安全芯片 NRSEC3000
硬件使用手册

版本历史

版本号	日期	作者	版本说明
ver1.0	2011-05-18	韦小刚	初稿
ver1.1	2011-5-18	黄益彬	格式调整，文字描述部分修改
ver1.2	2011-5-23	韦小刚	添加了芯片的电气特性等
ver1.3	2011-5-26	韦小刚	添加了算法、接口性能参数以及接口使用简介
ver1.4	2012-3-5	韦小刚	加入了芯片封装尺寸
ver1.5	2013-7-31	韦小刚	对芯片使用补充说明

目录

1 简介

1.1 芯片概述

处理器：本安全芯片采用32位嵌入式RISC架构的CPU，特点是低功耗、高性能、高代码密度，具有独立的存储器保护单元（MPU）和存储器加密单元（MEU）。

加密算法：芯片内部实现了国家商用密码产品所需的SM2和SM1算法专用加密模块、DES/3DES加密模块和RSA公钥算法引擎。另外，芯片提供32位硬件加密处理器，可用于实现公钥算法、摘要算法以及AES、DES等对称算法。芯片内嵌32位真随机数发生器TRNG，可满足COS开发者的密码学应用，可节约软件开销，提高软件实现效率。

通讯接口：芯片拥有丰富的对外接口，包括：7816（智能卡接口、一种串口，半双工）主/从收发器，可实现T=0和T=1协议，支持多种通信速率；硬件SPI（一种串口，全双工）主/从模块。

信息安全：芯片提供增强的安全特性。通过对存储器管理单元MMU进行配置，完成工作模式设置及相关权限设置，可实现由硬件保证安全性的一卡多应用。另外，芯片提供了包括电压、频率检测机制，程序和数据加密存储机制以及代码保护机制等安全机制，以对抗物理攻击、剖片探测等。

应用领域：芯片是高性能、低功耗、具有丰富的内部协处理器和对外接口的安全芯片，可以作为智能卡、电子密钥、SIM 卡或接触式智能 IC 卡，用于国家商用密码专用算法应用、网络银行应用、PKI 卡、SIM 卡、付费电视应用、城市一卡通应用等对信息安全有较高要求的应用场合。

1.2 芯片结构

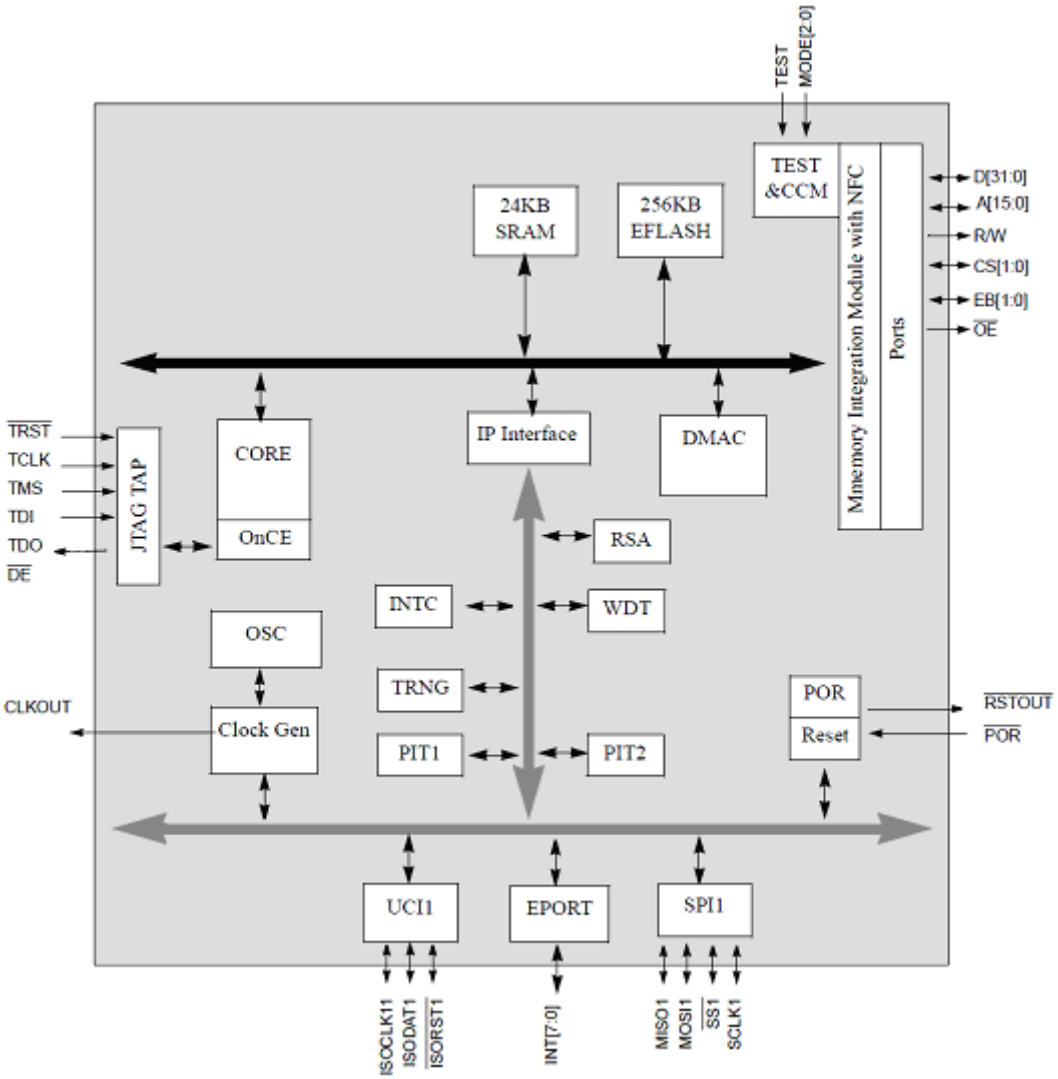


图 1-1 芯片结构

图 1-1 所示为安全芯片的资源分布，下面对芯片中的重要模块、部件及接口进行说明。

1.2.1 中央处理器（CORE）

该 CPU（CORE）是针对信息安全应用的 32 位 RISC 核，包括与 RISC 核整合在一起的存储器保护单元（MPU）。MPU 模块将存储器空间划分为 2 个固定和 8 个可编程的存储器区，通过灵活、强大的访问保护模式，数据/地址的加密/解密机制，防止对敏感数据的非法访问，为 CPU 提供更多安全保护。硬核中还加

入了先进的反攻击机制，使以之为核的 SOC 芯片更加安全。

主要特性：

1) 高性能的安全 RISC 核；
2) 低功耗、高性能设计；
3) 32 位读取/存储 RISC 架构；
4) 高度优化的多级流水线结构；
5) 16*32 位通用寄存器文件；
6) 13*32 位控制寄存器文件；
7) 快速中断支持（支持向量/自动向量中断，128 个中断/异常向量，16*32 位交替寄存器文件用于快速中断支持）；
8) CLB 总线、AMBA 总线支持（支持 byte/halfword/word 访问）；
9) 强大的安全性能（提供存储器保护单元、优化的布局提高了安全性能，不可跟踪和重复的安全测试模式）；
10) 可扩展的模拟器，便于应用软件开发和安全调试。

1.2.2 芯片配置模块（CCM）

芯片配置模块用来控制芯片的配置和工作模式。

主要特性：

1) 选择芯片工作模式（主模式及从模式，单芯片模式及多芯片模式，EFLASH 测试模式，真随机数发生器 TRNG 测试模式）；
2) 选择 boot 设备；
3) 对总线进行配置。

1.2.3 复位控制器模块

复位控制器模块用来决定系统是否需要复位，在适当的时候为系统唤醒复位信号，并对产生复位的原因进行记录。复位模块中包含了低电压检测器（LVD）和高电压检测器（HVD）。

主要特性：

1) 四个复位源（上电复位，看门狗定时器复位，低电压检测复位，高电压

检测复位）；

2) 软件设置复位管脚 RSTOUT 使芯片系统复位；

3) 软件读取状态字（从状态字可以看出上次复位的原因）。

1.2.4 时钟模块

时钟模块包含晶振（OSC）、状态和控制寄存器以及控制逻辑单元。

主要特性：

1) 两个可选时钟源（外部晶振，内部环形振荡器）

2) 支持低功耗模式；

3) 独立的时钟信号；

1.2.5 存储器集成模块

存储器集成模块用来控制内部总线与内存模块间信息的传输。具有两个外部存储器的片选信号 CS0 和 CS1。

主要特性：

1) 固定基地址，具有 256KB 空间

2) 具有两个外部存储器的片选信号 CS0 和 CS1。

1.2.5 嵌入式 Flash 模块（EFM）

嵌入式 FLASH（EFLASH）模块具有 32 位可编程嵌入式 FLASH 存储器，使用页擦除操作可以擦除一页（2048 字节）上的所有数据，擦写操作是在 CPU 指令的控制下进行的。

主要特性：

1) 256KB 的 FLASH 内存；

2) 自动擦写操作；

3) 具有安全机制；

1.2.6 看门狗定时器模块（WDT）

16 位看门狗（Watchdog）定时器是在程序非正常运行的情况下强制恢复系统。实际上就是一个减法计数器，一般给看门狗一个大数，程序开始运行后看门狗开始倒计数。如果程序运行正常，过一段时间 CPU 应发出指令让看门狗复位，重新开始倒计数。如果看门狗减到 0 就认为程序没有正常工作，强制整个系统复位。

工作模式如下：

1) 等待模式；
2) 休眠模式；
3) 停止模式；
4) 调试模式。

1.2.7 可编程中断定时器模块（PIT）

16 位可编程中断定时器在系统出现正常中断时提供精准的中断信号，它实际上也是一个减法计数器。

其工作模式与看门狗定时器相同：

1) 等待模式；
2) 休眠模式；
3) 停止模式；
4) 调试模式。

1.2.8 静态随机存储器（SRAM）

静态随机存储器特点如下：

1) 空间大小为 20KB；
2) 地址空间固定；
3) 支持字节（8 位）、半字（16 位）及字（32 位）读写访问；
4) 超级用户或普通用户都可以访问。

1.2.9 加密处理器模块

加密处理器模块支持常用的公钥加密算法。

主要特性：

1) 整数运算；
2) 模运算；
3) 大数操作。

1.2.10 DMA 控制器

DMA(Direct Memory Access)即直接内存存取，它允许不同速度的硬件装置直接进行沟通，而不需要或尽量减少 CPU 的参与。

主要特性：

1) 一个可编程 DMA 控制器通道；
2) 数据以 8 位、16 位、32 位传输；

1.2.11 通用串行接口（USI）

这里采用的接口即 ISO7816 接口。

主要特性：

1) 支持智能卡模式和读卡器模式；
2) 支持 T=0 和 T=1 协议；
3) 数据传输为半双工；
4) 1 个数据发送缓冲器和 1 个数据接收缓冲器；
5) 13bit 波特率可选，F/D 因子可选（11.625,23.25,46.5,93,186,372,744）；
6) 采用硬件奇偶校验。

1.2.12 串行外设接口模块（SPI）

串行外设接口（SPI）为 MCU 和外设提供同步全双工的串行通讯，可以使用软件进行对串口的设置。

主要特性：

1) 主/从工作模式；
2) 可以传输字(32 位)、半字（16 位）和字节（8 位）；
3) 低功耗设计；
4) 时钟信号由主设备产生；
5) 从设备使能信号由主设备产生。

1.2.13 真随机数发生器（TRNG）

真随机数发生器用于产生随机数，为“公私密钥对生成”和“会话密钥协商”等环节提供随机数。

2 芯片封装及电路连接

2.1 封装与尺寸

芯片采用 LQFP 封装（48pin），其封装及管脚定义分别如图 2-1 和表 2-1 所示。

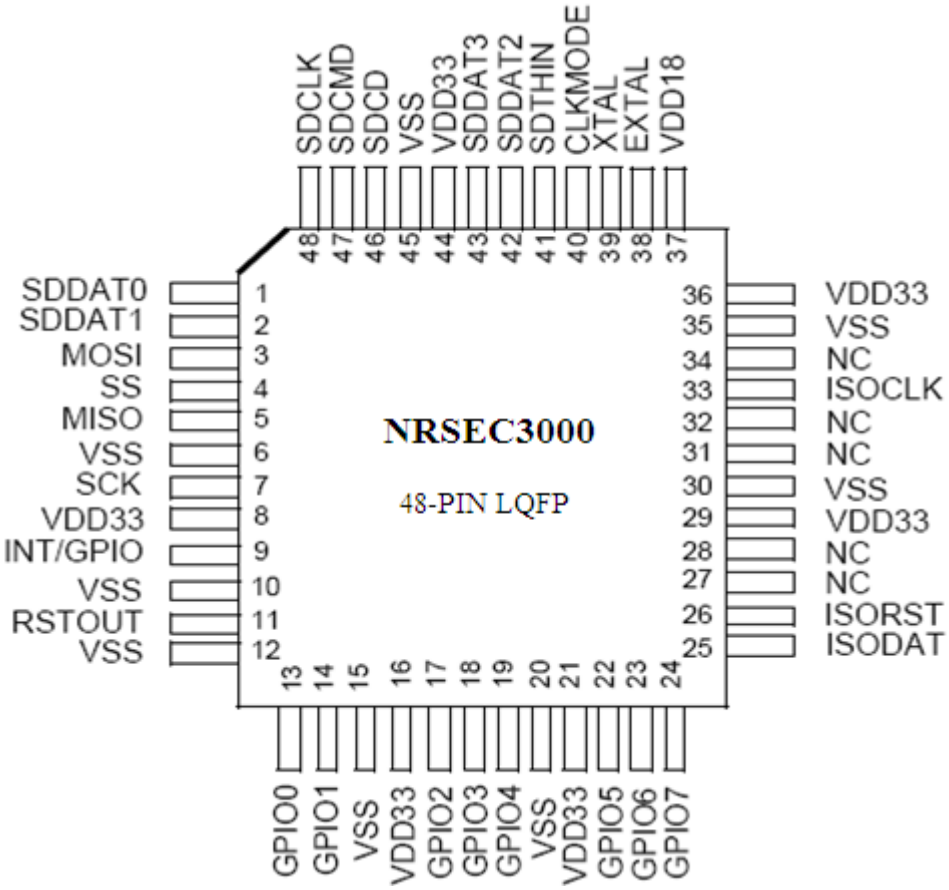


图 2-1 芯片封装

表 2-1 管脚定义

序号	管脚名	功能描述
1	SDDAT0	SD 数据线0
2	SDDAT1	SD 数据线1
3	MOSI	SPI 主机输出/从机输入
4	SS	SPI 从机选择
5	MISO	SPI 主机输入/从机输出
6	VSS	地
7	SCLK	SPI 时钟信号
8	VDD33	3.3V 电源输入

9	INT/GPIO	外部中断输入/GPIO， 3.3V 信号
10	VSS	地
11	RSTOUT	芯片复位输出
12	VSS	地
13	GPIO0	GPIO， 3.3V 信号
14	GPIO1	GPIO， 3.3V 信号
15	VSS	地
16	VDD33	3.3V 电源输入
17	GPIO2	GPIO， 3.3V 信号
18	GPIO3	GPIO， 3.3V 信号
19	GPIO4	GPIO， 3.3V 信号
20	VSS	地
21	VDD33	3.3V 电源输入
22	GPIO5	GPIO， 3.3V 信号
23	GPIO6	GPIO， 3.3V 信号
24	GPIO7	GPIO， 3.3V 信号
25	ISODAT	7816 数据端口
26	ISORST	7816 复位端口
27	NC	未定义
28	NC	未定义
29	VDD33	3.3V 电源输入
30	VSS	地
31	NC	未定义
32	NC	未定义
33	ISOCLK	7816 时钟端口
34	NC	未定义
35	VSS	地
36	VDD33	3.3V 电源输入
37	VDD18	1.8V 电源输入
38	EXTAL	外部震荡输入
39	XTAL	外部震荡输出
40	CLKMODE	内部/外部时钟选择信号脚
41	SDTHIN	SD thin 信号脚
42	SDDAT2	SD 数据线2
43	SDDAT3	SD 数据线3
44	VDD33	3.3V 电源输入
45	VSS	地
46	SDCD	SDCD 信号脚
47	SDCMD	SD 命令信号脚
48	SDCLK	SD 时钟信号脚

芯片的详细尺寸如图 2-2 及表 2-2 所示，供 PCB 设计时参考。

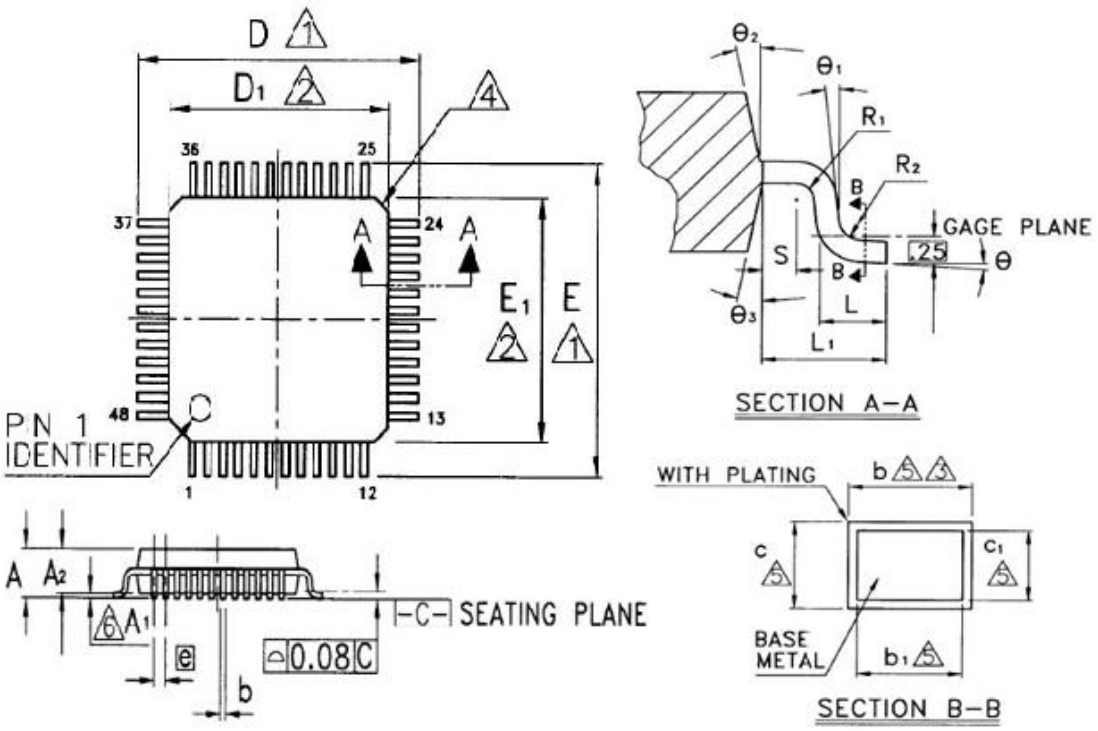
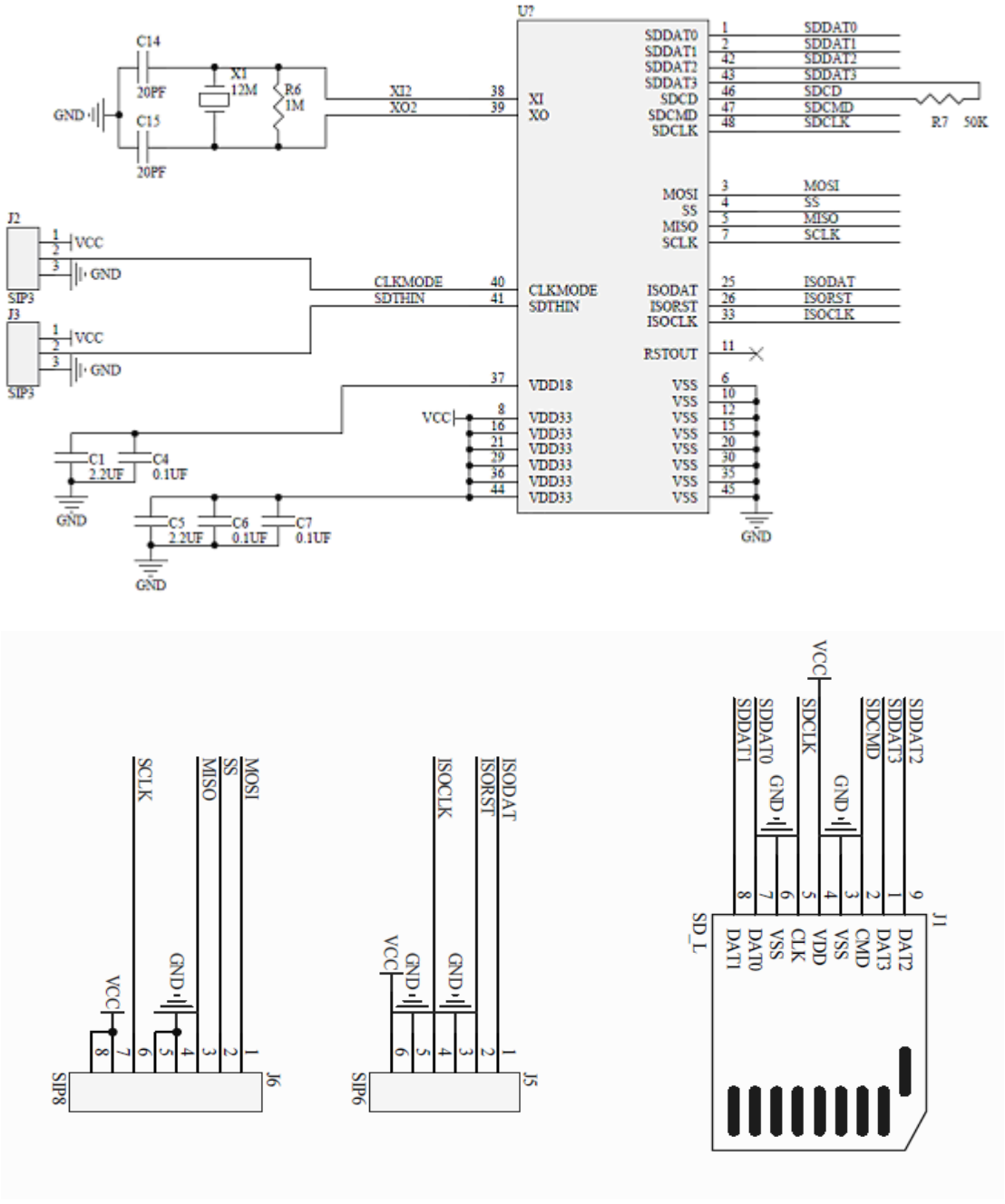


图 2-2 尺寸图示

表 2-1 尺寸说明

Symbol	Dimension in mm			Dimension in inch		
	Min	Nom	Max	Min	Nom	Max
A	—	—	1.60	—	—	0.063
A_1	0.05	—	0.15	0.002	—	0.006
A_2	1.35	1.40	1.45	0.053	0.055	0.057
b	0.17	0.22	0.27	0.007	0.009	0.011
b_1	0.17	0.20	0.23	0.007	0.008	0.009
c	0.09	—	0.20	0.004	—	0.008
c_1	0.09	—	0.16	0.004	—	0.006
D	9.00 BSC			0.354 BSC		
D_1	7.00 BSC			0.276 BSC		
E	9.00 BSC			0.354 BSC		
E_1	7.00 BSC			0.276 BSC		
e	0.50 BSC			0.020 BSC		
L	0.45	0.60	0.75	0.018	0.024	0.030
L_1	1.00 REF			0.039 REF		
R_1	0.08	—	—	0.003	—	—
R_2	0.08	—	0.20	0.003	—	0.008
S	0.20	—	—	0.008	—	—
θ	0°	3.5°	7°	0°	3.5°	7°
$θ_1$	0°	—	—	0°	—	—
$θ_2$	12°TYP			12°TYP		
$θ_3$	12°TYP			12°TYP		

2.2 电路连接参考



说明：

1） 电路中的 R7 只保留位置，不用焊接；

2） 建议用户同时支持 ISO7816 接口和 SPI 接口，SD 卡接口作为可选（通过 SDTHIN 管脚选择 SD 卡类型），用户根据需要决定是否引出；

3） 安全芯片 48pin，采用 LQFP 封装，面积为 7*7(mm^2)，图中未出现管脚不用；

4） 管脚 CLKMODE 不要悬空，接地时表示芯片采用内部晶振工作。

3 基本电气特性

以下是安全芯片基本的电气参数，仅供参考

3.1 额定参数

序号	参数	符号	值	单位
1	供电电压	V_{DD33}	-0.5 to +4.6	V
2	输入电压	V_{IN}	-0.5 to +6.0	V
3	单针瞬时最大电流限制	I_D	25	mA
4	工作温度范围	T_{OPT}	-40 to +85	^{O}C
5	储藏温度范围	T_{STG}	-25 to +125	^{O}C

说明：输入值必须为表中的额定值

3.2 ESD 保护参数

Parameter[1,2]	Symbol	Value	Units
ESD target for human body model	HBM	2000	V
ESD target for machine model	MM	200	V
HBM circuit description	R_{Series}	1500	W
	C	100	pF
MM circuit description	R_{Series}	0	W
	C	200	pF
Number of pulses per pin (HBM) Positive pulses Negative pulses	—	 3 3	—
Number of pulses per pin (HBM) Positive pulses Negative pulses	—	 3 3	—
Interval of pulses	—	1	Sec

说明：ESD 即静电放电，以上为测试值。

3.3 DC 电气参数

Parameter	Symbol	Min	Typical	Max	Unit
Supply Voltage	V_{DDH}	2.97	3.3	3.63	V
Input High Voltage	V_{IH}	2.0	—	5.5	V
Input Low Voltage	V_{IL}	-0.3	—	0.8	V
Threshold point	V_T	1.45	1.58	1.74	V
Schmitt trig. Low to High Threshold point	V_{T+}	1.44	1.50	1.56	V
Schmitt trig.High to Low Threshold point	V_{T-}	0.89	0.94	0.99	V
Output High Voltage	V_{OH}	2.4	—	—	V
Output Low Voltage	V_{OL}	—	—	0.4	V
Input Leakage Current	I_{IN}	—	—	±10	μA
Tri-state output Leakage Current	I_{OZ}	—	—	±10	μA
Pull-up Resistor	R_{PU}	39	65	116	kΩ
Low level output currernt @ V_{OL}=0.4V	I_{OL}	9.4	15.9	19.8	mA

3.4 VD 电气参数

Parameter	Symbol	Min	Max	Unit
Low-Voltage Detect Trip Voltage(V_{DD} falling) (LVCTR=0)	V_{LDV}	2.63	2.66	V
Low-Voltage Detect Trip Voltage(V_{DD} falling) (LVCTR=1)	V_{LDV}	2.80	2.83	V
Low-Voltage Detect Hysteresis(V_{DD} rising)	V_{LDV}	60	100	mV
High-Voltage Detect Trip Voltage(V_{DD} rising) (HVCTR=0)	V_{HDV}	3.89	3.91	V
High-Voltage Detect Trip Voltage(V_{DD} rising) (HVCTR=1)	V_{HDV}	3.73	3.75	V
High-Voltage Detect Hysteresis(V_{DD} falling)	V_{LDV}	60	100	mV

3.5 外部接口时序特性

(V_{DD} = 2.97V to 3.63 V, V_{SS} = 0V, T_A = T_L to T_H)

No.	Characteristic(1),(2)	Symbol	Min	Max	Unit
1	CLKOUT period	t_{cyc}	16	-	ns
2	CLKOUT low pulse width	t_{CLW}	$0.5t_{cyc}$-1	-	ns
3	CLKOUT high pulse width	t_{CHW}	$0.5t_{cyc}$-1		ns
4	All rise times	t_{CR}	-	2	ns
5	All fall times	t_{CF}	-	2	ns
6	CLKOUT high to A[22:0],$\overline{CS[1:0]}$, FCE,FALE, FCLE, R/$\overline{W}$ valid(3)	t_{CHAV}	-	4	ns
7	CLKOUT high to A[22:0], $\overline{CS[1:0]}$, FCE,FALE,FCLE R/$\overline{W}$ invalid	t_{CHAI}	0	-	ns
8	CLKOUT high to $\overline{OE}$,$\overline{EB}$,$\overline{FOE}$,$\overline{FWE}$ asserted(3)	t_{CHOEA}	$0.5t_{cyc}$	$0.5t_{cyc}$+4	ns
9	CLKOUT high to $\overline{OE}$,$\overline{EB}$ read, $\overline{FOE}$ negated	t_{CHOEN}	0	4	ns
9A	CLKOUT low to $\overline{FWE}$, $\overline{EB}$ write negated	t_{CLEN}	$0.5t_{cyc}$	$0.5t_{cyc}$ +3	ns
10	CLKOUT low to data-out valid write	t_{CLDOVW}	-	4	ns
11	CLKOUT high to data-out invalid write/show	t_{CHDOIW}	2	-	ns
12	Data-in valid to CLKOUT high read	t_{DIVCH}	9	-	ns

4 附录

4.1 接口使用简介

4.1.1 SPI 接口的使用

使用 SPI 接口工作（全双工）时，需要四根信号线，即两根数据线（MOSI 和 MISO）、时钟线（SCK）以及片选线（/SS)。其时序如图 4-1 所示，为方便起见，推荐用户在 SPI 通信主端优先采用模式 3。另外，与芯片 SPI 通讯不正常时，可从下面几个方面考虑：

- 硬件连接（包括管脚连接）和硬件设计是否影响信号传输；
- 软件上命令发送过程中是否加入了必要的延时；
- SPI 模式，低位在前还是高位在前；
- 发送和接收一个字节时片选要有由高到低再到高的过程；
- CLKMODE 接地表示使用片内晶振，一般用片内晶振；
- SDTHIN 接高电平，不要悬空；
- 通讯不稳定可能问题在于接地，多接几个 VSS；
- 芯片没有复位引脚，可采用重新上电的方式实现芯片的冷复位。

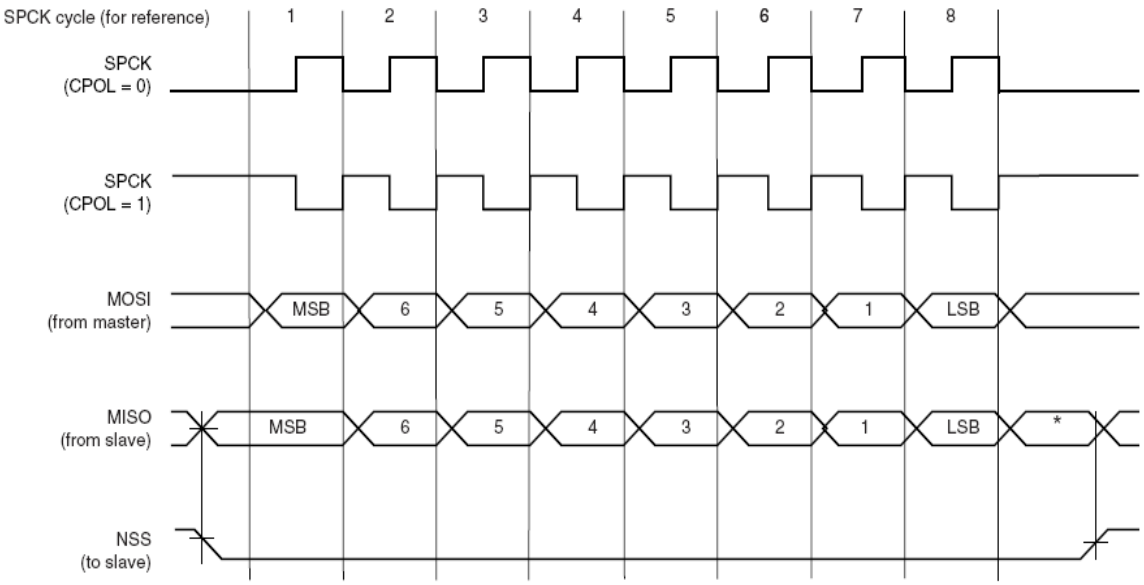


图 4-1 SPI 时序图示意

说明：

SPI 使用的时钟频率为 33MHz

CPOL — Clock Polarity Bit

CPHA — Clock Phase Bit

4.1.2 ISO7816 接口的使用

使用 ISO7816（USI）接口工作（半双工）时，需要三根信号线，即数据线（ISODAT）、时钟线（ISOCLK）以及复位线（ISORST)。

具体操作请参考 IEC/ISO7816-3 及 IEC/ISO7816-4 协议规范。

4.2 算法及接口性能参数

下面是系统时钟为 32MHz 时，密码学算法 DES、3DES、SM1、SM2、RSA 的性能以及接口 ISO7816、SPI 的性能的测试结果，仅供参考，其中为“公私密钥对生成”和“会话密钥协商”等环节提供随机数的随机数发生器的速度为 200K bytes/s。

表 4-1 DES 算法执行库时间性能表

运算		执行时间	测试次数
加密	ECB	10.67MB/s	10000 次
	CBC	10.67MB/s	10000 次
解密	ECB	10.67MB/s	10000 次
	CBC	10.67MB/s	10000 次

表 4-2 3DES 算法执行库时间性能表

运算		执行时间	测试次数
加密	ECB	4.59MB/s	10000 次
	CBC	4.59MB/s	10000 次
解密	ECB	4.59MB/s	10000 次
	CBC	4.59MB/s	10000 次

表 4-3 SM1 算法执行库时间性能表

运算		执行时间	测试次数
加密	ECB	3.38MB/s	10000 次
	CBC	3.38MB/s	10000 次
解密	ECB	3.38MB/s	10000 次
	CBC	3.38MB/s	10000 次

表 4-4 SM2-256 算法库时间性能表

运算	执行时间	测试次数
点乘	1.62 s/次以上	100
生成密钥	1.62 s/次	100
公钥运算	4.67 s/次	100
私钥运算	1.63 s/次	100
签名	2.34 s/次	100
验证	4.68 s/次	100

表 4-5 SM2-192 算法库时间性能表

运算	执行时间	测试次数
点乘	0.73 s/次以上	100
生成密钥	0.73 s/次	100
公钥运算	2.10 s/次	100
私钥运算	0.73 s/次	100
签名	1.05 s/次	100
验证	2.11 s/次	100

表 4-6 RSA-1024 算法库时间性能表

运算	执行时间	测试次数
生成密钥（公钥 17bit、私钥 1024bit）	1.62 s/次	100 次
生成密钥（公钥 1024bit、私钥 1024bit）	2.81 s/次	100 次
生成 CRT 密钥（公钥 17bit、私钥 1024bit）	1.82 s/次	100 次
生成 CRT 密钥（公钥 1024bit、私钥 1024bit）	2.92 s/次	100 次
私钥运算(非 CRT，私钥 1024bit)	11.6 次/s	100 次
公钥运算(非 CRT，公钥 17bit)	843 次/s	100 次
公钥运算(非 CRT，公钥 1024bit)	11.7 次/s	100 次
私钥运算(CRT，私钥 1024bit)	18 次/s	100 次
公钥运算(CRT，公钥 17bit)	803 次/s	100 次
公钥运算(CRT，公钥 1024bit)	11.7 次/s	100 次

表 4-7 ISO 7816 端口速度

读卡器输出频率	波特率因子	速度（K bytes）
3.59M	11.625	12.6
4.77M	11.625	16.7

表 4-8 SPI 端口速度

主设备输出频率	速度（K bytes）
10M	32.4
21M	69.6