华大电子

CIU96S192UFB 芯片数据手册

- 华大自主设计的 16 位 CIU96 核的 IC 安全芯片
- 代码和数据 MMU 存储管理单元
- 6K 字节 RAM，192K 字节 FLASH
- 灵活的中断机制，40 个中断源
- 硬件防 DPA 攻击 DES 协处理器
- 国产专用密码算法 SSF33 和 SM1（SCB2）
- 1024bit/2048bit 模乘协处理器
- 支持 USB2.0 协议低速和全速接口
- 支持 SPI 和 GPIO 接口
- 真随机数发生器
- 硬件 CRC 模块

[2009-10]

北京中电华大电子设计有限责任公司
CEC Huada Electronic Design Co.,Ltd.

处理器特性

- 华大自主研发的 CIU96 高安全 CPU 核
  - 16 位 CISC
  - 同时支持 8 位和 16 位运算方式，部分特殊操作支持 32 位运算方式
  - 哈佛结构：独立的数据和代码空间，可通过特殊指令按冯诺依曼结构访问整个存储空间
- 动态 MMU 管理：代码空间 MMU 和数据空间 MMU
- 可通过软件配置时钟系统
  - CPU 时钟可配置为 6MHz、12MHz 或 24MHz
  - 协处理器时钟可配置 24MHz 或 48MHz
- 灵活的中断机制
  - 中断例程的执行优先级与中断产生优先级分开
  - 40 个中断源，包括 7 个异常中断、16 个软陷阱中断、10 个事件中断和 7 个软件中断
- 支持存储器之间以及存储器与外设之间的 DMA 传输
- 两个 16Bit 的定时器（Timer）/计数器（Counter）
  - Timer 可对 CPU 时钟及其 4 分频、16 分频和 64 分频进行计数
  - 在 ISO7816 通讯模式下，Counter 可对 ISO 7816 ETU 时钟进行计数

片上存储器

- 6KB RAM
  - 支持字节和字访问
- 192KB FLASH（128KB FLASH0 + 64KB FLASH1）
  - Block 大小为 4K 字节
  - FLASH0 的 Sector 大小为 512B，FLASH1 的 Sector 大小为 64B
  - 字/字节编程时间：63us
  - Sector/Block 擦时间：1.33ms
  - 片擦时间：21.3ms
  - 擦写次数大于 10 万次，数据保持时间大于 10 年
  - 用户可在 192KB FLASH 空间灵活配置特殊安全算法下载区

通讯接口

- ISO7816 串口
  - 支持多种波特率，最高分频比为 31
  - 支持外部时钟 1～6MHz
- USB 接口
  - 支持 USB2.0 协议低速和全速
  - 支持五个端点，包括一个双向控制端点、两个 Bulk/Interrupt 输入端点和两个 Bulk/Interrupt 输出端点
  - 支持双 Buffer 功能
  - 支持内部软链接或外部上拉电阻

- 支持 SPI 接口
  - 作为 SPI 主设备，通信速度可达 4Mbps
- 20 路双向 GPIO，支持两个外部中断

电气特性

- 工作电流
  - ISO 7816 模式：动态功耗小于 30mA，Standby 状态和 Stop Clock 状态功耗均小于 3mA
  - USB 模式，动态功耗小于 40mA
- 工作电压
  - ISO7816 模式 2.7V～5.5V
  - USB 模式 4.0V～5.5V
- 工作温度
  - －40℃～85℃
- ESD 大于 4000V

安全特性

- 支持国产专用密码算法 SSF33
  - 硬件加解密处理时间 0.67us（CPU 频率 24MHz，不含数据装载）
- 支持国产专用密码算法 SM1（SCB2）
  - 硬件加解密处理时间 16.8us（CPU 频率 24MHz，SCB2 协处理器频率 48MHz，不含数据装载）
  - 支持 ECB、CBC、OFB 和 CFB 算法模式
  - 支持专用和通用 SCB2 算法
- DES 算法
  - 硬件加解密处理时间 0.67us（CPU 频率 24MHz，不含数据装载）
  - 支持硬件防 DPA 的 DES 加解密
  - 支持软件实现 3DES 加速功能
  - 支持 ECB 的加解密操作
- 支持 1024bit/2048bit RSA 算法，1024bit RSA 运算性能见表 1

表 1 1024bit RSA 运算速度

操作	运算速度
1024bit RSA 密钥对生成	2.11 秒/次
1024bit RSA 认证	168 次/秒
1024bit RSA 签名	21 次/秒

注：表 1 中数据测试条件为 CPU 工作频率 24MHz、模乘协处理器工作频率 48MHz

- 支持 192bit、256bit 国标 ECC 算法，性能见表 2

表 2 国标 ECC 算法运算速度

操作	192bit 曲线	256bit 曲线

国标 ECC 密钥对产生	2.79 次/秒	1.91 次/秒
国标 ECC 加密	1.22 次/秒	0.81 次/秒
国标 ECC 解密	1.85 次/秒	1.28 次/秒
国标 ECC 签名	3.17 次/秒	2.05 次/秒
国标 ECC 认证	1.72 次/秒	1.10 次/秒
国标 ECC 密钥交换出 8 字节密钥	0.94 次/秒	0.64 次/秒
国标 ECC 密钥交换出 16 字节密钥	0.94 次/秒	0.64 次/秒
国标 Hash 运算		14.3 次/秒

注 1：表 2 中数据测试条件为 CPU 工作频率 24MHz、模乘协处理器工作频率 48MHz
注 2：支持国家标准的 ECC 算法版本为 2006 年 12 月版
注 3：支持国家标准的 HASH 算法版本为 2006 年版

- 真随机数发生器
  - 符合国际 FIPS-140-2 随机数测试标准
- 硬件 CRC 模块
  - 遵循 ISO/IEC 13239 协议
  - 支持 8Bit 和 16Bit 操作
  - 支持 CRC 初值可任意配置
- 安全传感器探测保护单元
  - 高低电压检测
  - 高低频率检测
- 存储器加密机制
  - RAM 地址和数据加密
  - Flash 地址和数据加密
- 唯一芯片序列号

开发环境

- 集成开发环境，界面友好
- 可使用汇编和 C 语言混合编程
- 提供丰富 C 函数库

CIU96S192UFB 芯片硬件结构

CIU96S128UFB 芯片是一款支持多种安全算法的高性能安全芯片。采用华大自主研发的 16 位微处理器内核，具有执行速度快、支持高级语言和实时多任务执行等重要性能；适用于大容量 USBKEY 和智能卡领域；可以实现包括片上密钥管理、片上签名及身份认证及高速率的数据加解密等功能。

该芯片提供灵活的代码及数据存储器管理机制(MMU)，支持异常及事件等多种中断机制，存储器之间以及存储器与外设之间支持 DMA 传输。芯片支持软、硬多种复位方式，提供完善的时钟配置方案，并支持多种节电模式。芯片提供三种操作模式和两个堆栈空间的硬件防火墙机制，结合动态 MMU、RAM 地址和数据乱序功能，Flash 地址和数据加密功能以及高低压、高低频检测等功能，能够有效阻止外部对芯片的攻击、干扰。

该芯片支持 ISO7816、USB、、GPIO 和 SPI 接口，具有模乘协处理器、国产专用密码算法 SSF33 和 SM1（SCB2）协处理器、防 DPA 硬件 DES 协处理器、CRC、16 位 TIMER、M 序列和真随机数发生器（TRNG）。

芯片硬件系统结构如下：

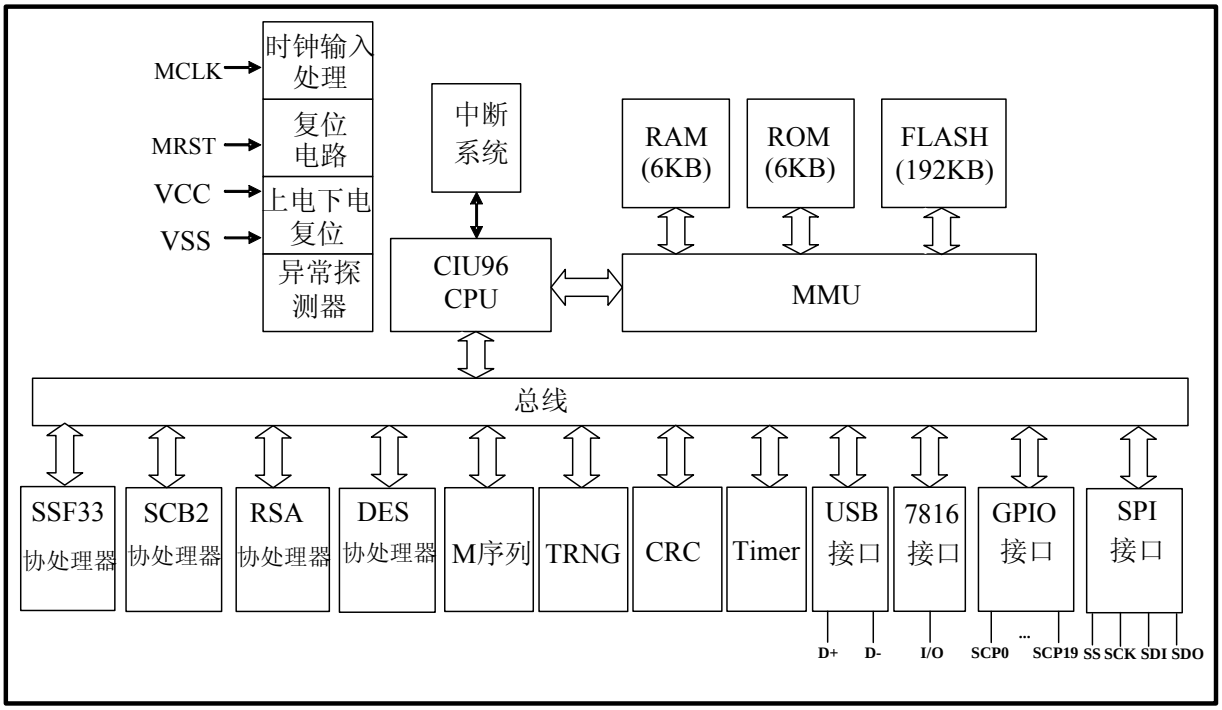

图 1 CIU96S192UFB 芯片系统结构

CIU96S192UFB 芯片封装说明

■ **LQFP44 封装**

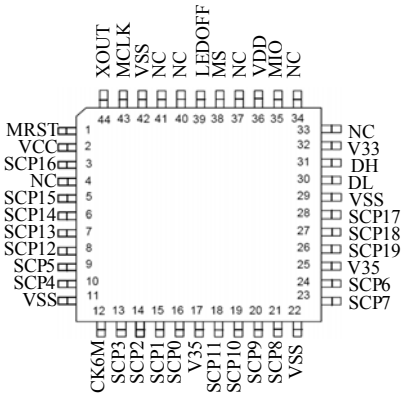

表 3 LQFP44 封装管脚说明

管脚编号	引脚名称	类型	说明
1	MRST	I	复位，缺省为高电平，内置与 VCC 连接的上拉电阻
2	VCC	P	主电源输入 ISO7816 工作模式下输入范围为 2.7~5.5V USB 工作模式下输入范围为 4.0~5.5V
3	SCP16	IO	通用通讯接口，SCP16，缺省为输入
4	NC		空
5	SCP15	IO	通用通讯接口，SCP15，缺省为输入
6	SCP14	IO	通用通讯接口，SCP14，缺省为输入
7	SCP13	IO	通用通讯接口，SCP13，缺省为输入
8	SCP12	IO	通用通讯接口，SCP12，缺省为输入
9	SCP5	IO	通用通讯接口，SCP5，缺省为输入
10	SCP4	IO	缺省为 SPI 通讯接口的 SDO（输出） 可配置为通用通讯接口，SCP4，此时缺省为输入
11	VSS	G	地
12	CK6M	I	时钟输入，内置下拉电阻
13	SCP3	IO	通用通讯接口，SCP3，缺省为输入
14	SCP2	IO	通用通讯接口，SCP2，缺省为输入
15	SCP1	IO	通用通讯接口，SCP1，缺省为输入
16	SCP0	IO	通用通讯接口，SCP0，缺省为输入

17	V35	P	管脚 3（SCP16）至管脚 28（SCP17）的电源输入，可接 2.7V～5.5V 电源，取决于管脚 3 至管脚 28 的外接器件的工作电压
18	SCP11	IO	通用通讯接口，SCP11，缺省为输入
19	SCP10	IO	通用通讯接口，SCP10，缺省为输入
20	SCP9	IO	通用通讯接口，SCP9，缺省为输入
21	SCP8	IO	通用通讯接口，SCP8，缺省为输入
22	VSS	G	地
23	SCP7	IO	缺省为 SPI 通讯接口的 SDI（输入） 可配置为通用通讯接口，SCP7，此时缺省为输入
24	SCP6	IO	缺省为 SPI 通讯接口的 SCK（时钟输出） 可配置为通用通讯接口，SCP6，此时缺省为输入
25	V35	P	管脚 3（SCP16）至管脚 28（SCP17）的电源输入，可接 2.7V～5.5V 电源，取决于管脚 3 至管脚 28 的外接器件的工作电压
26	SCP19	IO	通用通讯接口，SCP19，缺省为输入
27	SCP18	IO	通用通讯接口，SCP18，缺省为输入
28	SCP17	IO	通用通讯接口，SCP17，缺省为输入
29	VSS	G	地
30	DL	IO	USB D-
31	DH	IO	USB D+
32	V33	P	电源输出，3.3V
33	NC		空
34	NC		空
35	MIO	IO	ISO 7816 通讯接口，内置与 VCC 连接的上拉电阻（20KΩ）
36	VDD	P	电源输出，2.5V
37	NC		空
38	MS	I	芯片工作模式选择 ‘1’为 USB 模式，‘0’为 ISO 7816 模式； 缺省为 ISO 7816 模式，内置下拉电阻
39	LEDOFF	O	开漏输出，USB 通讯灯闪烁控制；导通为有效，关闭为无效；
40	NC		空
41	NC		空
42	VSS	G	地
43	MCLK	I	时钟输入
44	XOUT	O	时钟输出，与 MCLK 搭配用于外部晶振驱动

■ **SSOP20 封装**

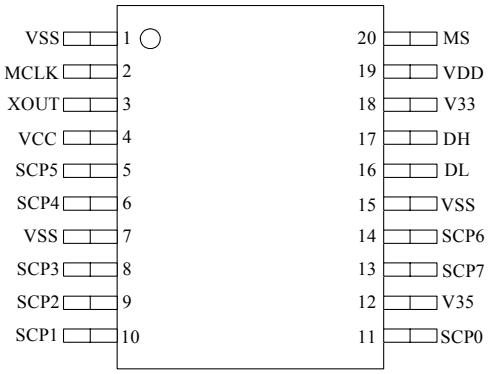

表 4 SSOP20 封装管脚说明

引脚编号	引脚名称	属性	说明
1	VSS	G	地
2	MCLK	I	时钟输入
3	XOUT	O	时钟输出，与 MCLK 搭配用于外部晶振驱动
4	VCC	P	主电源输入，ISO7816 模式输入范围 2.7V~5.5V，USB 模式的输入范围 4.0V~5.5V
5	SCP5	IO	通用通讯接口，SCP5，缺省为输入
6	SCP4	IO	缺省为 SPI 通讯接口的 SDO（输出） 可配置为通用通讯接口，SCP4，此时缺省为输入
7	VSS	G	地
8	SCP3	IO	通用通讯接口，SCP3，缺省为输入
9	SCP2	IO	通用通讯接口，SCP2，缺省为输入
10	SCP1	IO	通用通讯接口，SCP1，缺省为输入
11	SCP0	IO	通用通讯接口，SCP0，缺省为输入
12	V35	P	管脚 5（SCP5）~ 管脚 14（SCP6）的电源输入，可接 2.7V ~ 5.5V 电源，取决于管脚外接器件的工作电压
13	SCP7	IO	缺省为 SPI 通讯接口的 SDI（输入） 可配置为通用通讯接口，SCP7，此时缺省为输入
14	SCP6	IO	缺省为 SPI 通讯接口的 SCK（时钟输出） 可配置为通用通讯接口，SCP6，此时缺省为输入
15	VSS	G	地
16	DL	IO	USB D-

17	DH	IO	USB D+
18	V33	P	电源输出，3.3V
19	VDD	P	电源输出，2.5V
20	MS	I	芯片工作模式选择，‘1’为 USB 模式，‘0’为 ISO 7816 模式；缺省为 ISO 7816 模式；内置下拉电阻

- **ISO7816 智能卡封装**

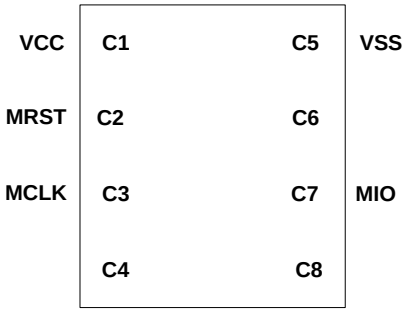

表 5 ISO7816 智能卡封装说明

管脚编号	管脚名称	属性	说明
C1	VCC	P	电源输入，2.7～5.5V
C2	MRST	I	ISO 7816 通讯接口复位输入
C3	MCLK	I	ISO 7816 通讯接口时钟输入
C5	VSS	G	地
C7	MIO	IO	ISO 7816 通讯接口数据端

CIU96S192UFB 芯片管脚电特性

表 6 绝对工作条件

符号	说明	条件	数值	单位
V_{CC}	工作电压	USB 工作模式	4.0～5.5	V
		ISO 7816 工作模式	2.7～5.5	
V_{IN}	输入电压		-0.3～V_{CC}+0.3	V
I_{CC}	工作电流	USB 工作模式	40	mA
		ISO 7816 工作模式	30	
T_A	工作温度		-40～85	℃
T_{STG}	存储温度		-65~150	℃

表 7 V_{CC}电特性

符号	说明	条件	最小	典型	最大	单位
V_{CC}	工作电压	ISO 7816 工作模式	2.7	5.0	5.5	V
		USB 工作模式	4.0	5.0	5.5	
I_{CC}	工作电流	ISO 7816 工作模式			30	mA
		USB 工作模式			40	
I_{RST}	复位电流	ISO 7816 工作模式，V_{CC}＝5V			2	mA
		USB工作模式，V_{CC}＝5V			2	
I_{SPD}	Suspend 电流	USB Suspend状态，V_{CC}＝5V			3	mA
I_{STD}	Standby 电流	ISO 7816 模式，Standby状态，V_{CC}＝5V			3	mA
I_{STP}	Stop Clock 电流	ISO 7816 模式，Stop Clock状态，V_{CC}＝5V			3	mA

表 8 V33 电特性

符号	说明	条件	最小	典型	最大	单位
V_{33}	工作电压	USB工作模式，V_{CC}＝5V	3.0	3.3	3.6	V
		USB 工作模式，Suspend状态，V_{CC}＝5V	3.0	3.3	3.6	
I_{33}	输出电流	USB工作模式，V_{CC}＝5V			20	mA
		USB工作模式，Suspend状态，V_{CC}＝5V			30	

表 9 VDD 电特性

符号	说明	条件	最小	典型	最大	单位
V_{DD}	工作电压	ISO 7816 工作模式，V_{CC}＝5V	2.25	2.5	2.75	V
		USB工作模式，V_{CC}＝5V	2.25	2.5	2.75	
		USB 工作模式，Suspend状态，V_{CC}＝5V	2.25	2.5	2.75	
I_{DD}	输出电流	ISO 7816 工作模式，V_{CC}＝5V			50	mA
		ISO 7816 工作模式，Standby状态，V_{CC}＝5V			70	
		ISO 7816 工作模式，Stop Clock状态，V_{CC}＝5V			70	
		USB工作模式，V_{CC}＝5V			40	
		USB工作模式，Suspend状态，V_{CC}＝5V			70	

表 10 V35 电特性

符号	说明	条件	最小	典型	最大	单位
V_{35}	工作电压	USB 工作模式	2.7	3.3	5.5	V
I_{35}	工作电流	USB工作模式，V_{35}＝3.3V			2	mA

表 11 MIO 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{CC}≤5.5V	0.7*V_{CC}		V_{CC}+0.3	V
V_{IL}	输入低电平电压	2.7V≤V_{CC}≤5.5V	-0.3		0.3*V_{CC}	V
I_{IH}	输入高电平电流	V_{CC}=5V	- 5		5	uA
		V_{CC}=3V	- 5		5	uA
I_{IL}	输入低电平电流	V_{CC}=5V	-242	- 291	-365	uA
		V_{CC}=3V	-145	-174	-219	uA
V_{OH}	输出高电平电压	外置上拉电阻 20KΩ			V_{CC}	V
V_{OL}	输出低电平电压	2.7V≤V_{CC}≤5.5V I_{OL}＝1mA	0		0.4	V
I_{OH}	输出高电平电流	V_{CC}=5V，V_{OH}＝4V		- 50		uA
		V_{CC}=3V，V_{OH}＝2.5V		- 25		
I_{OL}	输出低电平电流	V_{CC}=5V，V_{OL}＝0.4V		6.66		mA
		V_{CC}=3V，V_{OL}＝0.4V		5.35		

R_{PU}	上拉电阻		13.7K	17.2K	20.7K	Ω

表 12 MCLK 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{CC}≤5.5V	0.7 *V_{CC}		V_{CC}+0.3	V
V_{IL}	输入低电平电压	2.7V≤V_{CC}≤5.5V	-0.3		0.3*V_{CC}	V
I_{IH}	输入高电平电流	V_{CC}=5V	-5		5	uA
		V_{CC}=3V	-5		5	uA
I_{IL}	输入低电平电流	V_{CC}=5V	-5		5	uA
		V_{CC}=3V	-5		5	uA
F_{MCLK}	最大工作频率	V_{CC}=5V	1		16	MHz
		V_{CC}=3V	1		16	MHz

表 13 XOUT 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{CC}≤5.5V	0.7 *V_{CC}		V_{CC}+0.3	V
V_{IL}	输入低电平电压	2.7V≤V_{CC}≤5.5V	-0.3		0.3*V_{CC}	V
I_{IH}	输入高电平电流	V_{CC}=5V	-5		5	uA
I_{IL}	输入低电平电流	V_{CC}=5V	-5		5	uA
V_{OH}	输出高电平电压	2.7V≤V_{CC}≤5.5V	0.7 *V_{CC}		V_{CC}	V
V_{OL}	输出低电平电压	2.7V≤V_{CC}≤5.5V	0		0.3*V_{CC}	V
I_{OH}	输出高电平电流	V_{CC}=5V，V_{OH}=4V		-22.8		mA
		V_{CC}=3V，V_{OH}=2.5V		-12.1		
I_{OL}	输出低电平电流	V_{CC}=5V，V_{OL}=0.4V		13.4		mA
		V_{CC}=3V，V_{OL}=0.4V		11.4		

表 14 MRST 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤VCC≤5.5V	0.8 *V_{CC}		V_{CC}+0.3	V
V_{IL}	输入低电平电压	2.7V≤VCC≤5.5V	-0.3		0.12 *V_{CC}	V
V_{HIS}	回滞电压	4.5V≤V_{CC}≤5.5V		0.4		V
		2.7V≤V_{CC}≤3.3V		1.1		
I_{IH}	输入高电平电流	V_{CC}=5V	-5		5	uA
		V_{CC}=3V	-5		5	uA
I_{IL}	输入低电平电流	V_{CC}=5V	32	48	52	uA
		V_{CC}=3V	19	29	31	

R_{PU}	上拉电阻		96K	104K	157K	Ω

表 15 MS 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{CC}≤5.5V	0.7 *V_{CC}		V_{CC}+0.3	V
V_{IL}	输入低电平电压	2.7V≤V_{CC}≤5.5V	-0.3		0.3*V_{CC}	V
I_{IH}	输入高电平电流	V_{CC} =5V	242	291	365	uA
I_{IL}	输入低电平电流	2.7V≤V_{CC}≤5.5V	- 5		5	uA
R_{PD}	下拉电阻		13.7K	17.2K	20.7K	Ω

表 16 CK6M 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{35}≤5.5V	0.7 * V_{35}		V_{35}+0.3	V
V_{IL}	输入低电平电压	2.7V≤V_{35}≤5.5V	-0.3		0.3* V_{35}	V
I_{IH}	输入高电平电流	V_{35}=3.3V	159	192	241	uA
I_{IL}	输入低电平电流	2.7V≤V_{35}≤5.5V	- 5		5	uA
R_{PD}	下拉电阻		13.7K	17.2K	20.7K	Ω

表 17 LEDOFF 特性

符号	说明	条件	最小	典型	最大	单位
V_{CC}	工作电压	开漏输出状态	0		12.8	V
V_{OL}	输出低电平电压	2.7V≤V_{CC}≤5.5V I_{OL}=6mA			0.4	V
I_{OL}	输出低电平电流	V_{CC}=5V，V_{OL}＝0.4V		6.66		mA

表 18 DH、DL 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{CC}≤5.5V	2.0		-	V
V_{IL}	输入低电平电压	2.7V≤V_{CC}≤5.5V	-		0.8	V
I_{IH}	输入高电平电流	V_{CC}=5V	-5		5	uA
I_{IL}	输入低电平电流	V_{CC}=5V	-5		5	uA
V_{DI}	输入差分信号灵敏度		0.2		-	V
V_{CM}	输入共模电压范围		0.8		2.5	V
V_{CRS}	输出交叠电压		1.3		2.0	V
V_{OH}	输出高电平电压		2.8		3.6	V
V_{OL}	输出低电平电压		0		0.3	V

表 19 SCP19~SCP0 特性

符号	说明	条件	最小	典型	最大	单位
V_{IH}	输入高电平电压	2.7V≤V_{35}≤5.5V	0.7 * V_{35}		V_{35}+0.3	V
V_{IL}	输入低电平电压	2.7V≤V_{35}≤5.5V	-0.3		0.3* V_{35}	V
I_{IH}	输入高电平电流	2.7V≤V_{35}≤5.5V	- 5		5	uA
I_{IL}	输入低电平电流	V_{35}=3.3V	-31	-29	-19	uA
V_{OH}	输出高电平电压	V_{35}=3.3V，I_{OH}=-8mA	2.5		3.3	V
V_{OL}	输出低电平电压	V_{35}=3.3V，I_{OL}=8mA	0		0.4	V
I_{OH}	输出高电平电流	V_{35}=3.3V，V_{OH}＝2.5V		-14.1		mA
I_{OL}	输出低电平电流	V_{35}=3.3V，V_{OL}＝0.4V		25.7		mA
R_{PU}	上拉电阻		96K	104K	157K	Ω