

北京钐胜 科技有限公司

2024. 8





钊胜科技
QIAN SHENG KE JI



目录

C O N T E N T S

01

公司简介

Company profile

02

产品介绍

Product introduction





钊胜科技
QIAN SHENG KE JI

01

PART ONE 公司介绍



公司情况



Q I A N
S H E N G

成立：2022年5月

愿景：争做一流的数据加密领导企业

定位于集成电路与信息安全两大国家战略产业的融合

方向：安全芯片的应用开发及定制服务

产品：数据加解密及版权保护安全模组、加密存储UKey、高速加密MM卡以及密钥安全系统的定制开发服务



钊胜科技
QIAN SHENG KE JI

01

PART TWO 产品介绍



产品介绍-SE模组



SE模组是北京钐胜科技有限公司自主研发的一款安全模组，可以实现对称及非对称加解密运算、安全存储、身份认证等功能，广泛应用于物联网设备网络身份认证、网络应用授权访问、敏感数据的安全存储、通信数据流加解密等领域。同时可做为算法协处理器部件，应用于商用密码卡等安全模组中，降低软件开发复杂度。

功能特点

安全算法：

SM1/SM4/DES/3DES/AES128/AES 256对称算法

SM2/ECC/RSA(最高2048bit)非对称算法

SM3/SHA256杂凑算法

存储空间：

提供256KB敏感安全数据存储空间

支持密钥、证书的安全存储

擦写次数≥10万次，数据存储时间≥20年

定制功能：

支持唯一序列号（UID，可定制）

支持芯片封装、丝印定制

支持固件功能定制

产品参数

通讯接口	SPI接口；7816接口；UART接口
工作电压	2.0~5.5V
工作温度	-40℃~85℃
ESD	HBM ≥2KV
封装	DFN8

安全设计

电压异常检测单元、电源毛刺检测单元、频率异常检测单元、光照异常检测单元、温度异常检测单元、支持金属屏蔽保护、支持存储器数据加扰加密、高质量真随机数发生器、支持TLS安全连接建立，提供设备身份安全认证及联网通信密钥协商
支持计数功能，数到阈值后芯片功能指令全部失效

应用场景

物联网设备网络身份认证（建立安全TLS通信）
网络应用授权访问（UKey）
通信数据流加解密（如SM1等需要硬加密的场景）
版权保护、耗材认证
安全启动、安全下载



产品介绍-UKey



UKey系列是北京钤胜科技有限公司自主研发的一款具有高性能、高安全性的软件加密系列产品。采用32位国产安全芯片内核，内置32位加密操作系统，支持密钥协商、密钥生成、RSA、DES、SHA1等多种算法，既可用于文件数据的安全存储与管理，又可用于数据加解密处理。

功能特点

安全算法：

支持SM1、SM4、DES等对称算法

支持ECB、CBC 等多种对称加密模式

支持SM2、ECC素数域/二元域运算等非对称算法

支持密钥协商、密钥生成、签名、验签、加密、解密等非对称运算

支持SM3、SHA1 杂凑算法

安全特性：

支持CDK编译软件环境，具有丰富的系统调用和开发接口，支持多种数学运算

自主知识产权的加密COS系统

支持唯一序列号

具备两种不同原理的8路独立噪声源真随机数发生器，随机数生成速度可达20 Mbps

具备抗DPA、计时攻击、功耗分析的硬件保护电路

支持固件二次开发和非对称密码算法自定义

产品参数

工作电压	4.5~5.5V
工作温度	-20℃~75℃
数据空间	程序存储区 200KB
通讯方式	USB2.0全速模式

应用场景

上位机软件保护
财务软件版权保护
办公软件版权保护
设计软件版权保护
教育软件版权保护



产品介绍-MM卡

MM卡系列是北京钤胜科技有限公司遵循国家相关技术规范自主研发的一款系列高速MM模块。产品支持SM1、SM2、SM3、SM4等国密算法及DES、3DES、AES、RSA、SHA等国际算法，可满足应用系统数据加/解密、签名/验签等需求；并提供多线程、多进程的高速密码运算服务，保证传输信息的机密性、完整性和有效性；同时提供安全、完善的密钥管理机制。

性能参数

非对称密钥对存储	1024对
对称密钥对存储	1024个
SM1算法加解密速度	10Gbps
SM2密钥生成速度	160000对/秒
SM2签名速度	160000对/秒
SM2验签速度	55000次/秒
SM2加密速度	30000次/秒
SM2解密速度	40000 次/秒
SM3杂凑算法速度	15Gbps
SM4算法加解密速度	14Gbps
虚拟化	最大支持32个VF

产品特点

创新应用：适配多种国产操作系统
高安全：权威认证、算法芯片
高性能：主控芯片高性能



产品介绍-服务器MM机

服务器MM机系列产品是北京钤胜科技有限公司自主研发的采用创新软硬件平台、高性能MM卡，支持国密标准算法的安全设备。该系列产品采用严格的密钥管理和权限管理体制，提供完善的密钥备份恢复功能，支持多机热备、负载均衡功能，兼容适配银河麒麟等国产操作系统。可广泛应用于政府、电力、税务、公安、银行等对信息安全要求较高的单位，还可用作电子公文传输、电子签章、数据加解密平台等系统，为其提供高速加解密服务。

权限控制

高可用性

高性能

易用性

指标		参数
物理规格	规格	2U机架式
	处理器	飞腾D2000 8核 2.3GHz
	内存	16G
	密码卡	国家密码管理局批准的硬件芯片实现各类密码算法
	物理噪声源	国家密码管理局批准双物理噪声源生成随机数
	工作电源	标准服务器冗余电源
	网络接口	RJ-45 10/100/1000Mb * 2
	工作协议	TCP/IP
	平均无故障时间	50000小时
	工作温度	0℃-60℃
	工作湿度（非凝结）	5%-85%
	存储温度	-40℃-85℃
	存储湿度（非凝结）	5%-95%



感谢观看

—— 北京钤胜科技有限公司

