

# H88SXX 加密芯片

## 1、功能简介

恒森科技研发的 H88SXX 系列 CPU 加密芯片是集成了 FLASH 程序存储器，EEPROM 数据存储器 and ISO7816 通讯接口，并且引脚符合 ISO7816 标准的，CPU 加密功能的可靠的加密安全芯片，可广泛应用对主 MCU 的保护、数据辅助加解密、数据安全存取等功能。

该 CPU 加密安全芯片的 FLASH 程序存储器是让用户自行下载的，这样可保证用户的算法程序不会泄漏出去。更为优异的是：是否可重新下载 FLASH 由用户在建立文件系统的时候自己定义，这样就可实现一次性下载还是重复性下载。

H88SXX 加密芯片基本控制程序提供了 DES、3DES 加解密功能，同时负责用户文件系统的管理和用户自定义程序接口管理。

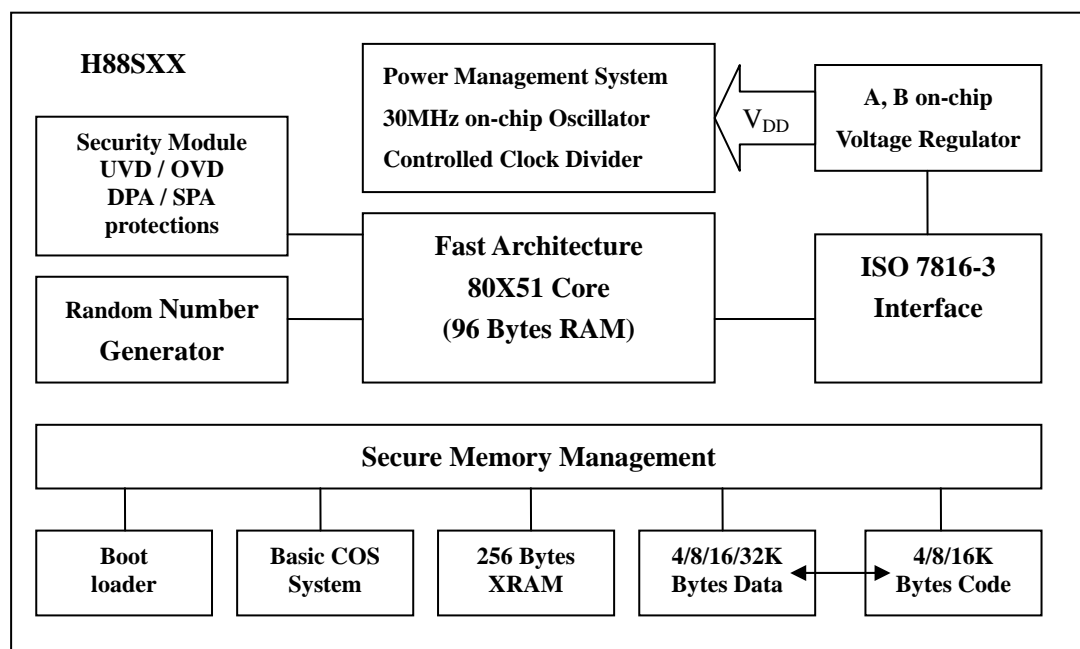
EEPROM 支持文件系统，用户可以自行建立文件系统来定义各个文件的读、写控制权限。数据文件支持二进制文件、定长记录文件、循环定长记录文件，且每个文件可自行设置不同的访问权限，比如每一个文件的在建立时可以任意设置成明文、密文、明文+MAC 或密文+MAC 的读取或更新模式，同时可以任意设定一个文件被访问时需要达到的安全权限。

用户自定义程序下载区可满足客户自定义算法的要求，更大程度上实现对主 MCU 的保护功能，同时可辅助处理相关功能。

## 2、H88SXX 系列加密芯片型号列表

型号	CODE 空间	EEPROM 空间	RAM 空间
H88S0004	0KBytes	4K Bytes	0
H88S0008	0KBytes	8KBytes	0
H88S0016	0KBytes	16KBytes	0
H88S0032	0KBytes	32KBytes	0
H88S0404	4KBytes	4KBytes	96+256Bytes
H88S0808	8KBytes	8KBytes	96+256Bytes
H88S1616	16KBytes	16KBytes	96+256Bytes

### 3、 芯片结构



### 4、 产品特性

- 工作电压：3.0~5.0V $\pm$ 10%
- 工作温度：-25~+85℃
- 外部时钟：1~8MHz
- 芯片内部主频：最大可达到 30MHz
- 精简指令集，极大地提高了芯片的执行效率
- 通讯速率可调，最高可支持 500KBps
- 数据保存期：10 年
- 数据擦写次数：10 万次
- 芯片支持休眠模式（100uA），降低功耗

- 提供 96 字节 RAM 及 256 字节 XRAM 供客户自定义算法调用。
- 芯片支持多种容量选择，可选择 4K、8K、16K、32K 字节的用户数据存储空间，及 4K、8K、16K 的用户自定义算法下载空间。
- 支持 Keil C 开发环境

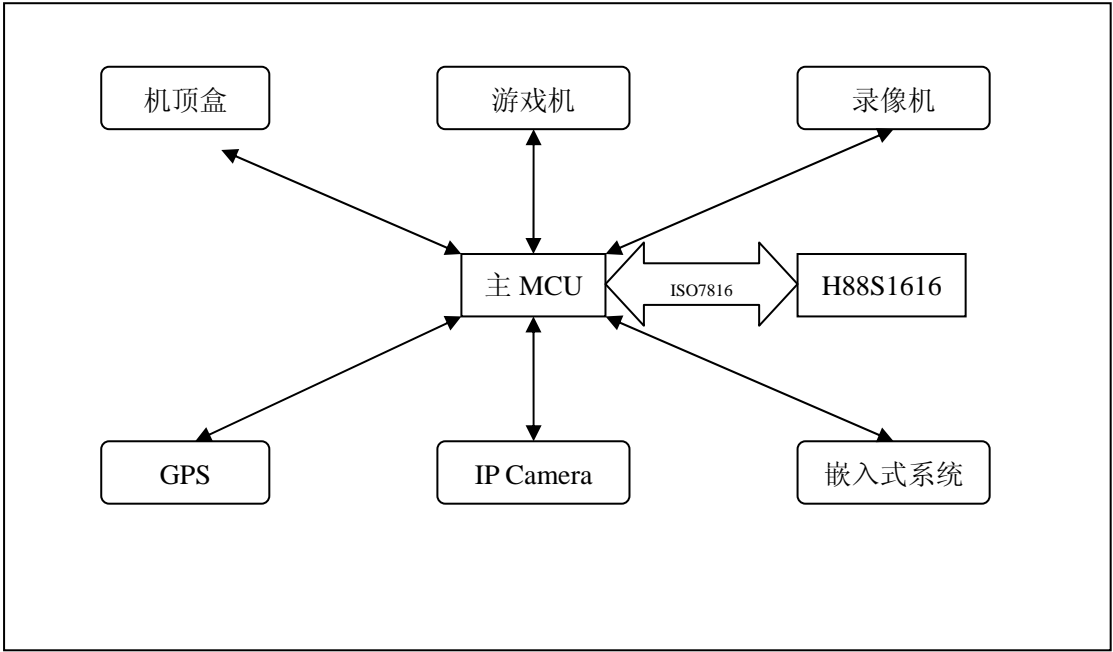
## 5、产品安全特性

- 用户空间支持文件系统，数据文件支持二进制文件、定长记录文件、循环定长记录文件，且每个文件可自行设置不同的访问权限。
- 支持 DES、Triple DES 等加密算法，并支持用户特有的安全加密算法的下载。
- 支持线路加密、线路保密功能，防止通信数据被非法窃取或篡改。
- 安全机制使用状态机，并支持 PIN 检验、KEY 认证、数据加密、解密、MAC 验证。
- 满足个别需求，H88SXX 可根据特殊行业的特殊用户的需求定制。
- 低电压保护，存储数据文件支持掉电保护功能。
- 采用了通过 EAL4+的智能卡芯片技术，最大程度保护了芯片自身的安全。
- 低频保护，防止静态分析
- 高频滤波防干扰

## 6、通讯协议

通讯协议符合 ISO7816-3 T=0 规范，最高可支持 500Kbps。

7、加密控制流程样例

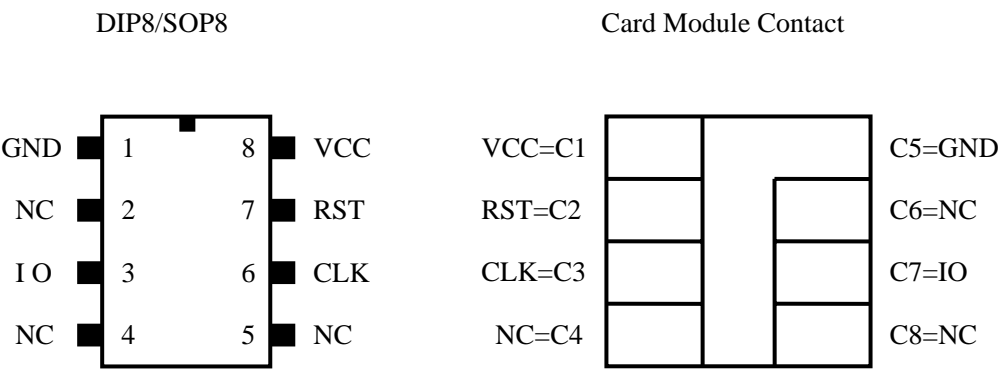


	MCU	ISO786-3 协议	H88SXX
外部 认证	①命令安全模块发送取随机数指令  ③用外部认证密钥加密 A 得到密文 A'  ⑤获取状态码	取随机数指令 ----->  返回随机数 A -----<  外部认证指令 ----->  -----<	②产生随机数 A    ④校验 A'并返回状态码 SW
内部 认证	①产生随机数 B  ③校验 B'	内部认证指令 ----->  返回 B' -----<	②用内部认证密钥加密 B 得到密文 B'并返回给 MCU
密文 校验 PIN	命令安全模块产生随机数 C  根据随机数 C, 由加密密钥得到加密过程密钥  使用加密过程密钥加密 PIN 得到 PIN 的密文 PIN'  获取状态码	取随机数指令 ----->  返回随机数 C -----<   Verify PIN ----->  -----<	产生随机数 C  根据随机数 C, 由加密密钥得到加密过程密钥  使用加密过程密钥解密 PIN'得到 PIN 的明文 PIN  校验 PIN, 并返回校验状态
明文 读	读取安全模块文件内容	读二进制/记录文件指令 ----->	判断该文件的访问条件, 如果满足, 读取文件内容

	得到文件明文数据 Data	返回明文数据 Data ←-----	得到明文数据 Data
密文 读	命令安全模块产生随机数 D	取随机数指令 -----→	产生随机数 D
	根据随机数 D，由应用维护密钥 加密随机数得到过程密钥	返回随机数 D ←-----	
	发送密文读取数据指令	密文读数据指令 -----→	根据随机数 D，由应用维护密钥加 密随机数得到过程密钥
	得到密文数据，使用过程密钥解 密密文数据 Data'得到明文数据 Data	返回密文数据 ←-----	使用过程密钥对要读取的数据 Data 加密得到数据密文数据 Data'
密文 更新	使用应用维护密钥加密数据 Data 得到密文数据 Data'并发送密文 写二进制/记录指令	密文写二进制/记录文件指令 -----→	使用应用维护密钥解密 Data'得到 文件明文数据 Data
	返回状态码	←-----	写入文件内容 Data
Call Patch	调用用户自定义代码功能  返回状态码	Call Patch 指令 -----→ ←-----	转入客户自由定义函数接口  执行自定义函数并返回结果

8、封装形式

- DIP8/SOP8/Card Module



管脚号	分配	管脚号	分配
1/C5	GND	5/C4	NC
2/C6	NC	6/C3	CLK
3/C7	I/O	7/C2	RST
4/C8	NC	8/C1	VCC