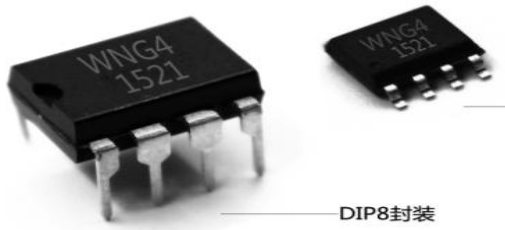
WNG
物理噪声源芯片

真随机数
经久不衰



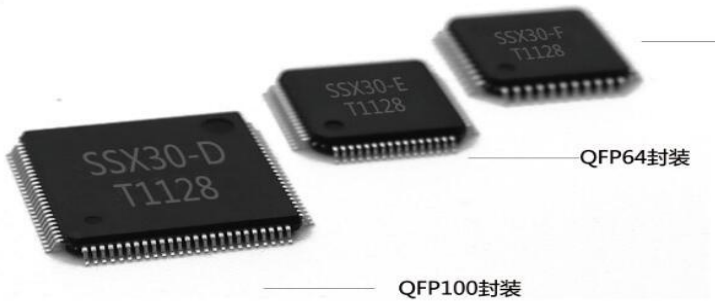
SOP8封装

DIP8封装

物理噪声源芯片WNG系列，用于产生真随机数序列，是信息安全及密码产品中不可缺少的基础部件，如：会话密钥、装置密钥的生成以及安全协议中的随机数、各种初始向量的设置等，都必须使用真随机序列，它们在通信、测量、声学等其它领域也有广泛用途。

SSX30
SM1专用算法芯片

SM1
高速



QFP44封装

QFP64封装

QFP100封装

- 可实现国家优选分组密码算法SM1和SM6密码算法
- 分组长度为128bit，密钥长度为128bit
- 具有ECB、CBC和OFB模式下的密码运算命令：ECB加/解密、CBC MAC、CBC加/解密、OFB乱数发生器
- 具有组包方式、命令方式两种操作方式
- SSX30-A/-D芯片具有单总线、双总线两种工作方式
- SSX30-A/-D内置4KB输入FIFO和4KB输出FIFO，均可缓冲存储256个分组的数据

获得国家密码管理局颁发的“商用密码产品型号证书”
2011年获省部级“密码科技进步二等奖”
国内最成熟的安全U盘方案
国内个人金融终端产品方案首选芯片

HS32U2
系统级安全芯片

32位
终端系列

LQFP80封装

LQFP44封装

HS32U2芯片是一款应用于加密终端的低功耗、低成本、高安全性、多功能的密码安全芯片。

- 采用CS320 IP核，高度优化的流水线
- 大容量片上存储器SRAM和FLASH，支持大容量COS开发
- 高安全性高性能硬件实现SM1、SM2、SSF33、RSA，AES/DES/TDES、SHA、TRNG等算法
- 片上密钥管理（包括密钥生成、密钥存储、密钥更新等）
- 支持USB高速/全速、HSPI/SPI、UART、EMI、ISO7816卡/读卡器接口等多种通讯接口，丰富的GPIO
- 支持外挂FLASH、SRAM存储器
- 适用于IC卡/SD卡/USBKEY/个人金融终端/身份认证/安全存储/读卡器

获得国家密码管理局颁发的“商用密码产品型号证书”
获得中国信息安全认证中心EAL4+认证

HSC08K1
系统级安全芯片

USB Key
主推

SOP20封装

SOP28封装

HSC08K1芯片是一款应用于USBKEY的低功耗、低成本、高安全性、多功能的密码安全芯片。

- 采用增强型8051 IP核，高度优化流水线
- 大容量片上存储器SRAM和FLASH
- 芯片内部硬件实现SM1、SM2、SM3、SM4、RSA、DES（TDES）、SHA、TRNG等算法
- 支持USB全速、SPI、UART等多种通讯接口
- 高安全抗DPA/SPA攻击、存储保护、主动屏蔽、电压频率温度检测等安全防护机制
- Wafer/DIE；SOP20；SOP28；QFN32 ；卷带；用户定制等封装形式
- 适用于IC卡/USBKEY/个人金融终端/身份认证/数据加密/读卡器

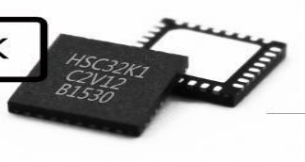
获得国家密码管理局颁发的“商用密码产品型号证书”
获得中国信息安全认证中心EAL4+认证

HSC32K1

系统级安全芯片

32位
超强优化

16K SRAM 32K



QFN32封装

HSC32K1芯片是一款应用于各类加密终端的低功耗、低成本、高安全性、多功能的密码安全芯片。

- 国产安全32位处理器CS320，具有存储保护功能
- 大容量片上存储器SRAM和FLASH，二次开发资源丰富
- 硬件实现SM1、SM2、SM3、SM4、SSF33、RSA，DES（TDES）、SHA、TRNG等算法
- 支持USB全速、SPI、UART、7816主接口等多种通讯接口，丰富的GPIO
- 高安全抗DPA/SPA攻击、存储保护、主动屏蔽、电压频率温度检测等安全防护机制
- Wafer/DIE；SOP20；SOP28；QFN32；QFN48；用户定制等封装形式
- 适用于SD卡/USBKEY/个人金融终端/身份认证/数据加密/读卡器/算法协处理器

获国家密码管理局颁发的“商用密码产品型号证书”
在国密局组织的专家评审会上获得“国际先进、国内领先”的高度评价
获得发改委“金融领域安全IC卡和密码应用专项”资金支持

HSM2-H1

SM2/SM3专用算法芯片

SM2/3
超高性能
首选

LQFP128封装

- SM2算法最高数字签名2.0万次/秒，SM2算法的数字签名验证1.0万次/秒
- SM3杂凑算法性能可达1.0Gbps。
- 支持SM2密钥对生成、数字签名、数字签名验证运算
- 支持在片外主控制器的调度下，实现SM2算法的密钥协商、数据加解密等运算
- 支持P域256位ECC算法
- 通信接口简单，32位数据总线宽度，具有与SRAM完全一样的访问接口
- 内置2KB的SM2数据缓存区和2KB的SM3数据缓存区
- 采取LQFP128封装形式

获国家密码管理局颁发的“商用密码产品型号证书”
在国密局组织的专家评审会上获得“国际先进、国内领先”的高度评价
获得发改委“金融领域安全IC卡和密码应用专项”资金支持

HSM4-H1

SM4专用算法芯片

SM4
超高性能
首选

LQFP128封装

- 在ECB模式双总线工作方式下加解密速率最高可达2.0Gbps。
- 在CBC模式双总线工作方式下加解密速率最高可达1.5Gbps。
- 支持ECB、CBC、OFB模式
- 内部高速流水线，使数据输入、运算、数据输出并行进行
- 通信接口简单，32位数据总线宽度，具有与SRAM完全一样的访问接口
- 具有单总线、双总线两种工作方式
- 内置4080Byte输入FIFO和4080Byte输出FIFO，可各缓冲存储255个分组的数据
- HSM4-H1采取LQFP128封装形式