芯片解密（单片机破解）技术解析

芯片解密又叫单片机破解，单片机破解，芯片破解，IC 解密，我们把 CPLD 解密，DSP 解密都习惯称为芯片解密。单片机攻击者借助专用或自制设备，利用单片机芯片设计上的漏洞或软件缺陷，通过多种技术手段提取关键信息，获得单片机内的程序即为芯片解密技术。

芯片解密属于法律边缘的行业，但仁者见仁智者见智。北京首矽致芯科技负责人表示，芯片解密只是一把刀，本身并没有对错，不过是握在谁的手里，拿刀去做什么，才最终决定了其性质的好坏。

撇开芯片解密的性质不谈，就芯片解密技术本身来说，也是一种精密复杂的高端科技，需要破解人员具有扎实的逆向工程知识及丰富的解密经验。否则，很可能解密失败，赔了“母片”又折兵。一般的解密方法包括：软件攻击、电子探测攻击、过错产生技术以及探针技术。

软件攻击技术

软件攻击解密技术即软解密技术，就是通过软件找出单片机的设计缺陷，将内部 OTP/falshROM 或 eeprom 代码读出，这种芯片解密方法并不是最理想的，因为研究时间太长且同一系列的单片机不是每个都一样。

电子探测攻击技术

电子探测攻击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。

芯片解密又叫单片机破解，单片机破解，芯片破解，IC 解密，我们把 CPLD 解密，DSP 解密都习惯称为芯片解密。单片机攻击者借助专用或自制设备，利用单片机芯片设计上的漏洞或软件缺陷，通过多种技术手段提取关键信息，获得单片机内的程序即为芯片解密技术。

芯片解密属于法律边缘的行业，但仁者见仁智者见智。北京首矽致芯科技负责人表示，芯片解密只是一把刀，本身并没有对错，不过是握在谁的手里，拿刀去做什么，才最终决定了其性质的好坏。

撇开芯片解密的性质不谈，就芯片解密技术本身来说，也是一种精密复杂的高端科技，需要破解人员具有扎实的逆向工程知识及丰富的解密经验。否则，很可能解密失败，赔了“母片”又折兵。一般的解密方法包括：软件攻击、电子探测攻击、过错产生技术以及探针技术。