产品简介

华大CIU98_A安全芯片

CIU98_A芯片采用55nm制造工艺，基于ARM 32位安全SC000核，320kB FLASH存储器，支持国际及国密码算法（DES/AES/ECC/RSA/SHA-n,SM1/SM2/SM3/SM4），支持多种接口：USB/ 7816/ SPI /UART/GPIO，面向金融、电子政务、IoT及嵌入式安全应用领域。

处理器	
CPU	ARM SC000
指令集	Thumb/Thumb2，大端模式
主频	48MHz@CPU 80MHz@PKE
MPU	支持，存储器分区保护
存储器	
FLASH	320KBytes
	10万擦写次数，10年数据保持
RAM	16KBytes
MPU	支持，存储器分区保护
接口	
USB	USB 2.0全速免外部晶振
主7816	一路主7816控制器，支持3组独立的智能卡读写器接口分时复用
从7816	一路从模式，支持T=0/1协议， 8～2048分频比
主SPI	支持Single/Dual/Quad模式，最高24MHz
从SPI	支持标准传输模式
UART	全双工，最高波特率115200bps
GPIO	21个（QFN32）
外设	
Timer	1个Systick Tmer，2个16/32位Timer
输入捕获	支持两路独立输入信号捕获
输出比较	支持单次和连续输出标准PWM输出
比较器	1个独立模拟比较器，一个差分比较器
电气特性	
工作电压	USB模式：3.6V～5.5V；
	其他模式： 2.7V～5.5V
工作温度	-25℃~85℃
功耗	工作电流<37mA
	Standby(状态保存)<135uA
	PowerDown（状态不保存）小于1uA
ESD	USB和7816：4kV， 其它:2kV

安全特性	
对称算法	支持DES/3DES/AES
	支持SM1/SM4国密算法
非对称算法	支持RSA(1024/2084)
	支持ECC(192/224/256/384)
	支持SM2（ Fp-256）
摘要算法	支持SHA-n（SHA1/256/384/512）
	支持SM3算法
随机数	真随机数，支持TRNG/PRNG，符合AIS31-P2标准
传感器	FD/VD/TD/LD/GD
有源屏蔽	支持
存储器安全	总线加密加扰，安全校验
唯一序列号	芯片唯一序列号不可更改
封装形式	
QFN32	尺寸：4.0 x 4.0 x 0.75mm
DFN10	尺寸：3.0 x 3.0 x 0.75mm
定制封装	支持
开发工具	
仿真器	硬件Emulator
Library	全套密码算法及应用函数库
应用领域	
一/二代KEY、蓝牙KEY	
物联网安全SE等领域	
资质证书	
商密二级证书	
EAL4+	
国家信息技术安全研究中心检测	