ET 金刚锁产品白皮书

坚石诚信科技股份有限公司

2010-9-14

ET 金刚锁是一款内置 32 位高强度，高性能，高稳定性智能卡芯片，和真硬件时钟芯片的高端加密锁产品。特别针对加密强度要求高，有计时保护需求的软件。ET 金刚锁采用高速 HID 无驱设计，功能强大，质量稳定，同类型产品价格最低，是广大软件加密厂商的首选。

ET 金刚锁提供 256K 超大用户使用空间，硬件支持 512/1024/2048 位 RSA、DES/3DES、SHA1、MD5 算法，具有超高性价比。通过锁内世界领先成熟的 C51 编程技术，保证加密后的软件无法破解。硬件时钟芯片日误差不超过 2 秒。同时，ET 金刚锁完全兼容 ET199 的所有应用。

产品特点:

- ET 金刚锁完全兼容 ET199 超级多功能锁的所有功能
- 32 位高强度智能卡安全芯片，硬件不可复制
- 256K 超大用户使用空间。是用户空间最大的加密锁产品
- 内置真硬件时钟芯片，提供独立的计时系统，不依赖计算机系统时间
- 硬时钟芯片最大误差每日不超过 2 秒。电池寿命 3 年以上，锁插在电脑上不耗电
- 安全硬件设计，杜绝一切篡改时钟芯片时间的非法手段
- USB 通讯硬件级加密，有效防止 USB 端口数据劫持，保证了传输数据的安全性
- 世界领先的锁内编程技术，使用成熟的 C51 语言开发
- 高强度外壳加密保护。支持 PE、.NET 程序及 PDF、Flash、视频等数据文件
- 硬件内部支持 512/1024/2048 位 RSA 非对称算法
- 硬件内部支持 DES/3DES 对称算法
- 硬件内部支持 MD5、SHA1 散列算法
- 硬件内部支持单/双精度浮点运算
- 安全远程升级
- 硬件擦写次数 10 万次，保存 10 年。读次数没有限制
- Windows、Linux、Mac 跨平台支持

同类比较:

	ET 金刚锁－32 位硬时钟芯片智能卡加密锁	其他厂家智能卡芯片加密锁
价格（硬时钟芯片产品）	35 元以下	50 元以上
性能提高 30％以上（执行 totest.c程序）	248ms	407ms
CPU 位数	32 位	16 位或以下
使用空间	256K 超大空间	64K 以内
时钟芯片	真硬件时钟芯片	标准版不具备硬件时钟芯片
时钟寿命	至少 3 年以上，插在电脑上不耗电	2 年
日误差	±2s	±20s
标准 RSA 算法	512/1024/2048 位	1024 位
复杂数学运算	单/双精度浮点数运算	不支持或单精度浮点数
驱动	HID 无驱产品，兼容所有 USB 鼠标可以正常使用的任何平台操作系统。	有驱产品，存在驱动安装失败，重启等众多问题

硬件参数:

核心芯片	32 位高强度智能卡安全芯片
真硬件时钟芯片	提供独立的计时系统，不依赖计算机系统时间。最大日误差 2 秒
硬件序列号	全球唯一 64 位（bit）硬件序列号
安全存储空间	256K 字节
硬件内置非对称算法	512/1024/2048 位 RSA 算法
硬件内置对称算法	DES/3DES
硬件内置散列算法	MD5、SHA1 散列算法
复杂数学运算	硬件内部支持单/双精度浮点运算
读次数	没有限制
写次数	至少 10 万次
USB 通讯	全系统兼容的高速 HID 无驱 USB 设备，USB1.1 标准设备，兼容 USB2.0 接口。通讯硬件级加密。

物理参数:

默认外壳	ABS 工程塑料
默认颜色	蓝白色
外壳尺寸	65×20×10（毫米）
重量	10 克
防水	防水浸泡 10 分钟
接口类型	USB A 类接头
工作温度	0℃～70℃
存放温度	－25℃～80℃
工作湿度	20%～80%
工作功率	0.5W（最大）
工作电压	5V
工作电流	100mA（最大）
数据保存年限	至少 10 年

安全性:

硬件核心	32 位高强度智能卡安全芯片，彻底杜绝硬件复制
真硬件时钟芯片	提供独立的计时系统，不依赖计算机系统时间。最大日误差不超过 2 秒
锁内硬件可编程	可使用成熟的 C51 语言开发锁内程序
USB 通讯	硬件级通讯加密，有效防止 USB 端口数据劫持，保证了传输数据的安全性
文件存储	可执行文件、密钥文件等机密文件不可导出，杜绝锁内算法泄漏
安全数据存储	智能卡硬件保证锁内数据安全存储
非对称加解密算法	硬件内部支持 512/1024/2048 位 RSA 非对称算法
对称加解密算法	硬件内部支持 DES/3DES 对称算法
散列算法	硬件内部支持 MD5、SHA1 散列算法
复杂数学运算	硬件内部支持单/双精度浮点运算
外壳加密	高强度外壳保护。支持 PE、VS.NET 程序及 PDF、Flash、视频等数据文件
远程升级	建立在 RSA 算法体系上的安全远程升级
全球唯一 ID	64 位（bit）
超大用户空间	256K

相关信息:

开发商口令（24 字节）	开发商在进行软件保护开发时使用到的，用于对 ET199 进行设置，如：创建文件/目录，删除文件/目录，设置客户号，设置 ATR 等。初始值为：“123456781234567812345678”。
用户口令（8 字节）	在程序中调用 ET199 中的可执行文件前，需要验证用户口令。初始值为：“12345678”。
口令权限和重试次数	ET199 中每个目录都有各自的开发商口令和用户口令。重试次数可以设置为 1～254 次，当设置为 0 或者 255 时表明没有重试次数限制。注意：当根目录开发商口令锁死后，没有任何办法能恢复，只能退回来重新生产。
客户号（4 字节）	通过种子机制产生，设置前需要验证根目录开发商口令。种子机制的优势：种子是由开发商自己设定的一串数据，其他人即使得到客户号，但不知道产生该客户号的种子，因此无法制作相同客户号的 ET199。
ATR（16 字节）	设置 ATR，设置前需要验证根目录开发商口令。
可执行文件	可执行文件是由 C51 语言编写的，在加密锁内部运行的文件。通过开发商口令验证后，在锁内创建，该文件不能被读取。杜绝锁内算法泄漏。
内部数据文件	存放数据信息的文件。该文件在开发商口令验证后，可以通过 API 接口写入。或者通过锁内可执行文件来读取和写入。
密钥文件	存储 RSA 密钥对（公钥和私钥）的文件。写入时需要验证开发商口令，公钥可以读取，私钥文件不能读取。杜绝锁内私钥泄漏。

产品外观: