MCU 芯片加密历程

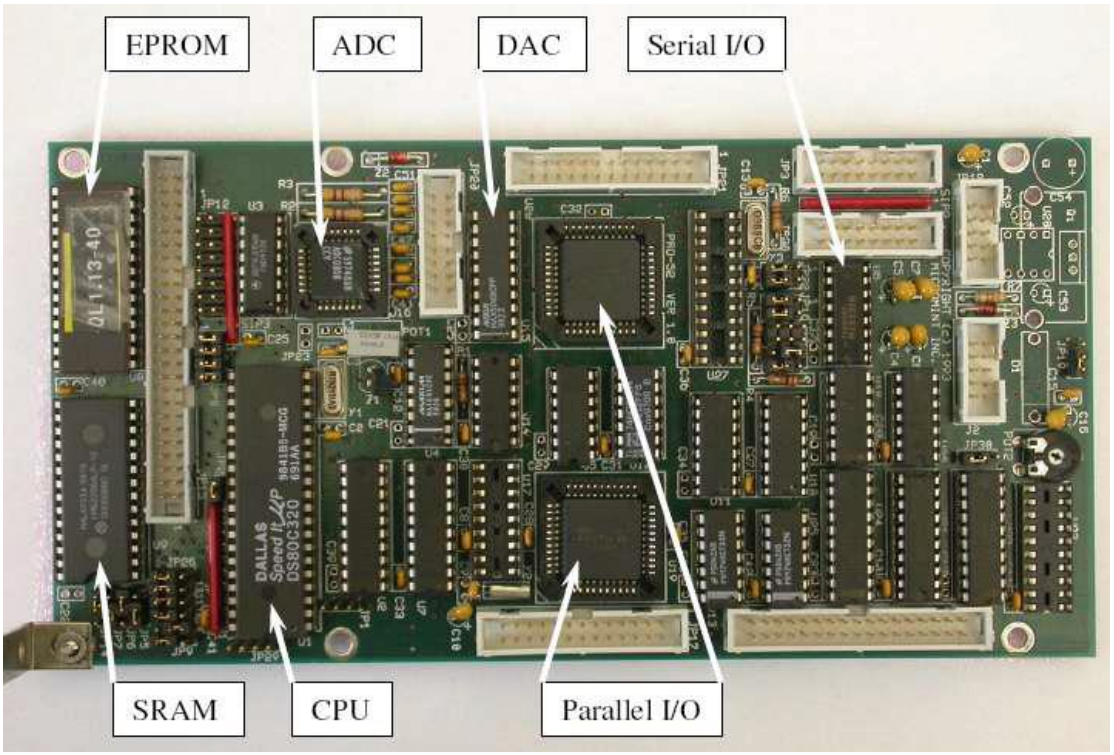
作者:武者

目录

自从上世纪七十年代 MCU 诞生以来，芯片的破解技术与防止芯片被破解方案就在不断在上演着“道高一尺，魔高一丈”，一山更比一山高的追逐。本文将单片机在安全保护方面的发展历程与大家分享。并在文章的最后，总结了现阶段安全级别最高的智能卡芯片的优点及其缺点。

一、单板机时代

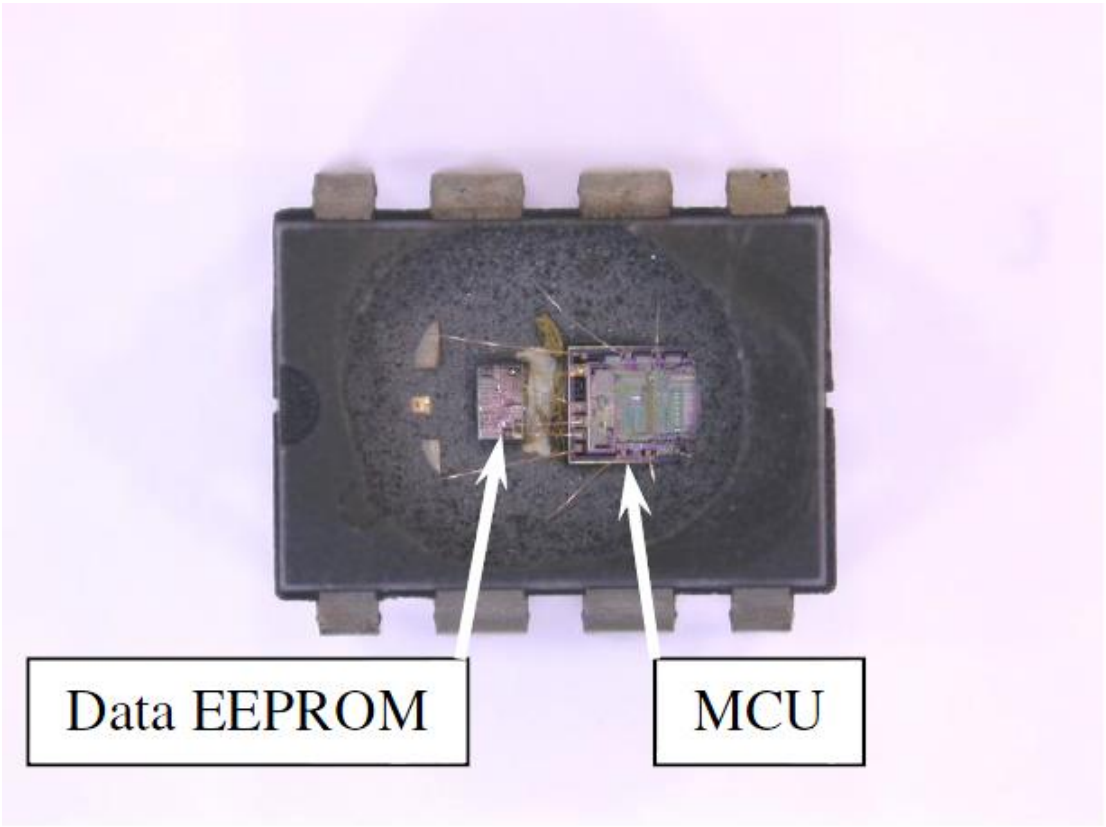
上世纪 70 年代初期，嵌入式系统是由分离部件如： CPU、ROM、RAM、I/O 缓存、串口和其他通信与控制接口组成的控制板。如图：



这一时期除法律外，几乎没有保护措施来防止侵入者复制单板机上 ROM 区的数据。

二、单片机时代

随着大规模集成电路技术的发展，中央处理单元(CPU)、数据存储器(RAM)、程序存储器(ROM)及其他 I/O 通信口都集成在一块单片机芯片上了，微控制器 MCU 取代了单板机。如图：

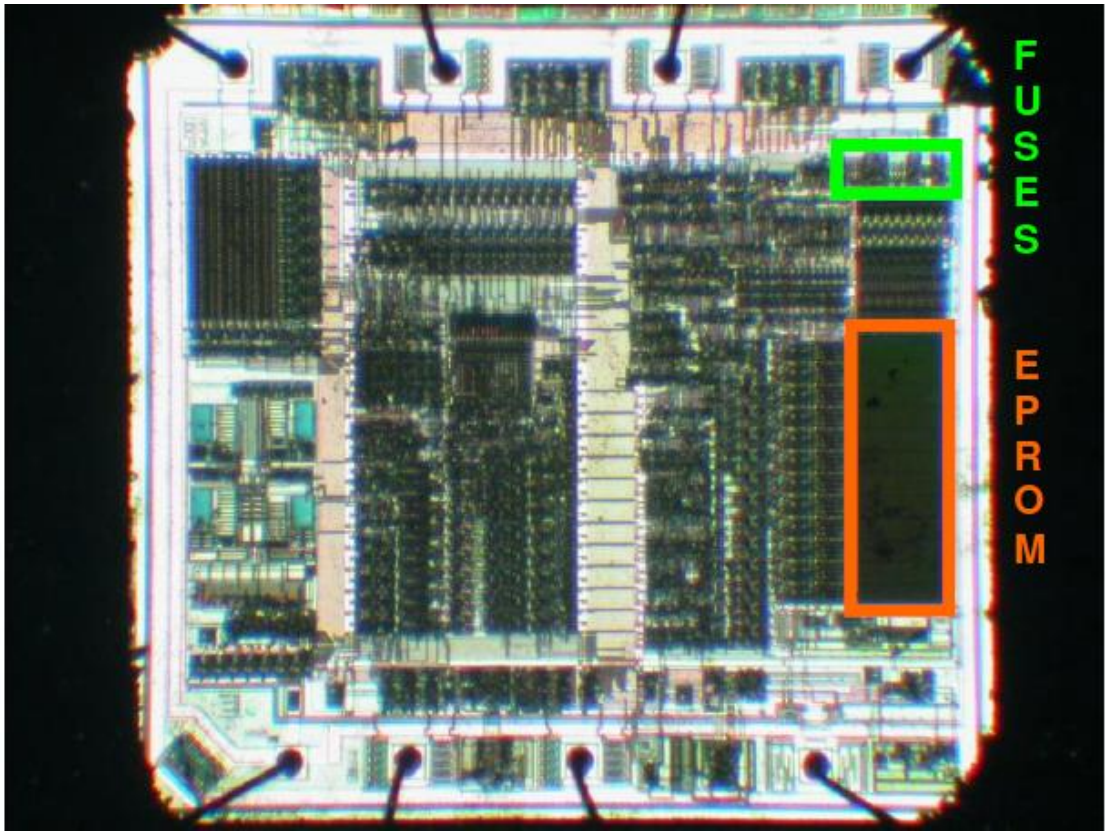


这一时期，内部存储器 EEPROM 和 MCU 是分开封在同一封装内部。侵入者可用微探针来获取数据。

三、安全熔断丝(Security Fuse)

随着入侵者的增加，MCU 为了自身的安全，后来增加了安全熔

断丝(Security Fuse)来禁止访问数据。如图：

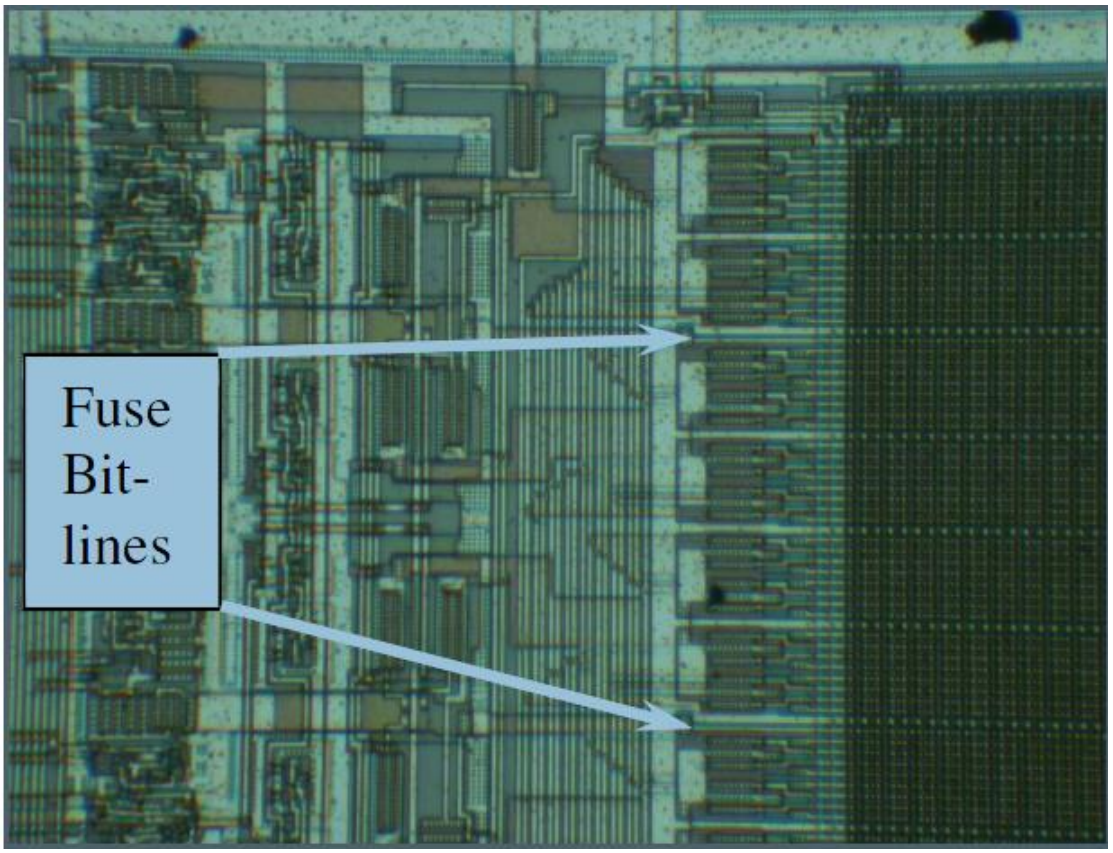


优点：很容易做到，不需要完全重新设计 MCU 构架，仅用熔断丝来控制数据的访问。

缺点：熔断丝容易被定位、攻击。例如：熔丝的状态可以通过直接把位输出连到电源或地线上来进行修改。有些仅用激光或聚焦离子束来切断熔丝的感应电路就可以了。用非侵入式攻击也一样成功，因为一个分离的熔丝版图异于正常存储阵列，可以用组合外部信号来使位处与不能被正确读出的状态，那样就可以访问存在内部芯片上信息了。用半侵入式攻击可以使破解者快速取得成功，但需要打开芯片的封装来接近晶粒。一个众所周知方法就是用紫外线擦掉安全熔断丝。

四、安全熔丝变成存储器阵列的一部分

再后来 MCU 制造商将安全熔丝做成存储器阵列的一部分，如图：



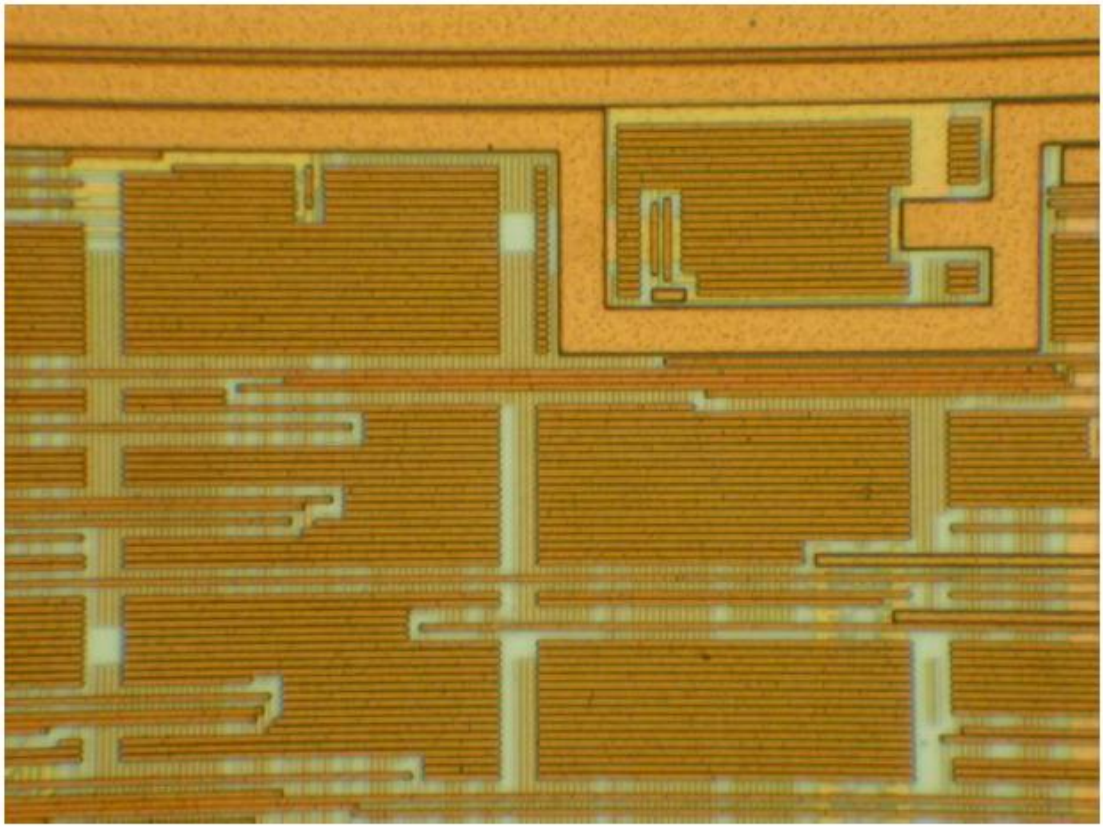
一般的熔丝与主存储器离得很近，或干脆共享些控制线，与主存储器用相同的工艺来制造，熔断丝很难被定位。非入侵试攻击仍然可以用，可以用组合外部信号来使熔断位处于不被正确读出的状态。同样，半侵入式攻击也可用。当然破解者需要更多的时间去寻找安全熔丝或控制电路负责安全监视的部分，但这些可以自动完成。进行侵入式攻击将是很困难需要手工操作，那将花费更多的成本来破解。

五、用主存储器的一部分来控制外部对数据访问

利用上电时锁定特定区域地址的信息，将它作为安全熔丝。或用密码来控制对存储器访问。例如德州仪器的 MSP430F112 只有输入正确的 32 字节密码后才能进行回读操作。如果没输入，只有擦字节密码后才能进行回读操作。尽管这个保护方法看上去比先前的更有效，但它有一些缺点可以用低成本的非侵入式攻击，如时序分析和功耗来破解。如果安全熔丝状态是上电或复位后存储器的一部分，这就给破解者用电源噪声来破解的机会，强制路进入存储中错误状态。

六、使用顶层金属网络

使用顶层金属网络设计，提升入侵难度。所有的网格都用来监控短路和开路，一旦触发，会导致存储器复位或清零。如图：

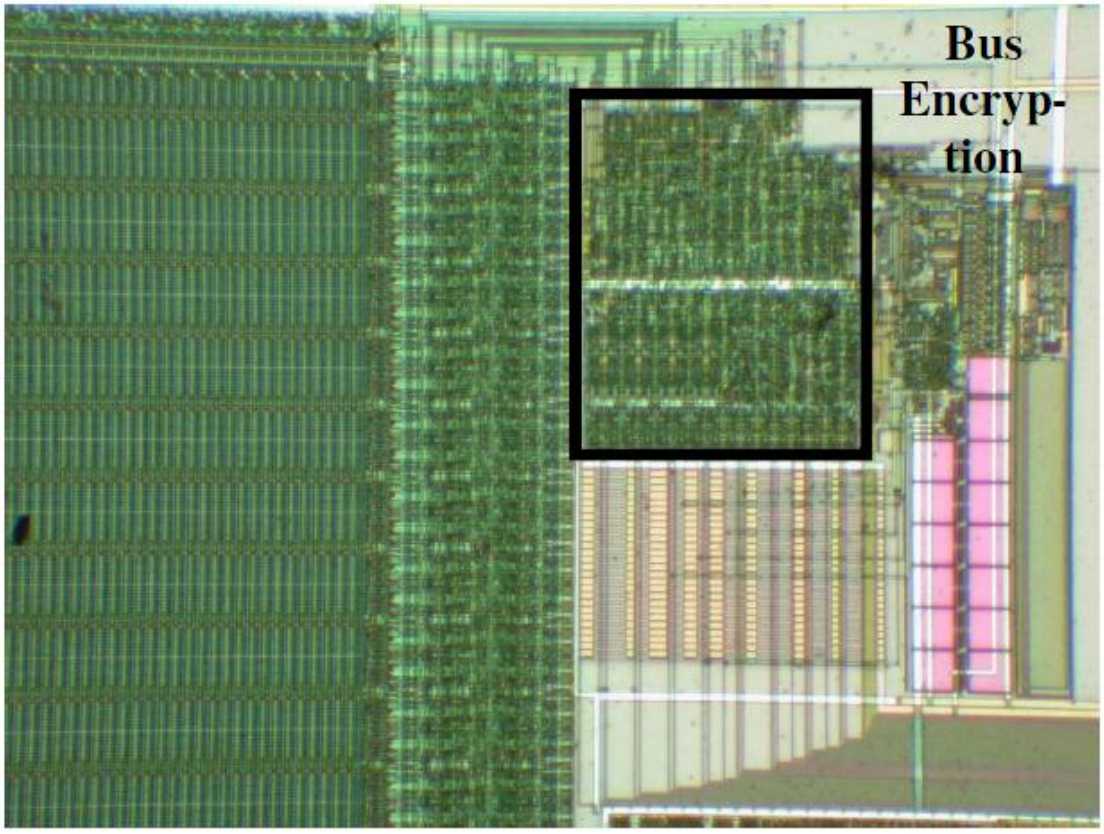


普通的 MCU 不会使用这种保护方法，因为设计较难，且在异常运行条件下也会触发，如：高强度电磁场噪声，低温或高温，异常的时钟信号或供电不良。故有些普通的 MCU 使用更廉价的伪顶层金属网格，会被非常高效的光学分析进行微探测而被攻击。另外，这些网格不能防范非侵入式攻击。同样不能有效防范半侵入式攻击，因为导线之间有电容，并且光线可以通过导线抵达电路的有效区域。

在智能卡中，电源和地之间也铺了一些这样的网格线。部分可编程的智能卡走的更远，干脆砍掉了标准的编程接口，甚至干掉了读取 EEPROM 接口，取而代之的是启动模块，可以在代码装入后擦掉或者屏蔽自己，之后只能响应使用者的嵌入软件所支持的功能。有效的防范了非侵入式攻击。

七、智能卡芯片安全设计

近些年，一些智能卡使用存储器总线加密(Bus Encryption)技术来防止探测攻击。如图：



数据以密文方式存储在存储器中。即使入侵者获得数据总线的数据，也不可能知道密钥或者别的敏感信息(如数据还原方法)。这种保护措施有效的防范了侵入式和半侵入式攻击。

有些智能卡甚至能够做到每张卡片总线加密密钥不同，这样即使入侵者完全破解了，也无法生产出相同功能的芯片来，因为每个智能卡芯片有唯一的 ID 号，无法买到相同 ID 号的智能卡。

另外值得一提的是，有些智能卡将标准的模块结构如解码器，寄存器文件，ALU 和 I/O 电路用类似 ASIC 逻辑来设计。这些设计成为

混合逻辑(Gle Logic)设计。混合逻辑使得实际上不可能通过手工寻找信号或节点来获得卡的信息进行物理攻击。大大提高了 CPU 内核的性能和安全性。混合逻辑设计几乎不可能知道总线的物理位置，有效的防范了反向工程和微探测攻击。

智能卡芯片加密方案优缺点

对于开发者来讲，选择更为安全设计的微控制器或可以得到更好的保护。与大多数微控制器相比，即使是十年前设计的智能卡也能提供更好的保护。

现代的智能卡提供了更多的防攻击保护，内部电压传感器保护免受电源噪声攻击(Power Glitch attacks)、过压和欠压保护。时钟频率传感器防止受到静态分析(Static analysis)的降低时钟频率攻击。同时也可以防止时钟噪声(Clock glitch attacks)进行提高时钟频率的攻击。顶层金属网格和内部总线硬件加密使可以防止微探测攻击。

但是与微控制器相比，智能卡芯片也有劣势，如：芯片价格昂贵，小批量的很难买到货。开发工具昂贵，需要和制造商签署保密协议，即使是说明书也要这样。很多制造商仅向特定客户销售大批量的智能卡。另一个不足是 I/O 的功能受限，普通智能卡芯片通常只有 ISO7816 接口，极少有单独的 I/O 口。这使得多数应用中不能取代微控制器，而只能用于安全要求非常高的行业，如：付费机顶盒，银行卡，SIM 卡，二代身份证，高端加密芯片等领域。

智能卡芯片在加密芯片领域的应用，将是个不错的方向。因为智

能卡芯片安全等级高，IO 资源少。 而普通 MCU 的硬件资源非常丰富，安全程度却不高，可以将 MCU 中一些关键算法及运行参数，以特殊形式存放在智能卡芯片中，从而实现高安全强度的强大功能。

后记

坚持不懈的尝试突破保护机制的破解团体和不断引入新的安全防范方案的制造商之间的斗争是没有尽头的。 “道高一尺，魔高一丈”，又或是“邪不压正”，将不停的在两派之间上演！