利用CPU卡加密协处理器技术实现安全功能

PC 软件的盗版一直是困扰软件行业发展的主要问题，同样，在嵌入式应用领域，随着近年来黑客技术和芯片解剖技术的发展，嵌入式系统所面临的攻击也越来越多，因此，为解决这一问题开发的防抄板技术引起了产品设计者的重视。

产品设计者所面临的问题主要是黑客对产品的仿制，其目的是获得产品设计技术或者降低产品设计成本，攻击手段主要是抄袭产品设计者的线路板布线图和通过拷贝获得产品运行程序。

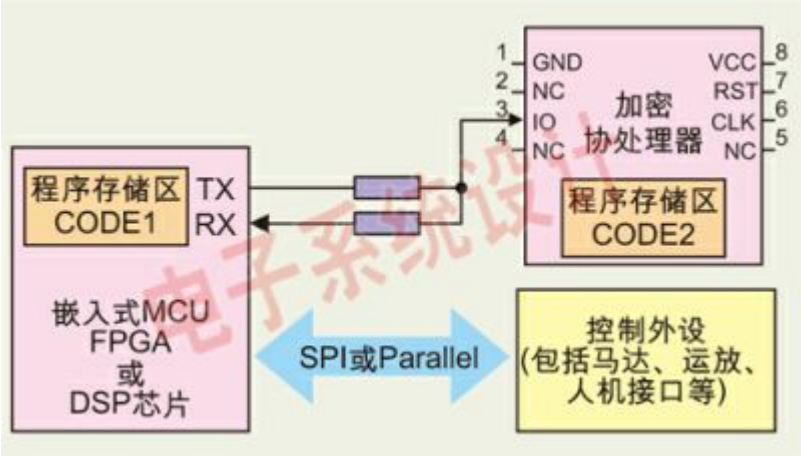
目前市场通用的 ARM、DSP、单片机通常安全防护手段很少，更多的程序暴露在透明的 Flash 或 EEPROM 中，面对不断发展的攻击技术以及黑客之间的竞争，产品的破解时间和成本越来越低，相对于产品仿制者获得的巨大利益，有时其破解成本甚至可以忽略不计。尤其在一些特殊行业，如游戏、消费电子行业，甚至出现了仿制产品大大多于自有产权产品的现象。因此，如何保护自身的利益，是产品设计者目前经常面对的问题，这也促进了嵌入式系统防抄板技术的发展。

在嵌入式系统中，更高的防护技术意味着更高的成本，但受到攻击的产品往往是产销量大的消费电子产品，为增加防护技术所增加的产品成本会削弱产品的价格竞争能力。市场上流行的防抄板安全技术及产品多属于低成本解决方案，下文将对这些主流方案进行探讨。

早期的口令认证防护技术：几年以前，产品设计者通常采用一个逻辑加密卡芯片来给产品定义唯一序列号或存储序列号，这种逻辑加密存储器必须通过口令认证后才能进行读写，这种防护技术面向黑客的示波器，口令和明文传输的数据可轻易被获得，防护技术已经完全失效和过时。

动态口令认证防护技术：为避免线路监控固定口令的缺陷，一些防护芯片采用动态口令技术，其基本原理是防护芯片和 MCU 内置相同的密钥和相同的对称算法，利用随机数作为通讯数据，MCU 通过判断防护芯片的计算结果正确与否来决定程序是否继续运行。这种产品和技术解决了认证过程线路监控的问题，但实际防护作用微乎其微。因为 MCU 本身没有硬件防护功能才选用防护芯片，而这种防护芯片的硬件安全性甚至不如 MCU,其内部存储的密钥可以很容易的被获取。更重要的一点是，MCU 在安全防护上仅仅实现了一个认证流程，可以很容易地被能够修改程序的黑客跳过。目前市场上这种芯片的销量虽然很大，但缺乏真正防护效果，实际上增加了产品设计者的成本。

动态口令认证＋数据存储技术：为解决仅需简单认证的问题，有些公司继续使用安全存储技术，防护芯片内置动态口令和认证算法，并具有数据存储功能。首先使用复杂的动态双向认证技术，获得存储器的读写权限，然后读写敏感的数据信息。这种防护芯片在硬件上具有一定的安全性，因此具有一些防护作用。但是 MCU 端的安全性并没有解决，黑客仍可以通过攻击 MCU 端的程序获取算法和密钥，通过认证后监控读写通道获取敏感数据，其安全性具有局限性。



采用 CPU 卡加密协处理器技术的功能示意图。

CPU 卡通用 COS 保护技术：CPU 卡在 SIM 领域和金融领域的广泛应用，使得其安全性得到了广泛的认知。金融应用以及 SIM 卡的巨大发卡量所带来的潜在安全风险，使 CPU 卡面临的安全挑战最大，因此 CPU 卡的硬件安全防护技术是比较全面的，而且在不断的升级，国际权威机构也有针对 CPU 卡的安全认证，其认证费用非常昂贵，因此 CPU 卡的设计和生产商往往是国际性的大公司，这也增加了人们对 CPU 卡的信任。

目前常用 CPU 卡的安全性体现在硬件和软件两个方面。CPU 卡的硬件设计增加了许多传感器，如高压和低压传感器、频率传感器、滤波器、光传感器、脉冲传感器、温度传感器等，这些传感器可以清晰地感觉到外部环境的变化，从而有效防止黑客利用改变硅片外部环境而诱导芯片误感应的半入侵攻击。为应对物理攻击，CPU 卡在芯片内部对存储器和总线系统进行加密，存储在芯片上的数据本身利用强大的密码算法进行加密，即使攻击者能够得到这些数据，也只能获得无用的信息。另一方面，采用有效的屏蔽网对攻击者构成有效的屏障。采用微米级的超细保护线来覆盖安全控制器。这些保护线被连续监控，如果出现短路、切断或损坏，就会启动报警。采用多层次的保护措施，就可以对控制器起到较好的保护作用，以免遭受物理攻击。此外，CPU 卡内部还具有真随机数发生器和硬件加密协处理器，以增加计算的安全性和速度。

除了 CPU 卡硬件安全性，CPU 卡还使用内部操作系统 COS 来实现数据的安全管理，如使用安全状态机来实现数据读写的权限管理，通过随机数认证机制获取存储器的权限，卡内存储的数据也可以使用密文或者动态密文的方式在线路传输，这些技术基本能够解决在防护芯片一端的数据安全性。

采用 CPU 卡进行防护已经成为一种领先技术，CPU 卡在 SIM 领域的巨量应用使得其成本也能够逐渐下降到被设计者接受的程度。

尽管 CPU 卡比较安全，但依然没有解决 MCU 一端的安全问题，对称算法的使用使得在 MCU 端依然会暴露算法和密钥，此外，对于 CPU 卡的使用者而言，COS 功能已经设计好，只能被动使用固定指令，功能扩展困难，而且第三方 COS 的资料是公开的，COS 本身的权威性和安全性也会受到人们的担心和质疑。

开放的 CPU 卡加密协处理器技术

CPU 卡实际上依然是一个单片机，尽管加载了各种安全技术，但它等同于一个迷你接口的安全单片机，针对 COS 厂商的软件开发人员而言，COS 编程等同于单片机开发，所使用的开发工具和编程语言与单片机甚至是相同的。因此，如果采用 CPU 卡作为主 MCU 的一个安全协处理器辅助 MCU 工作，使得一些重要程序或数据处理过程在 CPU 卡内部完成，将解决 MCU 一端的安全问题，同时 CPU 卡内部通常也具备很大的数据存储空间(20~120K 字节)，安全计算加大容量安全存储，大大提高了 CPU 卡应用的性价比。

但对于单片机工程师而言，编写 COS 或者与 CPU 卡进行通讯的过程中，面临的最大困扰是复杂的 ISO7816 协议，同时还要熟悉 CPU 卡内部的结构，为解决这个问题，有的 CPU 卡内部预置了固件，将 ISO7816 协议变成普通的串口协议，同时通过调用固件，可以轻松完成对 CPU 卡内部资源的管理，这样工程师就能够像针对单片机编程一样轻松自如地对安全单片机进行编程了。

开放的 CPU 卡加密协处理器技术相对于传统的认证技术具有极大的优势，依托安全的 CPU 卡硬件平台作为安全协处理器，设计工程师可以在安全协处理器内部自如地实现自己的设计思路，而不受第三方 COS 的制约，从而将设计思想和敏感数据完全控制在自己手中。

北京宝兴达信息技术有限公司日前开发的新兴产品 ESPU0808 已经引起了人们的兴趣，在很多领域得到了成功应用，例如在游戏机内部，使用 ESPU0808 来计算人机博弈的中奖概率，在安防、IC 卡消费、智能门锁等领域，利用 ESPU0808 对正常用户和黑名单进行管理，这项技术不仅增加了算法的安全性，同时减少了主 MCU 的负担。

不过，使用这项技术依然有一些问题需要考虑，在 CPU 卡加密协处理器内部运行的程序应具有很好的随机性，简单的程序和过少的数据交互会增加黑客的攻击机会。

随着技术的进步，防抄板技术也在不断地发展，以对抗不断增强的黑客攻击手段。