芯片加密建议

1、概述

在该说明文档中会讲述目前(2015.12.30)正在使用或者已知的一些加解密技术作为开发者加密建议，其实我们只是想表述一种思想、方法和简单的建议，更多的还是开发者自己去完成，不然加密方式千篇一律，其意义也不是很大；另外由于加解密技术会随着时间的推移而更加的多样化，所以列举的加解密方法会受实时影响，希望开发者能够理解。

首先要明确一个概念，采用更多的或更先进的加密手段，只能提高解密难度，但是不能绝对杜绝芯片被解密。随着芯片逆向技术的提高，做芯片解密研究的投入也在增加，总能找到办法解密芯片，没有绝对安全的加密手段。所以在做一个产品的时候，保密安全性是一个因素，但最为重要的还是产品的功能，所以不能因为加密而使设计提高了较大难度,从而影响了设备本身的功能。芯片加解密的最重要原则就是，**尽量做到解密成本大于开发成本**，这样解密也就没有价值和意义。

2、解密技术

这里讲解密技术不是为了普及解密方法，我们是要做到知己知彼，才能百战不殆，保住自己的劳动成果。以下会列举一些已知的解密方法，其实这些东西在网上或者专门做解密芯片的门户网站上也能有简单的说明，我们只要了解其使用方法，然后有针对性的做好加密工作。

单片机（Microcontroller）一般都有内部 ROM/EEPROM/FLASH 供用户存放程序。为了防止未经授权访问或拷贝单片机的机内程序，大部分单片机都带有加密锁定位或者加密字节，以保护片内程序。如果在编程时加密锁定位被使能（锁定），就无法用普通编程器直接读取单片机内的程序，这就是所谓拷贝保护或者说锁定功能。

目前，攻击单片机主要有四种技术，分别是：

(1)、软件攻击

该技术通常使用处理器通信接口并利用协议、加密算法的安全漏洞来进行攻击。软件攻击者利用单片机擦除操作时序设计上的漏洞，使用自编程序在擦除加密锁定位后，停止下一步擦除片内程序存储器数据的操作，从而使加过密的单片机变成没加密的单片机，然后利用编程器读出片内程序。

(2)、电子探测攻击

该技术通常以高时间分辨率来监控处理器在正常操作时所有电源和接口连接的模拟特性，并通过监控它的电磁辐射特性来实施攻击。因为单片机是一个活动的电子器件，当它执行不同的指令时，对应的电源功率消耗也相应变化。这样通过使用特殊的电子测量仪器和数学统计方法分析和检测这些变化，即可获取单片机中的特定关键信息。

(3)、过错产生技术

该技术使用异常工作条件来使处理器出错，然后提供额外的访问来进行攻击。使用最广泛的过错产生攻击手段包括电压冲击和时钟冲击。低电压和高电压攻击可用来禁止保护电路工作或强制处理器执行错误操作。时钟瞬态跳变也会复位保护电路而不会破坏受保护信息。电源和时钟瞬态跳变可以在某些处理器中影响单条指令的解码和执行。

(4)、探针技术

该技术是直接暴露芯片内部连线，然后观察、操控、干扰单片机以达到攻击目的。

为了方便起见，人们将以上四种攻击技术分成两类，一类是侵入型攻击（物理攻击），这类攻击需要破坏封装，然后借助半导体测试设备、显微镜和微定位器，在专门的实验室花上几小时甚至几周时间才能完成。所有的微探针技术都属于侵入型攻击。另外三种方法属于非侵入型攻击，被攻击的单片机不会被物理损坏。在某些场合非侵入型攻击是特别危险的，这是因为非侵入型攻击所需设备通常可以自制和升级，因此非常廉价。

大部分非侵入型攻击需要攻击者具备良好的处理器知识和软件知识。与之相反，侵入型的探针攻击则不需要太多的初始知识，而且通常可用一整套相似的技术对付宽范围的产品。因此，对单片机的

攻击往往从侵入型的反向工程开始，积累的经验有助于开发更加廉价和快速的非侵入型攻击技术。

侵入型攻击的第一步是揭去芯片封装。有两种方法可以达到这一目的：第一种是完全溶解掉芯片封装，暴露金属连线。第二种是只移掉硅核上面的塑料封装。第一种方法需要将芯片绑定到测试夹具上，借助绑定台来操作。第二种方法除了需要具备攻击者一定的知识和必要的技能外，还需要个人的智慧和耐心，但操作起来相对比较方便。

3、单片机加密建议

任何一款单片机从理论上讲，攻击者均可利用足够的投资和时间使用以上方法来攻破。所以，在用单片机做加密认证或设计系统时，应尽量加大攻击者的攻击成本和所耗费的时间。这是系统设计者应该始终牢记的基本原则。

单片机程序加密主要涉及到几个方面：①防止单片机内部程序（HEX/BIN）被读出 ②防止单片机内部程序被读出后能直接使用 ③防止 HEX/BIN 被反编译（难度较大）；因此给出以下几点建议：

3.1.选型建议

(1)、在选定加密芯片前，要充分调研，了解单片机破解技术的新进展，包括哪些单片机是已经确认可以破解的。尽量不选用已可破解或同系列、同型号的芯片。

(2)、产品的原创者，一般具有产量大的特点，所以可选用比较生僻、偏冷门的单片机来加大仿冒者采购的难度。

(3)、选择采用新工艺、新结构、上市时间较短的单片机。

(4)、在设计成本许可的条件下，应选用具有硬件自毁功能的智能卡芯片，以有效对付物理攻击。

为了保护开发者的劳动成果，对于 CH55X 系列单片机我们提供芯片硬件保护，开启后 Code 无法被读出，此外对于我们非常愿意与客户进行芯片代码保护的探讨。

3.2.硬件设计建议

(1)、让原芯片厂家将芯片的封装脚位全部调换；

(2)、将 CH55X 的印字印为 XXXX 等，打磨掉芯片型号等信息或者重新印上其它的型号，以假乱真；

(3)、用环氧树脂+酶（xxx 酶：可增加硬度，如将其弄开后芯片就报废了）将测试好的线路板密封上；

(4)、使用裸片来做产品；

(6)、将部分端口用大电流熔断；

(7)、使用四层板（故意多走一些线）；PCB 板上设置一些陷阱，比如给单片机经过一个烧断的二极管或电阻提供高压电源，如果仿制，上电就烧坏芯片；

(8)、如果条件许可，可采用两片不同型号单片机互为备份，相互验证，从而增加破解成本。CH55X 系列的单片机，根据我们公司的实际情况，如果客户满足一定的条件，我们也可以提供比如重新封装芯片、芯片磨字、更换封装材料、提供裸片等服务。

3.3.软件设计建议

(1)、在使用芯片的时候，使用芯片的 ID 功能，当解密以后把代码写到别的芯片里去，由于芯片的 ID 不同就不能工作；

(2)、使用 ISP 软件生成并烧录唯一密钥到单片机特定区域再烧录程序时需核对密钥等；另外可以将芯片本身具有的加密功能都击活；

(3)、设置密码文件，要想读出程序，必须有密码文件才可以，如果在读程序的时候，如果输入的密码错误就自动清除 FLASH 存储器；

(4)、在芯片的程序里加入芯片保护程序，如 XX 脚有电压输入时就将所有芯片的内容清除；

(5)、用 ISP 软件实现对程序的加密（防止终端用户接触 HEX，程序绑定单片机）：ISP 软件可以生成基于电脑的可执行文件，此文件内部包含升级代码，打开后直接连上产品就能升级，终端用户不会接触到升级代码。此软件可以锁定硬盘号，实行定向安装，保密性较好；

(6)、其他；