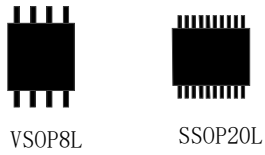
RJMU401

大容量增强型，基于 ARM 安全智能卡内核的国密安全芯片

内嵌 SM1、SM2、SM3、SM4 国密加密算法

功能

- **内核：高性能 32 位 ARM SC100 CPU**
  - 双总线架构，DMA 加速，快速中断响应
  - 支持 ARM 和 Thumb 指令集
  - 三级流水线
  - 采用软内核技术，防止外部对其进行扫描
  - 采用小端存储格式
  - 主频为 32MHz，可进行 3、4 分频，系统默认工作频率 8M
- **存储器**
  - 8KB ROM
  - 18K RAM
  - 128～550KB 的 FLASH 存储器
- **时钟、复位和电源管理**
  - 1.6V~5.5V 供电
  - CPU 时钟可由软件配置为内部时钟
  - 内置 32 MHz 高速 RC 振荡器，支持 3/4 分频
  - 内置多功能时钟发生电路
  - 内置 32 KHz 低功耗 RC 振荡器
- **多达 6 个定时器**
  - 3 个 16 位通用定时器、
  - 1 个 ETU 定时器
  - 1 个 Wake-up 定时器
  - 1 个 32 位看门狗定时器
- **多种密码算法**
  - 对称算法：DES、T-DES、AES、SM1、SM4
  - 非对称算法：RSA、SM2
  - 摘要算法：SM3、SHA-256
- **安全特性**
  - 存储保护单元（MPU）
  - 频率检测功能
  - 存储总线检测功能，防 FIA 攻击
  - 抗 EMA/DEMA 攻击
  - 硬件 CRC16/32 电路校验
  - 硬件真随机发生器
  - 防篡改检测电路
- **封装**



VSOP8L　　SSOP20L

- **外围接口**
  - 1 路智能卡接口，符合 ISO7816 标准，支持 T=0/T=1 协议
  - 1 路 SWP 接口，速率高达 1.2Mbps
  - 1 路 SPI 主从接口
  - 1 路 UART 接口
  - 高达 15 路 GPIO，支持多种中断方式，多达 12 路 GPIO 可复用
- **应用市场**
  - 城市一卡通 PBOC 终端、一卡通、银行 POS 机、移动无线支付等金融支付
  - SIM 卡、JAVA 卡、ESIM 卡等领域
  - 嵌入式软件安全保护
  - 手机、通信模块、路由器、对讲机等数据加密
  - 监控设备、自动化控制

Rev2.1
2018.5.17

1、简介

1.1 概述

RJMU401 安全芯片是一个基于 32 位 RISC 处理器的 SOC 芯片，具备高处理能力、高安全性、低功耗、低成本等特点。该芯片可用于 SIM 卡芯片，支持无线支付应用，也可以用于金融卡。

该芯片采用ARM SC100核，使用AHB+APB总线结构的SOC，内置定时器、终端控制器、系统控制器等完备的安全机制，同时内置多种加密算法，支持对称加密算法DES/3DES、AES、国密SM1、国密SM4;非对称加密算法RSA、国密SM2;摘要算法国密SM3、SHA-256，除此之外芯片内设计有频率安全探测器，以保证芯片在非正常工作条件下的操作安全。芯片内置大容量ROM、SRAM 以及Flash存储器，能够满足复杂操作系统以及应用程序开发的需求。芯片支持多种对外通讯接口，包括ISO7816-3、SWP接口、UART、SPI。SWP接口支持NFC近距离通信，能实现小额移动支付。

1.2 系统架构

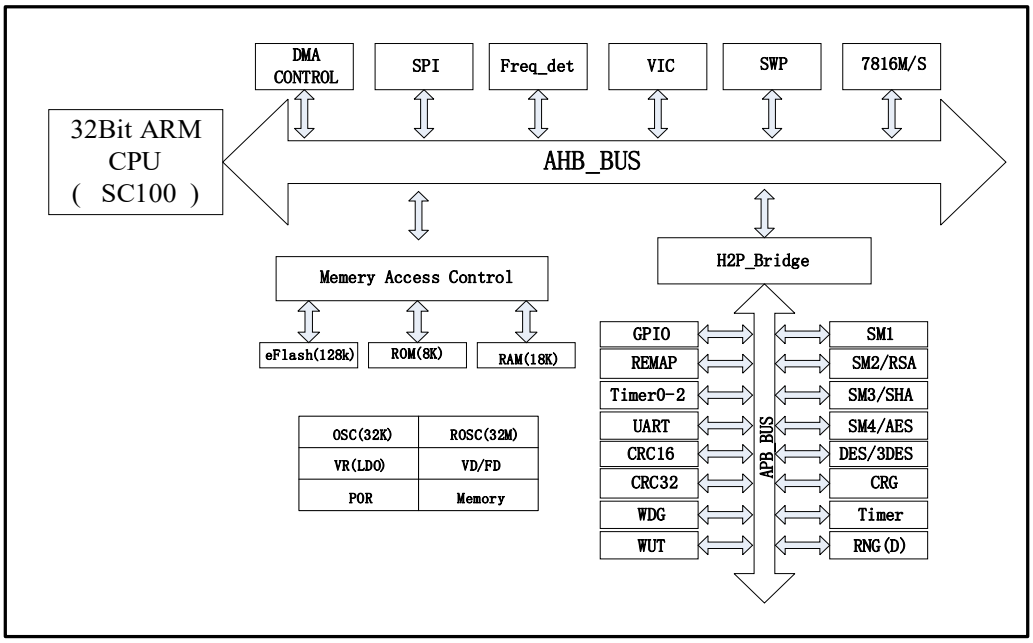


图 1 系统结构图

模块	描述
MCU	ARM 32位安全处理器核SC100
	AHB+APB 总线（含 Bus Arbitor 以及总线桥接器）
	2 channel DMA 控制器
	VIC，中断矢量控制器，可设置中断优先级
	Memory：128～548KB FLASH；8KB ROM；18KB RAM；
	MCtrl，memory 存储器访问控制模块
Timers，WDT	3个通用定时/计数器，1个ETU 定时器/计数器， 1个Wake-Up 定时器，1个32位看门狗定时器
ISO7816	符合ISO/IEC 7816-3 标准的IO从接口，支持T=0和T=1 通信协议
SWP	符合单线连接协议的接口
SPI	同步串行外设主/从接口
GPIO	15个GPIO，每一管脚都能配置成高电平、低电平、上升沿、下降沿、上升下降沿中断方式
UART	通用异步串行口

安全加密模块	分组加密协处理器：DES/3DES、AES； 公钥加密运算协处理器：RSA； 国密SM1； 国密SM2； 国密SM3； 国密SM4； SHA256； TRNG：2个真随机数发生器； CRC16，CRC32
Internal Clock	内部时钟产生32MHz、32KHz；
POR	上电复位
FD	外部时钟频率检测

2、性能参数

2.1 处理器系统

- 基于 ARM 结构设计而成的处理器核，采用小端对齐，支持 ARM 和 Thumb 指令集，均为 RISC 结构的指令；
- 双总线架构，支持 ARM-Thumb 技术，DMA 加速；
- 采用三级流水结构，取指、译码、执行可形成流水操作；
- 指令和数据共用 32 位总线，装载存储和交换指令可以对存储器中的数据进行访问；
- 具有 CP15 系统控制协处理器；
- 单指令乘法器和硬件除法；
- 支持存储器保护单元(MPU)，可以分别对存储器的不同部分进行权限设置，实现安全访问控制管理；
- 处理器支持七种操作模式，两种安全模式:用户或特权模式；
- 采用软内核技术，防止外部对其进行扫描探测；
- 可集成用户自己的安全特性和其他协处理器；
- Sleep 模式，支持唤醒模式；
  - 扩展 IO 电平变化唤醒；
  - UART 唤醒；
  - SPI 唤醒；
  - ISO7816；
  - SWP；

2.2 存储单元

- 片上集成 ROM 8KB；
- 片上集成 128～550KB 嵌入式 eFLASH（ 548KB FLASH+ 2KB OTP ）：
  - 支持页擦除、页写；
    1. 擦除和编程都必须按页进行；
    2. 编程之前必须先执行擦除操作；

3. 擦除后比特值为 0，编程后比特值为 1，支持芯片擦除；

- 页面大小 256Byte/页；
- 最小擦写次数 10 万次@25° C；
- 最短数据保持时间 100 年@室温；
- 可灵活用作代码区和数据区；
- 提供 2KB 的一次性可编程空间，可防止重要数据被篡改；

- 片上集成最大 18KB RAM；
- 支持存储保护单元(MPU)，FLASH 和 RAM 访问受 MPU 权限控制，实现安全访问控制和用户分区管理：
  - 保护 RAM 数据不被非法访问；
  - 保护 BOOT 数据不被非法访问；
  - 实现不同用户权限安全访问控制；

2.3 中断控制器

- 支持向量中断；
- 支持中断查询；
- 支持可配置优先级，32 路中断请求输入；
  - 32 个通道分为 8 个不同的优先级，通道 0—3 具有最高的优先级，通道 4—7 具有次高的优先级；
  - 相同优先级的 4 个通道之间不能相互打断；
- 各功能模块均能产生对应独立中断，支持 32 个外设中断源；

2.4 时钟与定时器

- CPU 时钟源可由软件配置为内部时钟：
  - 主频为 32MHz，可进行 3、4 分频，系统默认工作频率 8M；
- 内嵌 32 位看门狗计数器 WDT，其时钟源与系统时钟相同；
- 支持 Wake_up 定时器，以 OSC32k 时钟 12 分频或系统时钟 12 分频为时钟源，定时产生时钟唤醒和中断，用于唤醒系统；
- 时钟单元：

- 内置 32 MHz 高速 RC 振荡器，支持 3/4 分频；
- 内置多功能时钟发生电路；
- 内置 32 KHz 低功耗 RC 振荡器；
- 内置 3 个通用定时器、ETU 定时器和看门狗定时器；

2.5 安全性及物理防护

提供芯片级 ESD 防护水平和高可靠性安全防护算法，有效防止抄板，以及代码反向分析。

- **芯片级 ESD 防护**
  - MIL - STD - 883H Method 3015.8

    所有的接口：4KV；
  - GB/T 17626.2 - 1998(IEC/EN 61000 - 4 - 2)

    1、 <=4KV(达到标准 A 类等级，芯片不能出现物理损坏，芯片不会中断工作，或者暂时不工作，打击后自动继续工作)；

    2、 >4KV(在芯片未出现物理损坏之前，达到标准 B 类等级，没有借助外部控制，芯片自动进入复位状态，继而可重新恢复到安全的工作状态)；
- **安全算法**
  - 真随机数发生器

    1、 符合国家密码安全管理局《随机性检测规范》的相关要求；

    2、 通过随机数测试国际标准 FIPS 140 - 2 和 NIST SP800 - 22 标准测试；
  - DES 算法单元

    1、 支持 DES、3DES 算法加密、解密运算；

    2、 执行一次单 DES 操作，需要 17 个时钟周期；

    3、 执行一次 TDES 操作，需要 51 个时钟周期；

    4、 支持 ECB 模式
  - AES 算法单元

    1、 内嵌 AES 协处理器支持 128bit(加密 10 轮)、192bit(加密 12 轮)和 256bit(加密 14 轮)密钥长度；

    2、 支持 CBC、ECB 模式；

- SM1/SM4 算法单元

1、 支持 SM4 算法，实现加密、解密功能；

2、 内嵌 SM1 协处理器，支持 SM1-128、SM1-192、SM1-256 算法；

- SM3/SHA256 算法单元

1、 SM3 密码杂凑算法，用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成；

2、 芯片内嵌 SHA-256 硬件电路，自动产生一个 256 位的消息摘要；

3、 SHA-256 反向解密的时，一个位的错误即发生雪崩效应，芯片将自毁；

4、 通过配置寄存器 SM3_SHA_SEL 选择 SM3 或者 SHA；

- RSA/SM2 算法单元

1、 RSA 是目前最有影响力的公钥加密算法，已被 ISO 推荐为公钥数据加密标准；

2、 支持 1024-2048 位自定义位数的 RSA 加解密；

3、 SM2 加解密和签名验签运算；

- CRC 校验单元

1、 芯片内置了 16 位和 32 位 CRC 循环冗余校验码的计算电路；

2、 CRC16 采用 CRC-CCITT 算法，生成多项式为 G(x)=x^16+x^12+x^5+1；

3、 CRC32 采用 CRC-MPEG-2 算法；

4、 支持待校验数据生成循环冗余校验码方向配置；

5、 循环冗余计算初始值可配置(手动输入任意值或使用上次计算结果)；

6、 支持 CPU 模式；

7、 校验速度不小于 50Mbps；

- 芯片级安全系统级防护策略

1、 存储总线检测功能，防 FIA 攻击；

2、 抗 EMA/DEMA 攻击；

3、 主动防护层攻击；

4、 被动防护层攻击；

5、 片内 FLASH、RAM 等存储单元数据高强度加密及串扰防护；

6、 硬件提供频率检测模块（FD），以对抗频率攻击：

1）当频率超出正常范围后，卡片的频率检测模块将会报警，自动将芯片置于复位状态；

2）只有外部复位才可以使芯片重新开始工作；

2.6 对外接口

- SPI 主、从接口

1、 一路硬件 SPI 接口，可以使用一般方式与 DMA 方式进行 SPI 的通信；

2、 符合 SPI 接口协议规范；

3、 同步串行、全双工通信总线接口；

4、 支持四种模式(SPIS MODE 0~4)：时钟极性 CPOL、时钟相位 CPHA 可配置；

5、 可配置的传输速率，支持系统时钟的 1、2、4、8、16、32、64、128 分频；

6、 主机模式支持 DMA，但仅支持 DMAC 为流程控制单元；

7、 DMA 传输时，支持只发送，只接收 2 种工作模式；

8、 内部自带发送和接收 fifo，大小均为 16 字节；

- UART 接口

1、 1 路独立 UART 接口；

2、 以字节为单位收发数据；

3、 符合 UART 串口通信协议规范；

4、 异步串行、全双工通信总线接口；

5、 两根总线信号：TX 数据发送，RX 数据接收；

6、 数据位：8 bits；

7、 最高波特率支持 115200bps；

- ISO7816 接口（7816 主从）

1、 1 路独立 ISO7816 接口；

2、 符合 ISO/IEC7816 - 3 标准，支持 PBOC3.0 卡规范；

3、 支持 T=0/T=1 协议，即异步半双工字符传输协议；

4、 数据宽度 8bits；

5、 奇偶校验方式可配置；

6、 奇偶校验位自动生成及奇偶校验错误检测；

7、 自动错误检测并报告；

8、 传输自动切换模式可配置；

9、 奇偶校验错误自动重传；

10、 支持 11 种波特率: FD = 11, 91, 92, 93, 94, 95, 96；

11、 Flash 编程过程和数据接收过程可同时进行；

12、 专用的 ETU 计数器用于自动发送过程字符（0x60）；

- SWP 接口

1、 芯片含有硬件 SWP 接口，可作为 SWP Slave 设备进行数据收发；

2、 支持一般方式和 DMA 方式；

3、 内部自带发送和接收 fifo，大小均为 32 字节；

4、 主机信号是经过数字调制的电压信号，从机信号是经过数字调制的电流信号，当主机发送的电压信号为高时，从机可以发送低电流或高电流来传送从机信号，从而实现了半双工通信；

5、 发送超时检测；

6、 硬件错误检测；

7、 硬件 CRC 校验；

8、 传输速率最大为 2Mb/s；

- GPIO 接口

1、 总共有 15 个 GPIO；

2、 12 个 GPIO 可配置为第二功能，或者第三功能，第二、三功能的复用；

3、 支持高电平、低电平、上升沿、下降沿、上升下降沿有效的中断；

4、 当系统处于休眠模式下，GPIO 外部中断可以作为唤醒源；

2.7 算法性能

模块	内容	性能（系统 8MHz，算法 8MHz）
非对称算法性能	1024 位 RSA 加密	3.81 ms/次
	1024 位 RSA 解密	132.6 ms/次
	SM2 加密	171 ms/次
	SM2 解密	56 ms/次

对称算法性能	DES 加密/解密（ECB）		55.17 KB/S
	DES 加密/解密（CBC）		41.88 KB/S
	3DES 加密/解密（ECB）		34.78 KB/S
	3DES 加密/解密（CBC）		28.78 KB/S
	128 位 AES 加密/解密		51.61 KB/S
	192 位 AES 加密/解密		45.45 KB/S
	256 位 AES 加密/解密		39.41 KB/S
	SM1 加密/解密（长度，轮数）	128-8	188.24 KB/S
		128-10	181.82 KB/S
		128-12	183.91 KB/S
		128-14	179.78 KB/S
		192-8	190.48 KB/S
		192-10	181.82 KB/S
		192-12	177.78 KB/S
		192-14	175.83 KB/S
		256-8	190.48 KB/S
		256-10	183.91 KB/S
		256-12	181.82 KB/S
		256-14	177.78 KB/S
	SM4		45.98 KB/S
杂凑算法	SHA256		169.31 KB/S
	SM3		164.1 KB/S

2.8 模块功耗性能

模块	功耗	备注
7816	4mA	
SPI	3mA	

UART	2.5mA	发送功耗
	2.8mA	接收功耗
SWP	5mA	
GPIO	2.6mA	
CRC32/16	2.7mA	
VTC	2.8mA	
WDT	3.2mA	
WUT	2.7mA	
RSA	5.5mA	公钥加解密
		私钥加解密
SHA256	3.2mA	
SM1	3.5mA	192/256 位私钥长度，8-14 轮加解密时间
SM2	5mA	加密时间
		解密时间
		点乘模块
		数字签名
		验签时间
SM3	3.6mA	
SM4	2.4mA	128 位计算时间
AES	3.7mA	128 位加解密时间
		192 位加解密时间
		256 位加解密时间
DES/3DES	3.8mA	ECB 加解密时间
		ECB-3DES 加解密时间
		CBC-DES 加解密时间
		CBC-3EDS 加解密时间
Sleep	52uA	
Reset	1.4mA	

ROM	2.4mA	

2.9 其他模块

- MPU 采用四种保护机制：

  1、 对齐检查；

  2、 溢出检查；

  3、 区域访问权限检查；

  4、 未定义存储空间检查（外部中止）；

- RNG 真随机数发生器

  1、 内嵌两组 32 位随机数发生器，以满足某些应用中的安全交易流程需要；

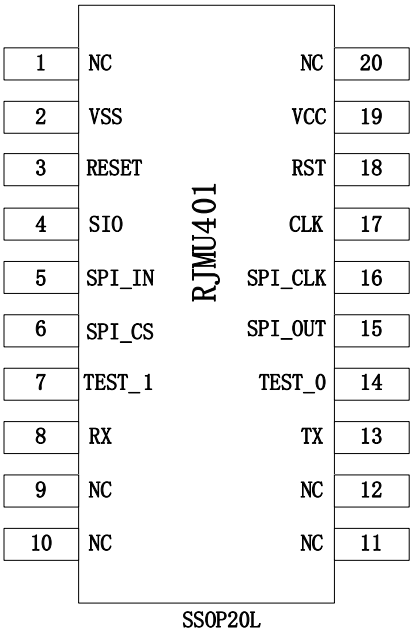
  2、 随机数发生器是数字振荡环方式真随机数发生器（DTRNG）；

2.10 模拟模块

- 集成 32MHz OSC，精度范围+/－5% @－25~85°C；
- 集成 32KHz OSC，精度范围+/－5% @－25~85°C；
- 输出电压精度+/－10%；
- 支持软件控制开关输出或断开输出电源功能；

3、引脚定义

3.1 引脚定义图：SSOP_20L

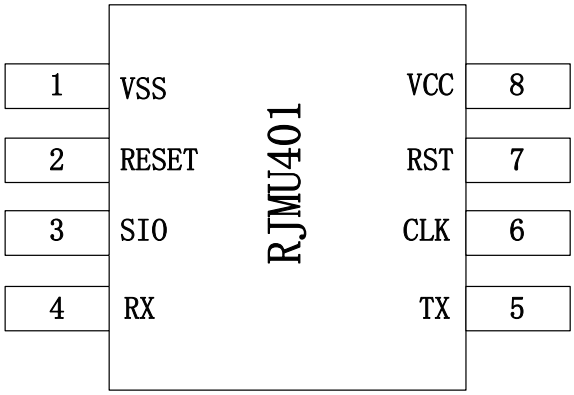


SSOP20L

PIN	信号名称	信号说明
1	NC	
2	VSS	地或是电源负极
3	RESET	芯片复位信号（高有效）
4	SIO	7816 输入输出（I/O）
5	SPI_IN	SPI Slave 输入
6	SPI_CS	SPI Slave 片选
7	TEST_1	测试引脚；不使用，请悬空，禁止接地。
8	RX	UART 输入
9	NC	
10	NC	
11	NC	
12	NC	

13	TX	UART 输出
14	TEST_0	测试引脚；不使用，请悬空，禁止接地。
15	SPI_OUT	SPI Slave 输出
16	SPI_CLK	SPI Slave 时钟
17	CLK	7816 时钟
18	RST	7816 复位
19	VCC	电源电压
20	NC	

3.2 引脚定义图：VSOP_8L



VSOP8

PIN	信号名称	信号说明
1	VSS	地或是电源负极
2	RESET	芯片复位信号（高有效）
3	SIO	7816 输入输出（I/O）
4	RX	UART 输入
5	TX	UART 输出
6	CLK	7816 时钟
7	RST	7816 复位
8	VCC	电源电压

4、接口电气特性

4.1 测试条件

除非特别说明，所有电压的都以 VSS 为基准。

4.1.1 最小和最大数值

除非特别说明，在生产线上通过对 100%的产品在环境温度 TA=25° C 和 TA=TAmax 下执行的测试(TAmax 与选定的温度范围匹配)，所有最小和最大值将在最坏的环境温度、供电电压和时钟频率条件下得到保证。

在每个表格下方的注解中说明为通过综合评估、设计模拟和/或工艺特性得到的数据，不会在生产线上进行测试；在综合评估的基础上，最小和最大数值是通过样本测试后，取其平均值再加减三倍的标准分布(平均±3Σ)得到。

4.1.2 典型数值

除非特别说明，典型数据是基于 TA=25° C 和 VCC=3.3V(2V ≤ VCC ≤ 3.3V 电压范围)。这些数据仅用于设计指导而未经测试。

4.2 7816 接口电气特性

参数	符号	最小值	典型值	最大值	单位
电源电压	VCC	1.6	3.3	5.5	V
电源电流	Icc	-	-	10	mA
电源峰值电流		-	-	50	mA
I/O	Vih	0.7xVcc	-	Vcc	V
	Iih	-300		20	uA
	Vil	0		0.15x Vcc	V
	Iil	-1000		20	uA

	Voh	0.7xVcc		Vcc	V
	Ioh	-		20	uA
	Vol	0		0.15x Vcc	V
	Iol	-20		-	uA
RST	Vih	0.8xVcc	-	Vcc	V
	Iih	-20		150	uA
	Vil	0		0.12x Vcc	V
	Iil	-200		20	uA
CLK	Vih	0.7xVcc	-	Vcc	V
	Iih	-20		100	uA
	Vil	0		0.5	V
	Iil	-100		20	uA

4.2.1 绝对最大额定值

参数	符号	最小值	典型值	最大值	单位
电源电压	Vcc	1.6	-	5.5	V
输入电压	VIN	1.6	-	5.5	V
工作温度	TA	-40	-	85	℃
存储温度	TS	-40	25	125	℃
抗瞬变脉冲群电压	VESD	4000	-	-	V
焊接温度	-	-	-	260	℃
焊接时间	-	-	-	9	S

4.3 SPI 接口电气参数

参数	符号	最小值	典型值	最大值	单位
电源电压	VCC	1.6	3.3	5.5	V

电源电流	Icc	-	-	10	mA
电源峰值电流		-	-	50	mA
MOSI	Voh	0.7xVcc		Vcc	V
	Ioh	-		20	uA
	Vol	0		0.15x Vcc	V
	Iol	-20		-	uA
RST	Vih	0.8xVcc	-	Vcc	V
	IIH	-20		150	uA
	Vil	0		0.12x Vcc	V
	Iil	-200		20	uA
SCK	Vih	0.7xVcc	-	Vcc	V
	IIH	-20		100	uA
	Vil	0		0.5	V
	Iil	-100		20	uA
SSN	Vih	0.7xVcc	-	Vcc	V
	IIH	-20		150	uA
	Vil	0		0.12x Vcc	V
	Iil	-200		20	uA

4.3.1 绝对最大额定值

参数	符号	最小值	典型值	最大值	单位
电源电压	Vcc	1.6	-	5.5	V
输入电压	VIN	1.6	-	5.5	V
工作温度	TA	-40	-	85	℃
存储温度	TS	-40	25	125	℃
抗瞬变脉冲群电压	VESD	4000	-	-	V

焊接温度	-	-	-	260	℃
焊接时间	-	-	-	9	S

5、 电源模块设计及工作条件

5.1 电源电路模块设计

片内系统外接电源电压包含三种规格：5V、3.3V 和 1.8V。其中主要应用为 1.8V 和 3.3V，5V 电压作为测试使用。系统要求在三种电源电压下都能完成对片内数字电路和模拟电路 1.8V 电源电压供电。其中数字电路最大供电电流为 10mA，模拟电路最大供电电流为 20mA。

系统整体方案如图 5-1 所示，其中包括 5V/3.3V/1.8V 检测电路、带隙基准电压电路、第一级 LDO 调制电路与第二级 LDO 调制电路。5V/3.3V/1.8V 检测电路：完成 5V、3.3V 和 1.8V 电压检测。带隙基准电压电路，提供两级 LDO 参考电压 Vref。第一级 LDO 调制电路：当电源电压为 5V 时，控制电路关断，第一级 LDO 输出调制后 3.3V；当电源电压为 3.3V 时，控制电路强拉调整管栅极为低电平，调整管进入深度线性区，输出电压跟随电源电压，当输出电流越小，调整管电阻越小，输出越接近 3.3V。第二级 LDO 调制电路：完成 3.3V 到 1.8V 转换，当电压为 1.8V 时，电压直接旁路输入。模拟电路和数字部分最大输出电流不同，需要设计不同调整管尺寸。

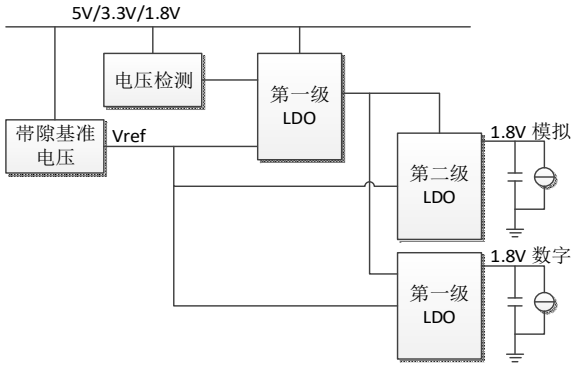


图 5-1 电源电路整体方案

5V/3.3V 检测电路检测电源电压 5V 时输出低电平，3.3V 时输出高电平，电路图如图 8-13 所示。基准电流源产生电流通过亚阈值 NMOS 来产生，这样可以避免利用带隙电路产生面积过大和普通电流源电路电压漂移过大。电源分压用 MOS 分压，可以减少使用电阻的面积，并且温度特性一定，由阈值确定的电压可以减少电源产生的影响。比较结果通过一级反相器整形输出。1.8V 检测电路被设计为当检测到 1.8V 电压时，输出高电平。此时控制信号让电压直通的方式经过电源电路，从而完成芯片对 1.8V，3.3V，5V 的兼容设计。

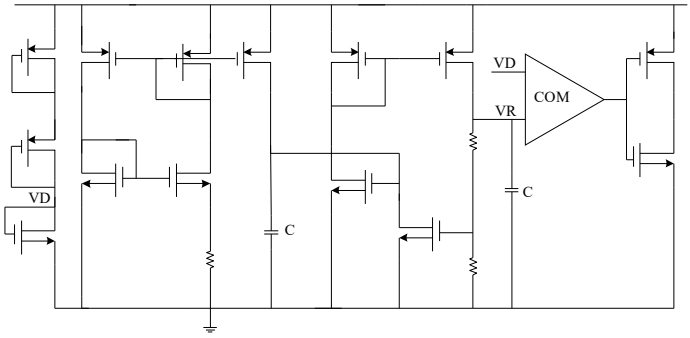


图 5-2　5V/3.3V 检测电路

5.2 推荐工作参数

推荐工作参数如表 11-2 所示。

参数	最小值	最大值	单位
工作电压	1.6	5.5	V
工作温度	-40	85	℃

6 、SPI 功能描述

6.1 概述

通常 SPI 通过 4 个引脚与外部器件相连：

SPI_OUT：从设备输出引脚，引脚在从模式下发送数据。

SPI_IN：从设备输入引脚，在从模式下接收数据。

SPI_CLK：从设备串口时钟，从设备的输入。

SPI_CS：从设备选择。这是一个可选的引脚，用来选择从设备。它的功能是用来作为“片选引脚”，让主设备可以单独地与特定从设备通讯，避免数据线上的冲突。从设备的 SPI_CS 引脚可以由主设备的一个标准 I/O 引脚来驱动。

注意：RJMU401 只有 SSOP20L 的封装具有 SPI 通信接口，该通信接口为从接口。

6.2 时钟信号的相位和极性

SPI_CR 寄存器的 CPOL 和 CPHA 位，能够组合成四种可能的时序关系。CPOL(时钟极性)位控制在没有数据传输时时钟的空闲状态电平，此位对主模式和从模式下的设备都有效。如果 CPOL 被清’0’，SCK 引脚在空闲状态保持低电平；如果 CPOL 被置’1’，SCK 引脚在空闲状态保持高电平。

如果 CPHA(时钟相位)位被置’1’，SCK 时钟的第二个边沿(CPOL 位为 0 时就是下降沿，CPOL 位为’1’时就是上升沿)进行数据位的采样，数据在第二个时钟边沿被锁存。如果 CPHA 位被清’0’，SCK 时钟的第一边沿(CPOL 位为’0’时就是下降沿，CPOL 位为’1’时就是上升沿)进行数据位采样，数据在第一个时钟边沿被锁存。 SPI 接口 STM32F10xxx 参考手册 CPOL 时钟极性和 CPHA 时钟相位的组合选择数据捕捉的时钟边沿。

图 6-1 显示了 SPI 传输的 4 种 CPHA 和 CPOL 位组合。此图可以解释为主设备和从设备的 SCK 脚、MISO 脚、MOSI 脚直接连接的主或从时序图。

注意： 1. 在改变 CPOL/CPHA 位之前，必须清除 SPE 位将 SPI 禁止。

2. 主和从必须配置成相同的时序模式。

3. SCK 的空闲状态必须和 SPI_CR1 寄存器指定的极性一致(CPOL 为’1’时，空闲时应上拉 SCK 为高电平；CPOL 为’0’时，空闲时应下拉 SCK 为低电平)。

4. 数据帧格式(8 位或 16 位)由 SPI_CR1 寄存器的 DFF 位选择，并且决定发送/接收的数据长度。

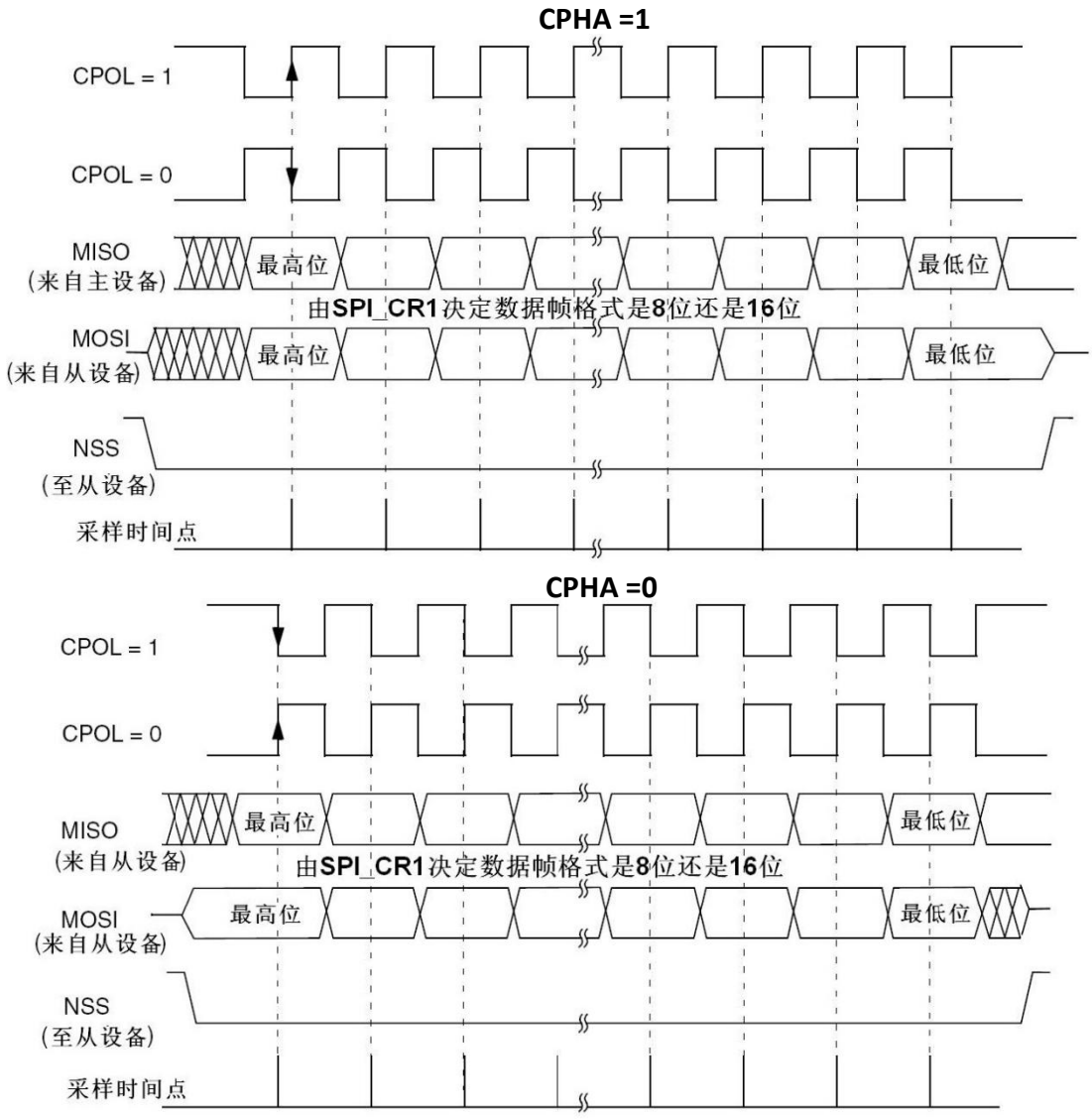


图 6-1 数据时钟时序图

7、应用电路图

7.1 RJMU401FHO 与 STM32F103 的 7816 参考电路

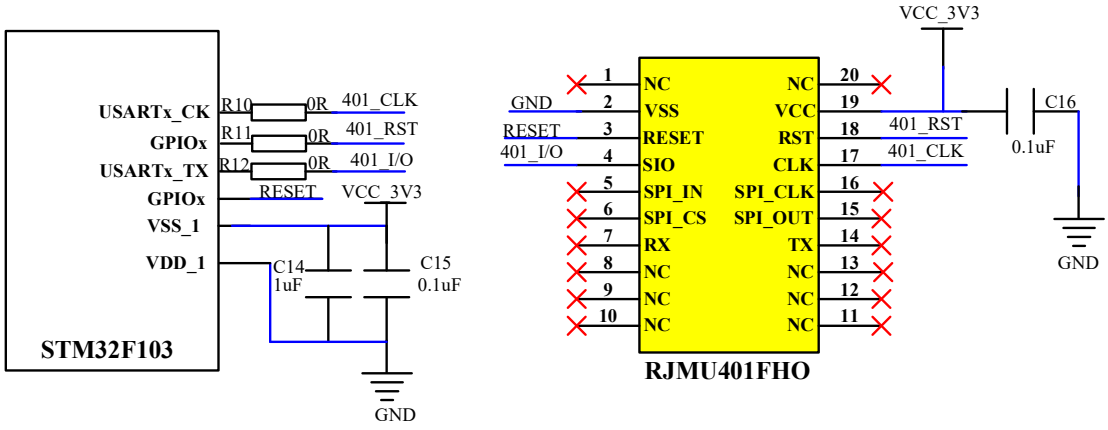
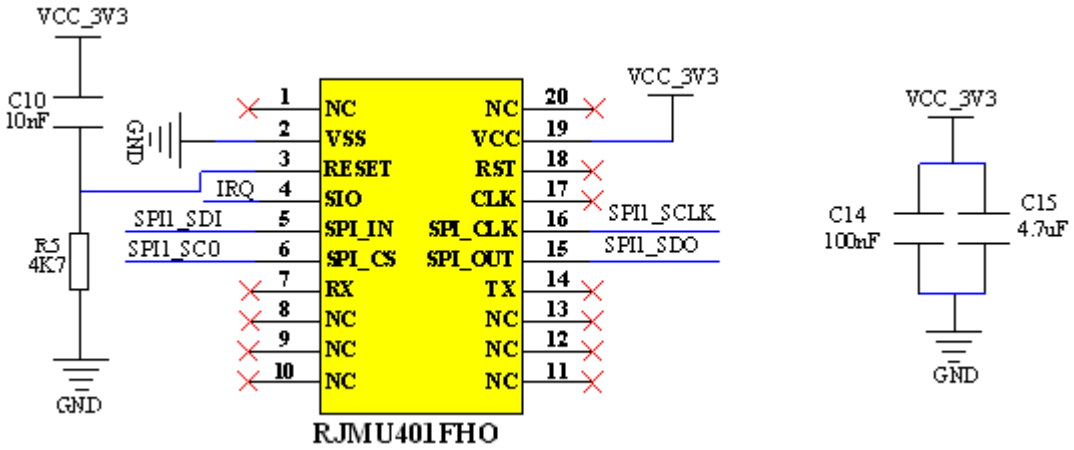


图 7-1 应用电路图

注意： RST: 为 7816 通信接口的复位管脚。

RESET:为芯片复位管脚，不需要可悬空。

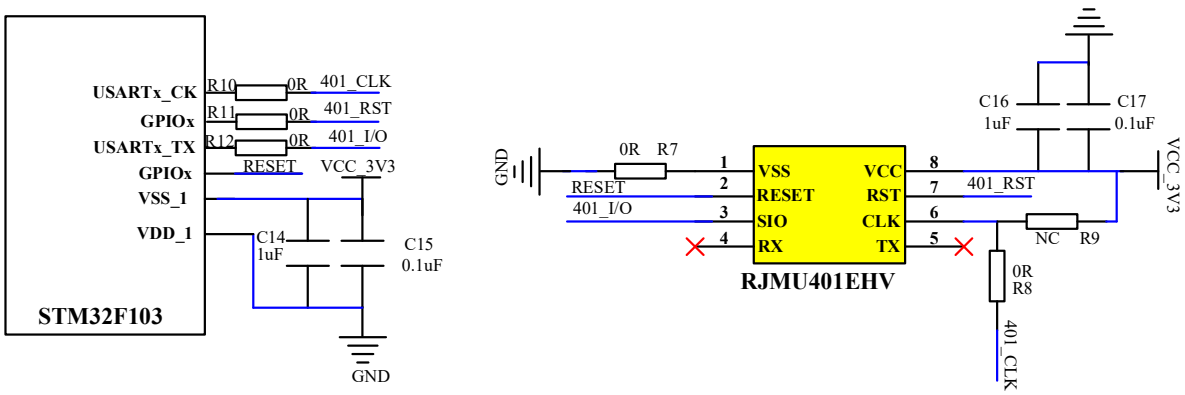
7.2 RJMU401FHO 的 SPI 参考电路



注意： SIO: 作为 IO 管脚输出功能，该管脚主要是作为中断引脚。可选其他 I/O 引脚作为中断引脚。

RESET；为芯片的复位管脚,高电平有效。

7.3 RJMU401EHV 与 STM32F103 的 7816 参考电路

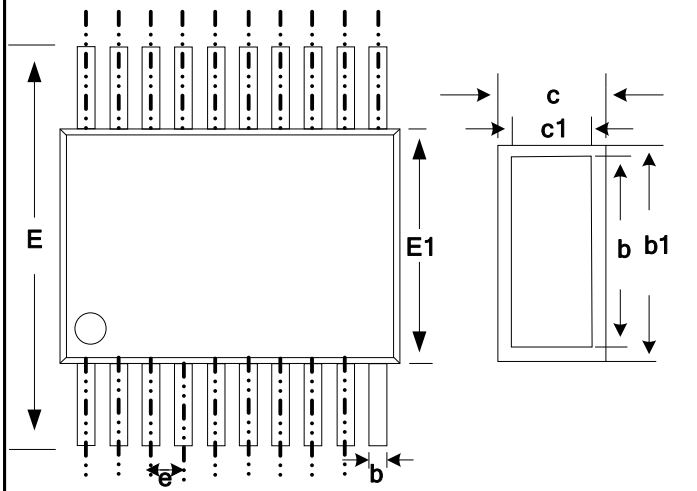


8、电气特性

- Sleep 模式功耗：<55uA；
- Idle 模式功耗：<2mA @CPU 8MHz；
- 最高频典型工作电流：<15mA @CPU32MHz；
- 工作温度：-40ºC~85ºC；
- 最大工作电流：<15mA @CPU32MHz；
- 支持工作电源输入范围：1.62V~5.5V；

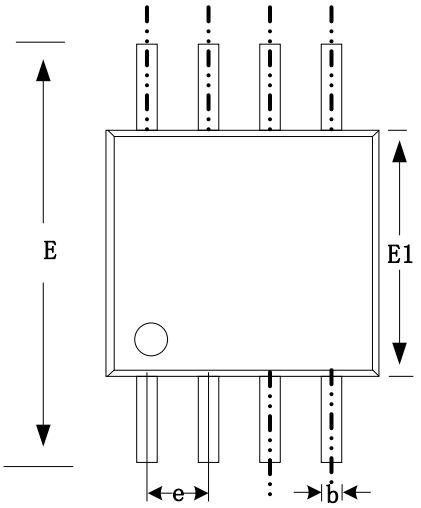
9、芯片封装信息

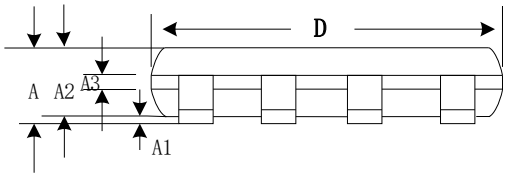
- 封装形式：SSOP20L；

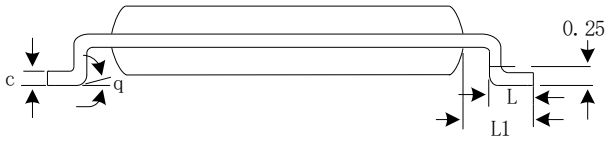


SYMBOL	MILLIMETER		
	MIN	MON	MAX
A	–	–	1.85
A1	0.05	–	0.25
A2	1.40	1.50	1.60
A3	0.62	0.67	0.72
b	0.28	–	0.36
b1	0.27	0.30	0.33
c	0.15	–	0.19
c1	0.14	0.15	0.16
D	7.10	7.20	7.30
E	7.60	7.80	8.00
E1	5.20	5.30	5.40
e	0.65BCS		
L	0.75	–	1.05
L1	1.25REF		
q	0º	–	8º

- 封装形式：VSOP_8L；







SYMBOL	MILLIMETER		
	MIN	MON	MAX
A	--	--	1.00
A1	0.05	0.10	0.15
A2	0.75	0.80	0.85
A3	0.29	0.34	0.39
b	0.38	--	0.46
b1	0.37	0.40	0.43
c	0.13	--	0.19
c1	0.12	0.13	0.16
D	5.18	5.28	5.38
E1	5.18	5.28	5.38
E	7.7	7.90	8.10
e	1.27BCS		
L	0.50	0.65	0.80
L1	1.31REF		
q	0°	--	8°

10、订货信息

器件型号	封装形式	默认丝印	耐温
RJMU401FHO6R	SSOP_20L 塑封	RJMU401	-40℃-85℃

RJ MU 401 F H O 6 R

公司名称前缀

RJ=武汉瑞纳捷电子技术有限公司

产品线

MU=安全 MCU 产品系列

产品系列

101 = 基于 ARM Cotex-SC100 简化型
201 = 基于 ARM Cotex-SC100 基础型
401 = 基于 ARM Cotex-SC100 增强型
301 = 基于 C51 内核的简化型

引脚数

E= 8 脚
D=14 脚
F=20 脚

Flash 容量

B= 128 KB
C=256 KB
D=386 KB
H=550 KB

封装形式

M=SOP
O=SSOP

工作温度

6=工业级，－40~85℃
7=工业级，－40~105℃

包装形式

T=管装
R=卷带盘装

11、修订历史

时间	版本	修正内容
2016.5	-1.00	初始版本
2017.8	-2.00	
2018.5.17	-2.10	1.添加 2.7 节 算法性能算法 2.添加 2.8 节 模块功耗性能

附录一：简称及缩略语

缩写	全称
B	Byte,字节
COS	Chip Operating System,(智能卡)片上操作系统
CPU	Central Processing Unit,中央处理器
CRC	Cyclic Redundancy Check,循环冗余校验
DES	Data Encryption Standard,数据加密标准
ESD	Electro-Static discharge，静电放电
FD	Frequency Detector，频率检测器
FPS	FLASH Page Size，FLASH 页面大小
GSM	Global System for Mobile communication，全球移动通信系统
ISO7816	International Standard ISO/IEC7816 module，ISO/IEC7816 国际标准
MAC	Memory Access Control，内存访问控制模块
MPU	Memory Protection Unit，存储器保护单元
NMROM	Normal Mode Read Only Memory ，正常模式只读存储器
NVM	Non-Volatile Memory，非易失性存储器
OTP	One Time Programmable，一次可编程存储器
PI	Product Information，生产信息
POR	Power On/Off Reset，上/下电复位
RNG	Random Number Generator，随机数发生器
SFR	Special Function Register，特殊功能寄存器
SIM	Subscriber Identity Module，用户识别模块
SN	Chip Serial Number，芯片序列号（唯一标识符）
TDES	Triple Data Encryption Standard，三重 DES
UI	User Information，用户信息
VD	Voltage Detector，电压检测器
VR	Voltage Regulator，电压调整器
WDT	Watch Dog Timer，看门狗计数器
WUT	Wake-Up Timer,唤醒定时器

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Security ICs / Authentication ICs ***category:***

Click to view products by Runjet ***manufacturer:***

Other Similar products are found below :

A1007TL/TA4STZ DS2476Q+T DS28C36Q+T DS28C22Q+T DS2401-SL+T&R DS28E35P+ ATECC608B-RBHCZ-B DS28E18Q+T W74M12JWSSIQ ATECC508A-MAHAW-S SLB9660XT12FW440XUMA2 SLS32AIA020A4USON10XTMA2 SLB9645XT12FW13332XUMA1 DS2401T&R DS1990R-F5# DS2411P+T&R A1006TL/TA1NXZ ATAES132A-SHER-B ATSHA204A-RBHCZ-B ATECC608A-SSHDA-T A1006UK/TA1NXZ ATAES132A-MAHEQ-S ATECC608A-MAHCZ-S IPL-CHP ATAES132A-MAHER-S AT88SC118-SH-CN-T AT88SC118-SH-CM-T SE050A2HQ1/Z01SHZ SE050A1HQ1/Z01SGZ SE050B2HQ1/Z01SFZ ATECC608A-MAHCZ-T AT88SC118-SH-CM AT88SC118-SH-CN ATAES132A-MAHER-T ATAES132-SH-EQ ATAES132-SH-ER-T ATECC508A-MAHCZ-T ATAES132A-SHEQ-B ATAES132A-MAHER-T ATECC108A-SSHDA-B ATECC508A-SSHCZ-B ATECC508A-SSHDA-B DS2460S+ SLB9645TT12FW13333XUMA2 SLB9665TT20FW563XUMA3 SLB9670VQ20FW785XTMA1 SLM9670AQ20FW1311XTMA1 SLS32AIA010MLUSON10XTMA2 SLS32AIA010MKUSON10XTMA2 SLS32AIA010MHUSON10XTMA2