单片机加密方法—保护自己的科研成果!

广州双龙电子　耿德根

单片机加密方法:(1)

科研成果保护是每一个科研人员最关心的事情,目的不使自己的辛苦劳动付注东流。加密方法有软件加密,硬件加密,软硬件综合加密, 时间加密,错误引导加密,专利保护等措施。有矛就有盾,有盾就有矛,有矛、有盾,才促进矛、盾质量水平的提高。加密只讲盾,也希望网友提供更新的加密思路。

现先讲一个软件加密:利用 MCS-51 中 A5 指令加密,(本人 85 年发现的,名软件陷阱),其实世界上所有资料,包括英文资料都没有讲这条指令,其实这是很好的加密指令。 A5 功能是二字节空操作指令。加密方法在 A5 后加一个二字节或三字节操作码,因为所有反汇编软件都不会反汇编 A5 指令,造成正常程序反汇编乱套,执行程序无问题。仿制者就不能改变你的源程序,你应在程序区写上你的大名、单位、开发时间及仿制必究的说法,以备获得法律保护。我曾抓到过一位“获省优产品”仿制者,我说你们为什么把我的名字也写到你的产品中?

硬件加密:8031/8052 单片机就是8031/8052掩模产品中的不合格产品,内部有 ROM(本人 85年发现的),可以把 8031/8052 当 8751/8752 来用,再扩展外部程序器,然后调用 8031 内部子程序。当然你所选的同批 8031 芯片的首地址及所需用的中断入口均应转到外部程序区。

单片机加密方法:(2)

各位,我在这里公开场合讲加密,有的只能讲思路,有的要去实验,要联想,要综合应用各种方法,甚至有的不能言传,只能意会。因为这里有的造矛者也在看我们如何造盾,当然,我们也要去看人家怎样造矛,目前国内、外最高造矛的水平怎样。“知已知彼,才能百战百胜”。

硬件加密: 使他人不能读你的程序

① 用高电压或激光烧断某条引脚,使其读不到内部程序,用高电压会造成一些器件损坏。

② 重要 RAM 数据采用电池(大电容,街机采用的办法)保护,拔出芯片数据失去。机器不能起动,或能初始化,但不能运行。

用真真假假方法加密:

① 擦除芯片标识。

② 把 8X52 单片机,标成 8X51 单片机,并用到后 128B 的 RAM 等方法,把 AT90S8252 当 AT89C52,初始化后程序段中并用到 EEPROM 内容,你再去联想吧!

③ 用激光(或丝印)打上其它标识。如有的单片机引脚兼容,有的又不是同一种单片机,可张冠李戴,只能意会了,这要求你知识面广一点。

④ 用最新出厂编号的单片机,如 2000 年后的 AT89C 就难解密,或新的单片机品种,如 AVR 单片机。

⑤ DIP 封装改成 PLCC,TQFP,SOIC,BGA 等封装。

⑥ 如果量大可以做定制 ASIC,或软封装。

⑦ 用不需外晶振的单片机工作(如 AVR 单片机中的 AT90S1200)。

⑧ 使用更复杂的单片机 FPGA+AVR+SRAM=AT40K 系列。

单片机加密方法:(3)

硬件加密与软件加密只是为叙说方便而分开来讲, 其实它们是分不开的,互相支撑,互相依存的。

软件加密:其目的是不让人读懂你的程序,不能修改程序,你可以.....

① 利用单片机未公开,未被利用的标志位或单元,作为软件标志位,如 8031/8051 有一个用户标志位,PSW.1 位,是可以利用的。

② 程序入口地址不要用整地址,如:XX00H,XXX0H,可用整地址-1,或-2,而在整地址处加二字节或三字节操作码。

③ 在无程序的空单元也加上程序机器码,最好要加巧妙一点。

④ 用大容量芯片,用市场上仿真器不能仿真的芯片,如内部程序为 64KB 或大于 64KB 的器件,如:AVR 单片机中 ATmega103 的 Flash 程序存储器为 128KB。

⑤ AT89S8252/AT89S53 中有 EEPROM,关键数据存放在 EEPROM 中,或程序初始化时把密码写到 EEPROM 中,程序执行时再查密码正确与否,然后.....。当然不能告说人家这是什么器件,尽量不让人家读懂程序,在这里说谎,骗人是正当防卫。

⑥ 用“真真假假,假假真真”,把几种不同品种的单片机放在同一设备中,如主芯片用 AVR(说是 MCS51),键盘显示用 AT89C2051(说是 GAL),I/O 口扩展驱动用 PIC(说是 AT90S1200)等,当然要求你知识面广一点。如果你用高级语言 C 编写程序就简单了,因为 C 语言程序移植方便。

⑦ 有些国家的产品能做到三年保修,三年保不坏,三年后保坏,或三年后保有故障,可能用什么技术?你去想吧。例:每次开机或关机,EEPROM 某单元加 1,也可二个、三个单元连接起来计数,达到某值停止工作。

⑧ 硬件用软件代替,软件用硬件代替。用大规模 CPLD 可编程器件。

关于单片机加密,讲到这里,就算抛砖引玉,下面请各位高手把玉亮出来吧。

对付购买你设备,想不付钱或想少付钱的人,你可采用先供限时(次)使用版软件,钱付清下载正式版软件(监控)!

于 2001/7/13 修订(今日中国申奥成功!)