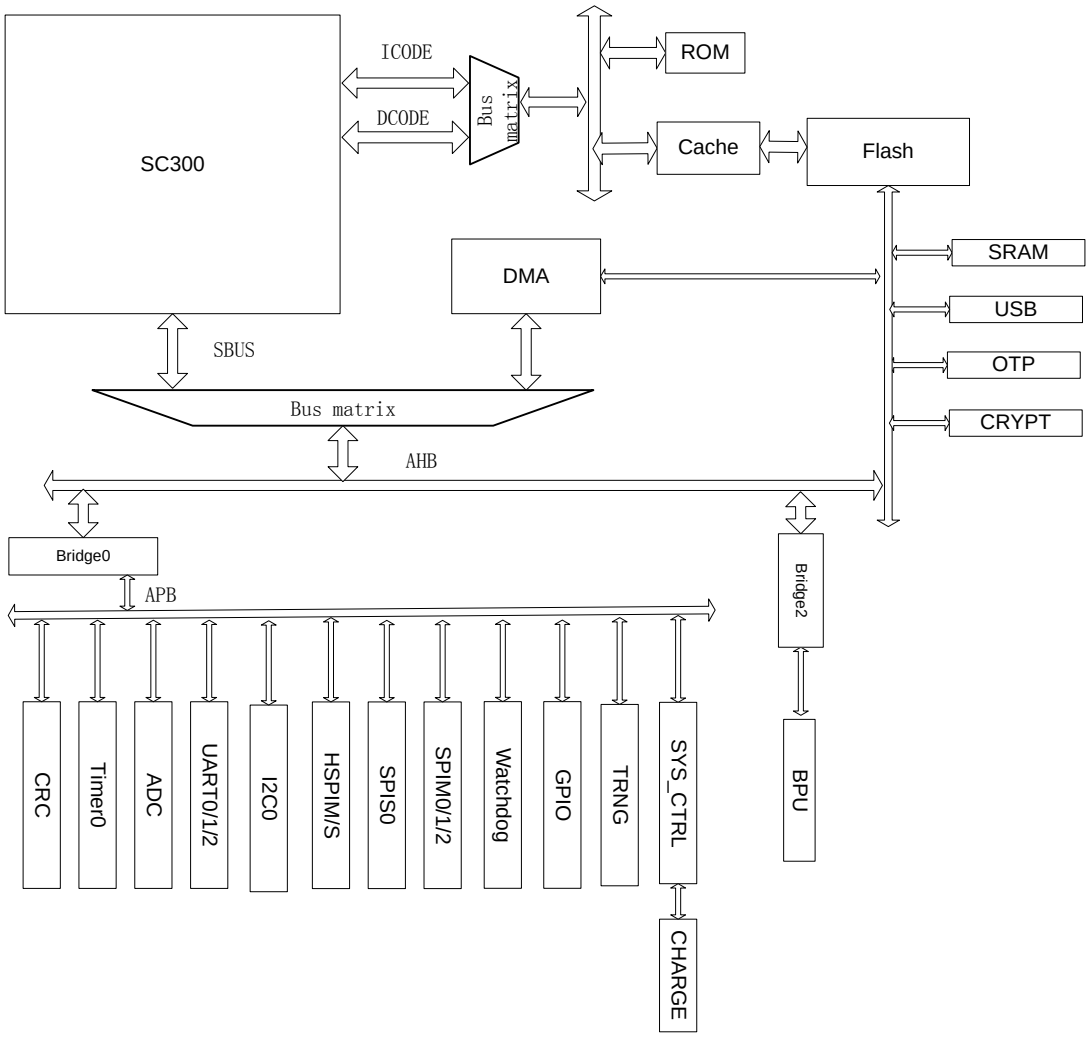


图 1-1 系统主要模块

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	℃
Tstg	储藏温度	-40~+125	℃
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	≥0.7×VDD	V
ViL	数字输入低电平	≤0.3×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
Vol	VDD=3.3V	-	0.4	V
Voh	VDD=3.3V	VDD – 0.3	-	V
VIH	VDD=3.3V	0.7×VDD	-	V
VIL	VDD=3.3V	-	0.3×VDD	V

表 2-3 功耗列表

工作模式	说明	功耗	单位
RUN	● 所有外设全开 ■ @144MHz ● 所有外设全关 ■ @144MHz	42 22	mA
CPU Sleep	所有外设全关 @144MHz	7.2	mA
Deep Sleep	● 支持 IO 低电平、RTC、攻击、充电和刷卡唤醒	120	uA

表 2-4 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 QFN32

表 2-5 ID812 QFN32 5mm×5mm 封装引脚定义

PIN No.	PIN name	ALT0	ALT1 (default)	ALT2	ALT3	备注
1	VDD33					

2	PA13		PA[13]	CLK_27P12	UART0_RTS	可配置输出 27.12M
3	PA14		PA[14]	UART2_RX	UART0_RX	
4	PA15		PA[15]	UART2_TX	UART0_TX	
5	PA0	UART0_RX/IrDA_IN	PA[0]	PWM0		
6	PA1	UART0_TX/IrDA_OUT	PA[1]	PWM1		
7	PA2	UART0_CTS	PA[2]	PWM2		
8	PA3	UART0_RTS	PA[3]	PWM3		
9	PB0	I2C0_SCL	PB[0]	PWM0	XTAL32K	
10	PB1	I2C0_SDA	PB[1]	PWM1	CLK_27P12	
11	PB2	SPI0_SCK	PB[2]	PWM2	SPI3_CLK	
12	PB3	SPI0_CSN0	PB[3]	PWM3	SPI3_CSN0	
13	PB4	SPI0_MOSI	PB[4]	PWM4	SPI3_MOSI	
14	PB5	SPI0_MISO	PB[5]	PWM5	SPI3_MISO	
15	VDD33					
16	VDD12					
17	PB6	SPI1_SCK	PB[6]	SPI3_SCK		
18	PB8	SPI1_MOSI	PB[8]	SPI3_MOSI		
19	PB9	SPI1_MISO	PB[9]	SPI3_MISO		
20	CHARGE_VCC					可以外电插入检测中断
21	PC4	TCK	PC[4]	ADC_IN4		
22	PC3	TMS	PC[3]	ADC_IN3	UART1_RTS	
23	PC1	TDI	PC[1]	ADC_IN1/DAC	UART1_TX/IrDA_OUT	
24	PC0	TRST	PC[0]	ADC_IN0	UART1_RX/IrDA_IN	
25	DN					USB DN
26	DP					USB DP
27	VBUS					USB VBUS
28	XI12M					XTAL 12MHz Input
29	XO12M					XTAL12MHz Output
30	VDD33					
31	PA4		PA[4]	PWM4	XTAL32K	
32	PA5		PA[5]	PWM5	27.12M	可配置输出 27.12M

2.2.2 QFN48

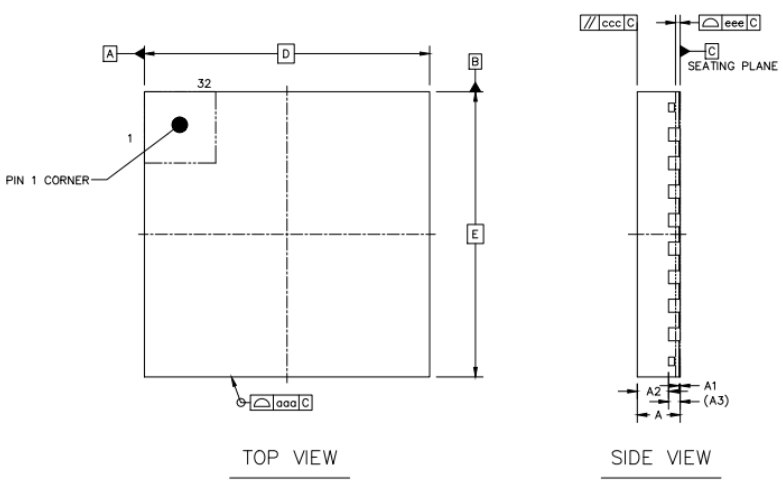
表 2-6 ID812 QFN48 6mm×6mm 封装引脚定义

PIN No.	PIN name	ALT0	ALT1 (default)	ALT2	ALT3	备注
1	VBAT33					电池供电电源
2	VDD33					
3	POWER_KEY					开关机按键
4	EN_LDO5V					外部 LDO 使能
5	PA12		PA[12]		UART0_CTS	
6	PA13		PA[13]	CLK_27P12	UART0_RTS	可配置输出 27.12M
7	PA0	UART0_RX/IrDA_IN	PA[0]	PWM0		
8	PA1	UART0_TX/IrDA_OUT	PA[1]	PWM1		
9	PA2	UART0_CTS	PA[2]	PWM2		
10	PA3	UART0_RTS	PA[3]	PWM3		
11	VDD33					
12	PD4	UART1_RX/IrDA_IN	PD[4]			
13	PD5	UART1_TX/IrDA_OUT	PD[5]			
14	PB2	SPI0_SCK	PB[2]	PWM2	SPI3_CLK	
15	PB3	SPI0_CSN0	PB[3]	PWM3	SPI3_CSN0	
16	PB4	SPI0_MOSI	PB[4]	PWM4	SPI3_MOSI	
17	PB5	SPI0_MISO	PB[5]	PWM5	SPI3_MISO	
18	PB12	SPI2_CLK	PB[12]	SPI3_CLK	UART1_RX/IrDA_IN	
19	PB13	SPI2_CSN	PB[13]	SPI3_CSN0	UART1_TX/IrDA_OUT	
20	PB14	SPI2_MOSI	PB[14]	SPI3_MOSI	UART1_CTS	
21	PB15	SPI2_MISO	PB[15]	SPI3_MISO	UART1_RTS	
22	VDD12					
23	RST_N					
24	PC9					
25	PC15	SPI1_MISO	PC[15]	SPI3_MISO	UART2_TX/IrDA_OUT	
26	PC14	SPI1_MOSI	PC[14]	SPI3_MOSI	UART2_RTS	
27	PC13	SPI1_CLK	PC[13]	SPI3_CLK	UART2_RX/IrDA_IN	
28	PC12	SPI1_CSN	PC[12]	SPI3_CSN	UART2_CTS	

29	CHARGE_VPROG					CHARGE 充电电流控制管脚
30	CHARGE_VCC					CHARGE 电源输入
31	CHARGE_VBAT					CHARGE 电源出，接电池
32	PC4	TCK	PC[4]	ADC_IN4		
33	PC3	TMS	PC[3]	ADC_IN3	UART1_RTS	
34	PC2	TDO	PC[2]	ADC_IN2	UART1_CTS	
35	PC0	TRST	PC[0]	ADC_IN0	UART1_RX/IrDA_IN	
36	VDD33					
37	DN					USB DN
38	DP					USB DP
39	VBUS					USB VBUS
40	XI12M					XTAL 12MHz Input
41	XO12M					XTAL12MHz Output
42	VDD33					
43	XO32					XTAL 32KHz Output
44	XI32					XTAL 32KHz Input
45	EXTS3					外部 Tamper3
46	EXTS1					外部 Tamper1
47	EXTS2					外部 Tamper2
48	EXTS0					外部 Tamper0

2.3 封装信息

2.3.1 QFN32



		SYMBOL	MIN	NOM	MAX
TOTAL THICKNESS		A	0.7	0.75	0.8
STAND OFF		A1	0	0.02	0.05
MOLD THICKNESS		A2	---	0.55	---
L/F THICKNESS		A3		0.203 REF	
LEAD WIDTH		b	0.18	0.23	0.28
BODY SIZE	X	D		5 BSC	
	Y	E		5 BSC	
LEAD PITCH		e		0.5 BSC	
EP SIZE	X	D2	3.6	3.65	3.7
	Y	E2	3.6	3.65	3.7
LEAD LENGTH		L	0.3	0.35	0.4
LEAD TIP TO EXPOSED PAD EDGE		K		0.325 REF	
PACKAGE EDGE TOLERANCE		aaa		0.1	
MOLD FLATNESS		ccc		0.1	
COPLANARITY		eee		0.08	
LEAD OFFSET		bbb		0.1	
EXPOSED PAD OFFSET		fff		0.1	

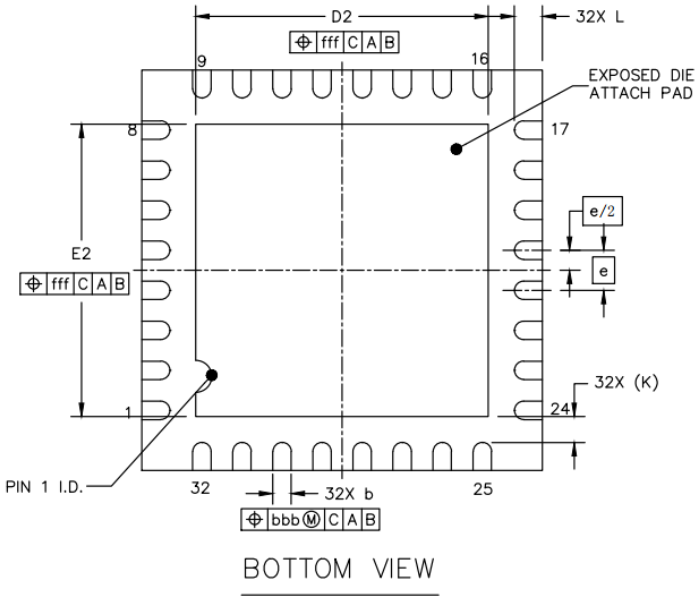
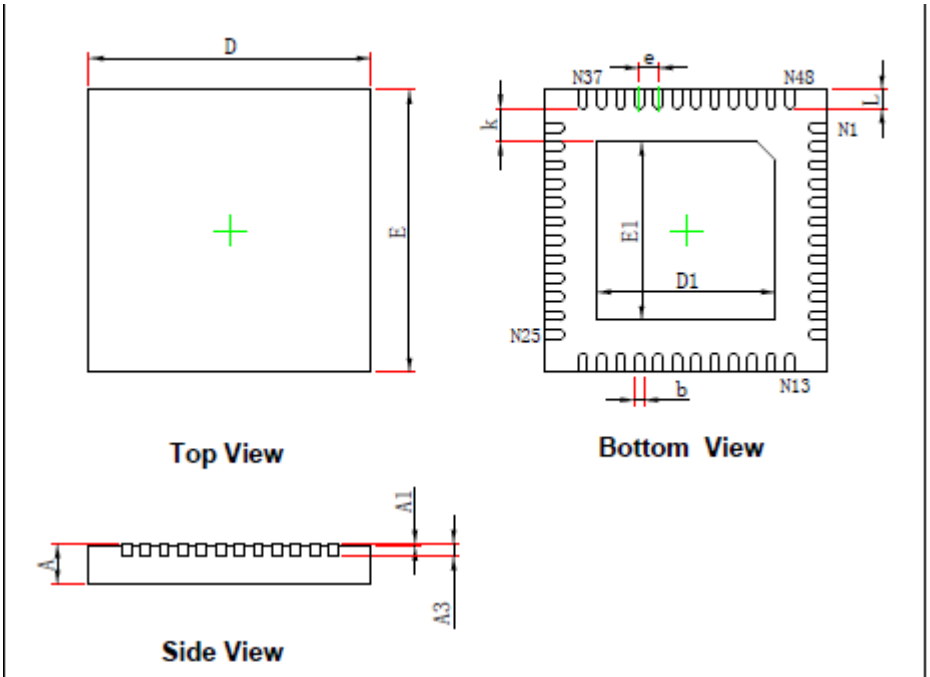


图 2-1 ID812 QFN32 5mm*5mm 封装尺寸

2.3.2 QFN48



Symbol	Dimensions In Millimeters		Dimensions In Inches	
	Min.	Max.	Min.	Max.
A	0.700/0.800	0.800/0.900	0.028/0.031	0.031/0.035
A1	0.000	0.050	0.000	0.002
A3	0.203REF.		0.008REF.	
D	5.924	6.076	0.233	0.239
E	5.924	6.076	0.233	0.239
D1	3.700	3.900	0.146	0.154
E1	3.700	3.900	0.146	0.154
k	0.200MIN.		0.008MIN.	
b	0.150	0.250	0.006	0.010
e	0.400TYP.		0.016TYP.	
L	0.324	0.476	0.013	0.019

图 2-2 ID812 QFN48 6mm*6mm 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。

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 Sermiconductor 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。

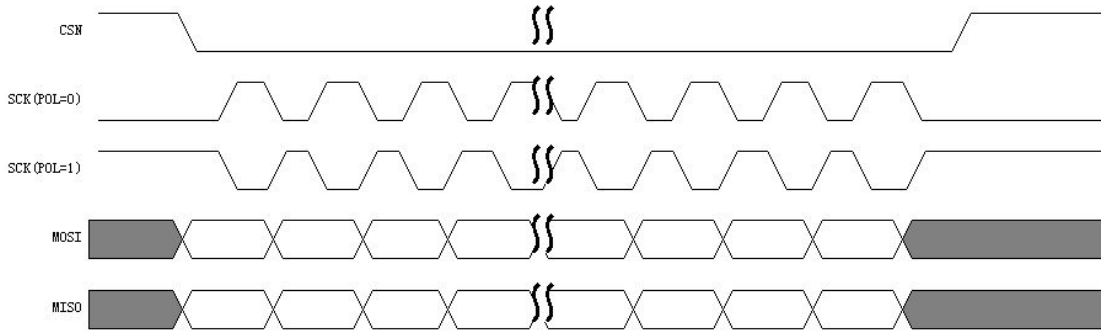


图 3-1 SPI 时序 1(CPHA=0)

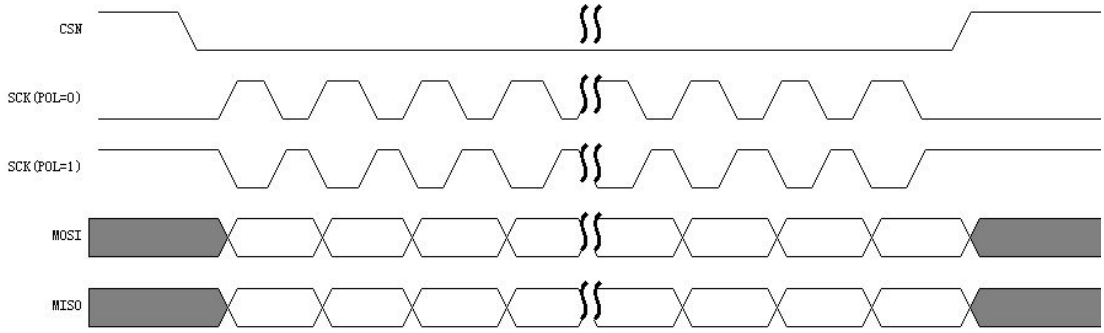


图 3-2 SPI 时序 2(CPHA=1)

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 USB

OTG_FS 控制器接口，符合 USB 2.0 标准

- 支持 USB2.0
- 支持 SRP 协议的 USB 全速/低速设备(B 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

3.1.5 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、12M 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。

3.1.6 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。

3.1.7 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。