# 使用 RF2148 实现烧断管脚的加密方法

**前言：**

现在普通的 AT89C5X/X051 单片机解密价格已经很便宜了，几百元几个小时就可以搞定了，辛苦开发的程序就这样被人家盗用了，这种情况下可以换型号，但有些情况下，换用后的兼容性没有以前好了，那你可以考虑烧断单片机的管脚（有时候称非恢复加密）来加密，这种方式对一般的单片机破解者无法破解，当然对高手照样可以破解，但是增加了费用和时间，甚至不能解密或破解。

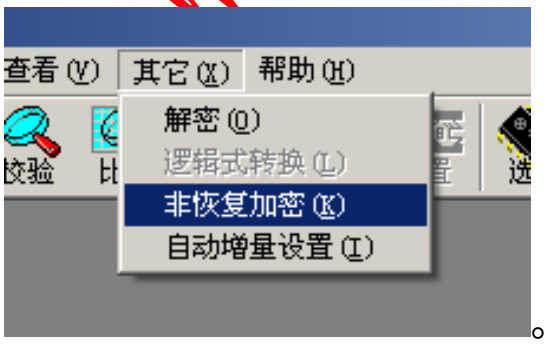
**正文：**

下面我们根据 RF2148 的说明书并根据我公加密解密的经验，讲讲如何使用 RF2148 来烧断 AT89C5X/X051 的管脚。

烧断单片机的管脚（有时候称非恢复加密）加密有 2 种方式：

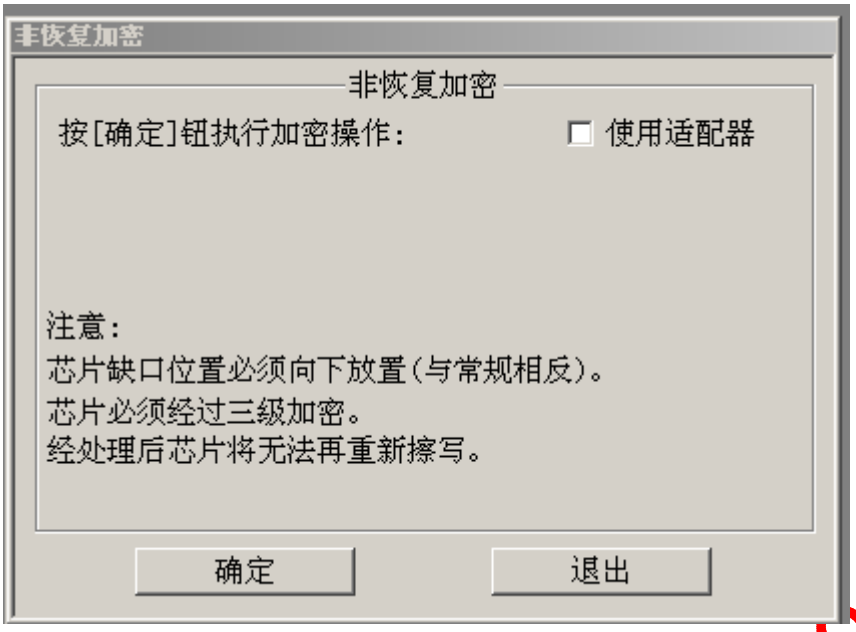
不使用适配器方式：（FR3148 无此方式）

对 AT89C5X 进行 OTP 非恢复加密，不使用适配器。将已经烧好程序、验证通过并且已经经过 3 级加密的芯片反方向（芯片缺口远离锁紧手柄，必须这样放，否则会损害芯片）放置于编程器锁紧座上，联后点击其他->非恢复加密，




。

联后弹出窗口：




点确认，这样就实现了烧断管脚的加密。

注意：芯片必须经过 3 级加密，必须芯片反方向放置（否则会损害芯片，我们试验过，11 脚将损害）。烧断管脚加密（OTP 非恢复加密）后，芯片将不能查擦除、改写。但是 OTP 加密后芯片不破坏数据总线，不影响扩展功能。

这种烧断加密后，芯片的 31 脚被烧断，但是建议使用中该脚接 VDD，这样芯片工作稳定性能好。

另外注意的是，这种加密只适用于该芯片使用片内存储空间，使用片外的请不要使用该加密方式。

**使用适配器方式：**

如使用 K51 加密适配器，则既可对 AT89C5X 芯片进行 OTP 非恢复加密，还可以对 AT89C5X 芯片的数据 P0.0-P0.7 或 AT89CX051 的数据线 P1.2-P1.7 中空闲不用的引脚予以破坏，进一步加强加密强度，甚至无法解密。破坏后的引脚不能正常使用。

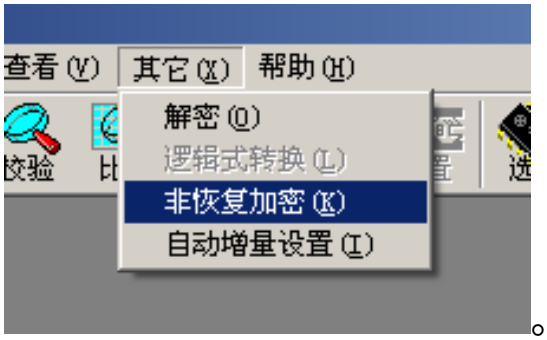
使用 K51 加密适配器的方法是：将 K51 加密适配器放置于编程器主机

上。选择加密操作的类型，有两种加密供选择：

1 非恢复 （OTP）加密。

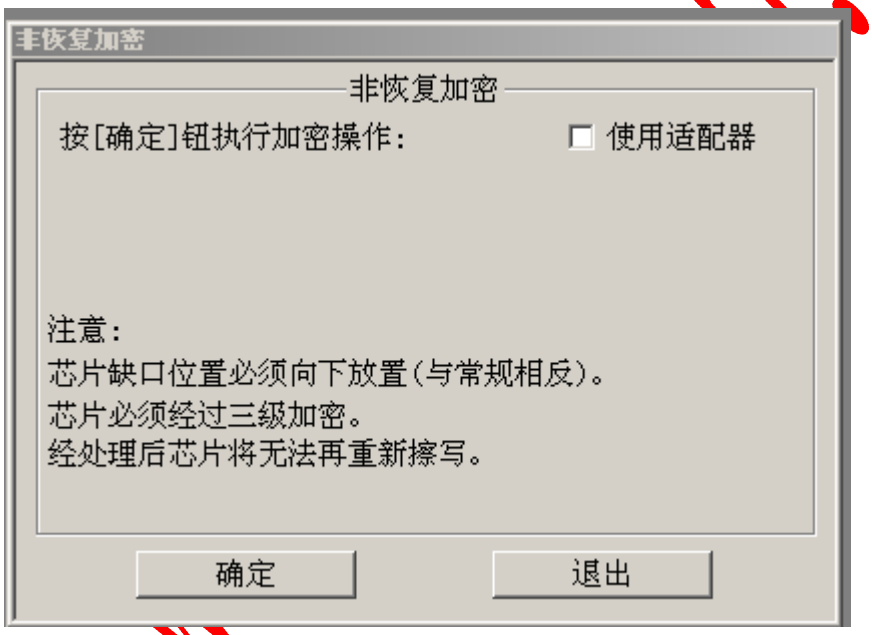
仅适用于 AT89C5X 芯片

点击其他－>非恢复加密，

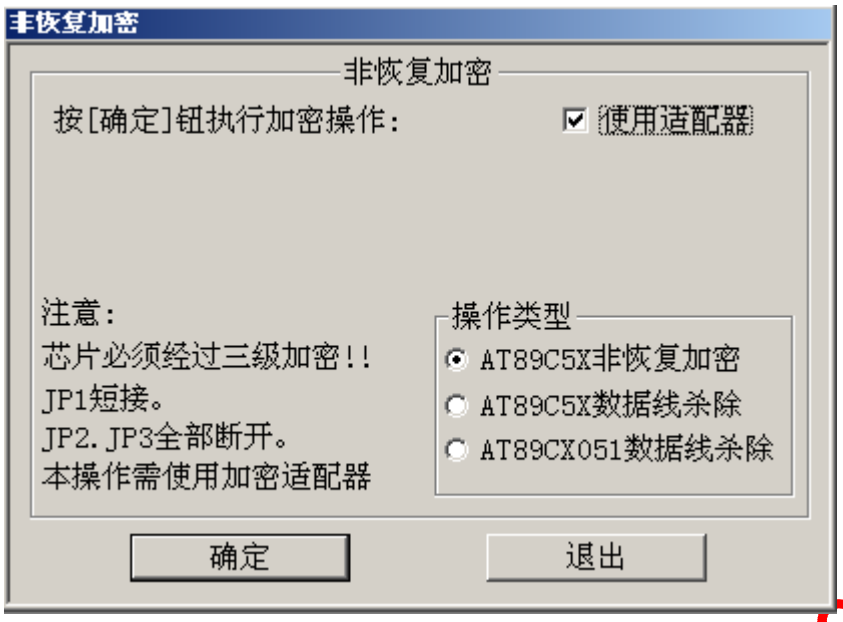



。

联后弹出窗口：




选中使用适配器：

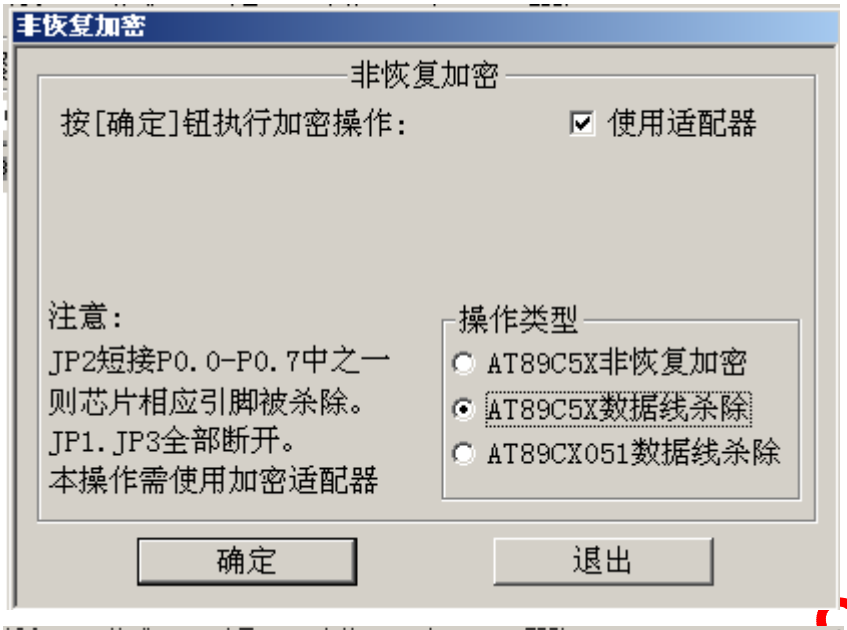


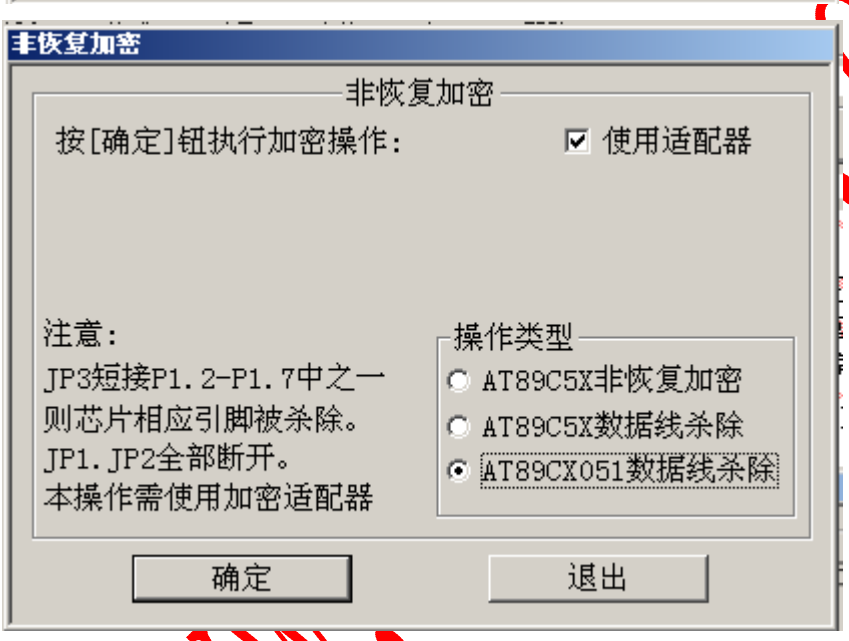

将 K51 适配器板上的跳线按照软件提示短接，将已经烧写好、经过验证并且经过了常规的三级加密的芯片正常放置于 K51 适配器锁紧座上，点击“ 确定 ”，就可以实现烧断管脚的加密了。

2．数据线杀除。(烧断数据线)

将已经烧录、一件验证程序的 AT89C5X/X051 芯片正常放置于 K51 锁紧座上，按照软件提示用跳线选择 AT89C5X 的 P0.0-P0.7，或用跳线选择 AT89CX051 的 P1.2-P1.7，选择好所要烧断的数据线后，点确认，就可以烧断芯片的数据线了。

这个过程前面和 1 一样，只有最后一步选择不一样：




附录：

其他烧断管脚或扳断管脚的方式：

.1.电压型烧断：

工具：使用 15V 电源串 47~470 欧小电阻（不能太小），并联一路二极管保护的发光管，发光管限流后接 Vcc 或 Gnd(极性不同)，接一探针。

再使用-15V 电源，电源的地接 IC 的 Vcc,至发光管亮，注意极性为负极性！

目的是击穿 Pin 的 Pmos 管（即上拉管）；再用 5V 电源，直接加在待烧 Pin 上，再次把已短路的 Pmos,烧开路。

使用+15V 电源，把探针点在待烧管脚至发光管亮，注意不能超过 3 秒，否则 IC 会损坏。发光管亮说明 Pin 的输出 Nmos（即下拉管）击穿;再用 5V 电源烧开路。

就 OK 啦，这个 Pin 将永远失效了！!

过程：电压烧坏 Pmos—电流烧坏 Pmos—电压烧坏 Nmos—电流烧坏 Nmos

如此烧断后，解密者就很难判断那个口被烧断了。

说明：EA 是读入脚(对 MCU 来说)，而烧 Pin 的原理是烧坏 Pin 的输出推挽管,如果想烧坏 Pin 的输入则要冒 IC 被烧坏的风险！

所以不能选只读的脚来烧，一定要烧编程时回读数据的 IO 口，最好烧断两个。

建议：根据以上原理，自己用 MCU 做一个自动烧断器，烧断就会非常可靠！

解密者一般是利用我们烧 Pin 的漏洞，钻空子才能解密的。

如只执行了上述烧 Pin 的某一步就留下了漏洞。

那是不是完全烧坏 Pin 以后就不能解密了呢，也不是！

但要想解密，完全烧坏两 Pin 的费用，需要 2K 以上，并且烧断管脚的同时，管脚的保护电路有可能被烧掉，解密者从表面更难推断是烧

什么连线,如果要破解还要找到真正的单片机破解高手。

2.特殊物理方法：

这个严格的讲，不是烧断了，可以封装 MCU 的时候，那个管脚就不引出（但是那种方式，你没有一定的量，封装厂是不会理睬你的，也可以正常的芯片使用一定的工具，把管脚到管芯 PAD 处的管脚完全去掉，联后用保密硅胶封住这个口；或者干脆物理性扳断，这种加密是比 1，2 更难破解。

沪生电子 蔡金生

WWW.HUSOON.COM

021-61021969

写于：2007.8.17　　最新修改于：2007.8.17