智能卡的攻击和防护探讨

北京智慧云测科技有限公司

关注智慧云测官方微信，获取更多资讯！

目录

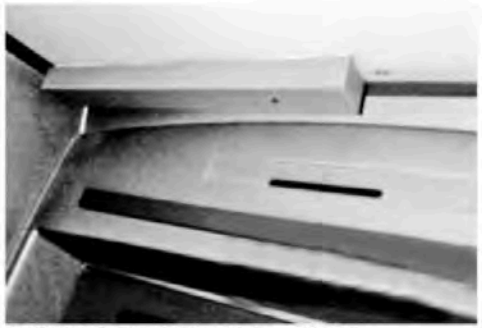
磁条卡的弱点

磁条卡伪卡制作成本低廉，耗时短。

不法分子通过非法手段窃取磁条卡磁道与密码信息后，可通过复制卡片来进行窃取持卡人资产资金。

银行卡复制器网上公开叫卖 盗卡内信息只需2分钟

来源：长江商报 发布时间：2013年07月19日 10:47 作者：


微型摄像机安装在ATM机附近。


复制器中的芯片装入插卡口，用来偷卡号。


用此机器“克隆”一张新卡。


银行卡复制器套装。 东方IC图

EMV迁移

EMV迁移是银行卡从磁条卡向智能卡转换的过程。

芯片卡降级交易本月关闭 刷卡将被插卡取代

2014年10月21日 05:59 南方都市报 微博 收藏本文

新发银行卡全为芯片卡

发布时间：2015-01-13 12:30:57 来源：齐鲁晚报 作者：佚名 责任编辑：罗伯特

芯片卡竟能降低盗刷风险20% 不是骗你！

字号 大 小

2016-04-22 16:33:00 来源：融360 评论 邮件 纠错

芯片卡伪卡欺诈率下降90%以上

作者：RFID世界网收录 来源：都市快报 加关注 3601

智能卡

安全防护等级高，难以复制

芯片卡更快更安全

2011年08月30日05:09　来源：　上海金融报　作者：周轩千龚新颖

将本文转发至：

更安全的银行芯片卡 你换了吗

2014年10月31日 15:17　钱江晚报　微博　收藏本文

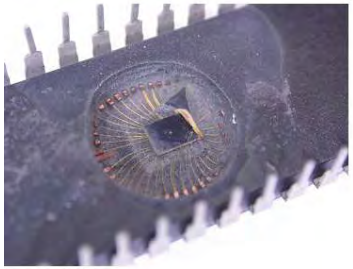
芯片卡为什么比磁条卡安全

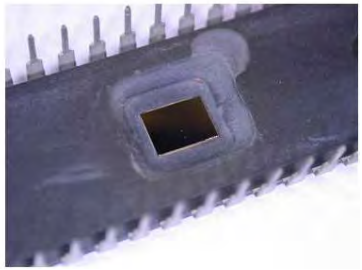
来源: 只做卡　发布时间: 2015-04-26 16:11　2530 次浏览　大小: 16px 14px 12px

大家知道，最早银行推出磁条卡的时候，那时候非常方便，只需要一刷即可以取钱，而现在为什么银行逐渐已经取消了磁条卡了呢。这里面最重要的一个原因就是芯片卡要比磁条卡安全的不知多少倍。下面我来给大家讲解一下为什么芯片卡要比磁条卡安全的很多倍。

■ 物理保障

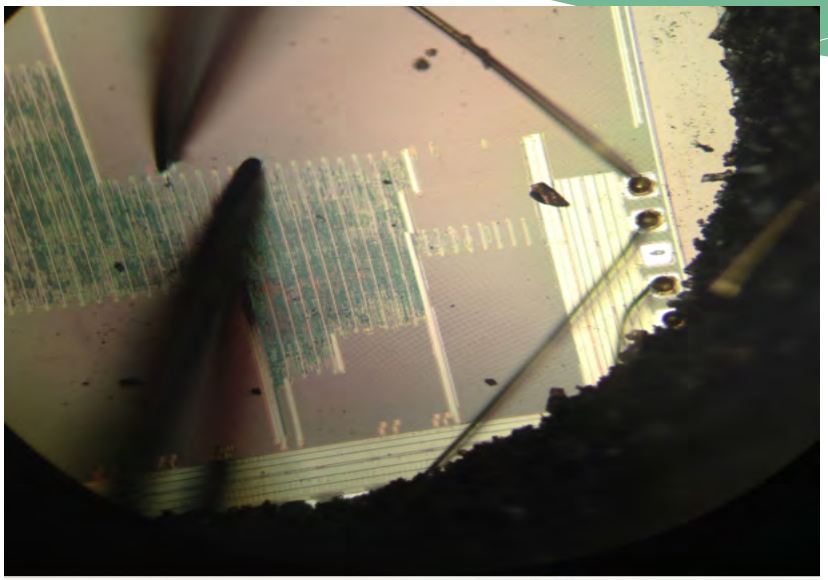
- ✓ 暴露芯片需要化学手段

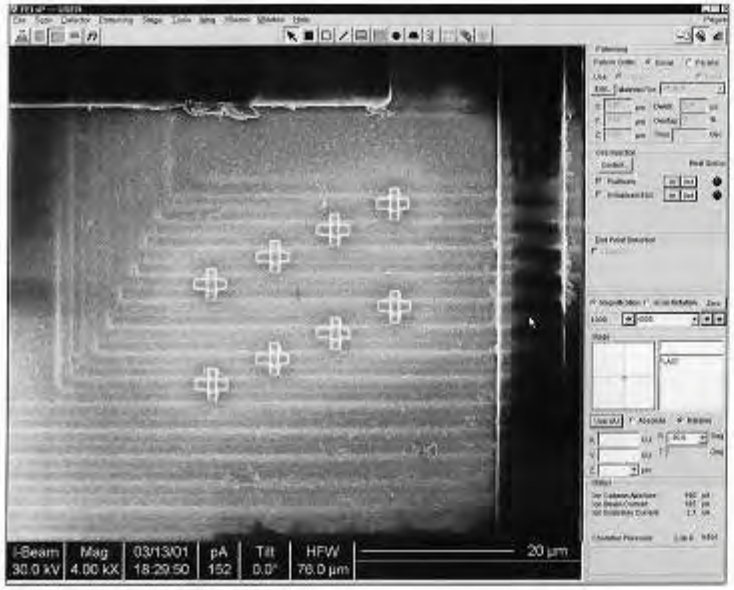


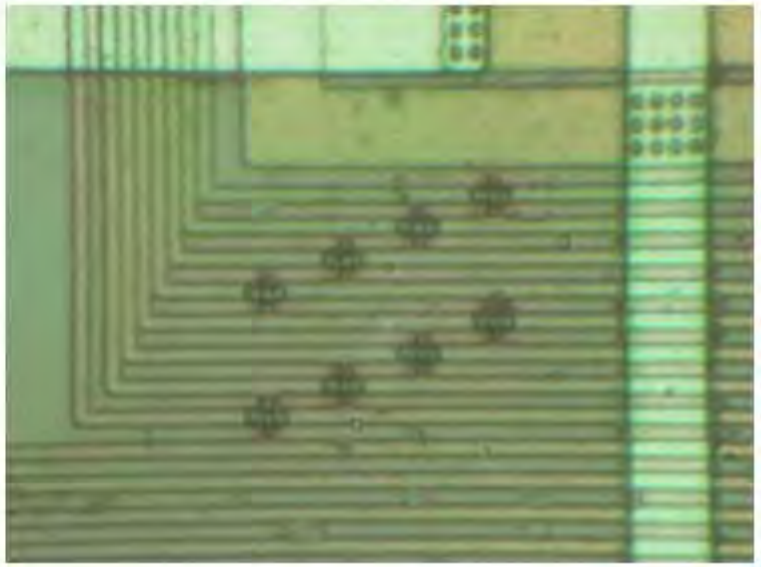


■ 物理保障

- ✓ 防止通过探针窃听信号线

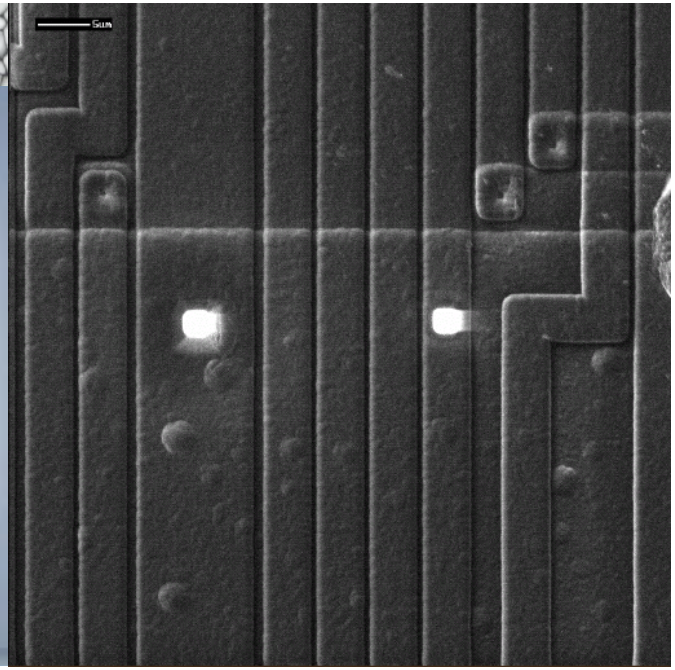


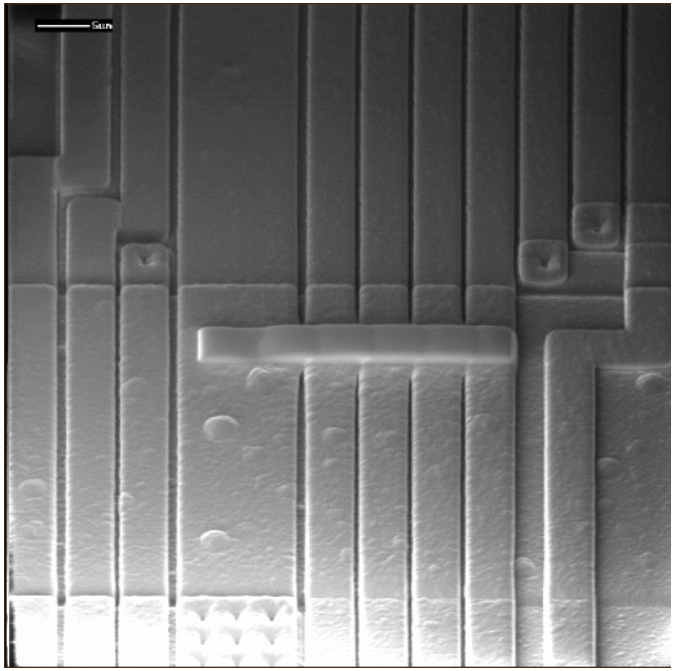




■ 物理保障

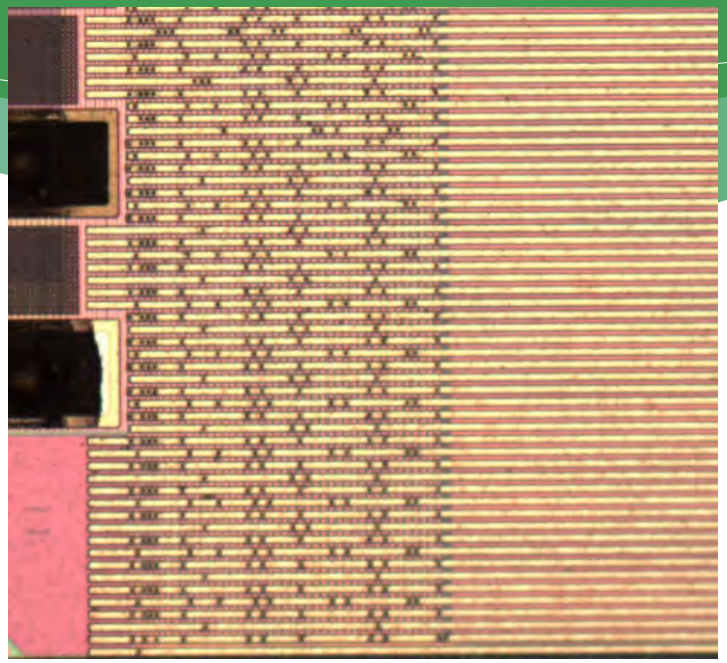
- ✓ 防止电路被修改





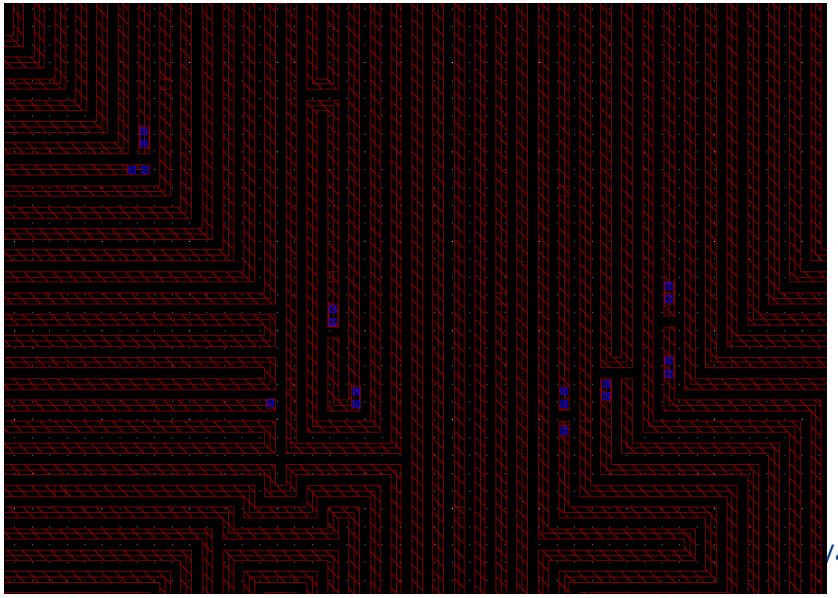
■ 物理保障

✓ 防止侵入式攻击、防止电磁注入、激光注入、防止电磁辐射分析EMA



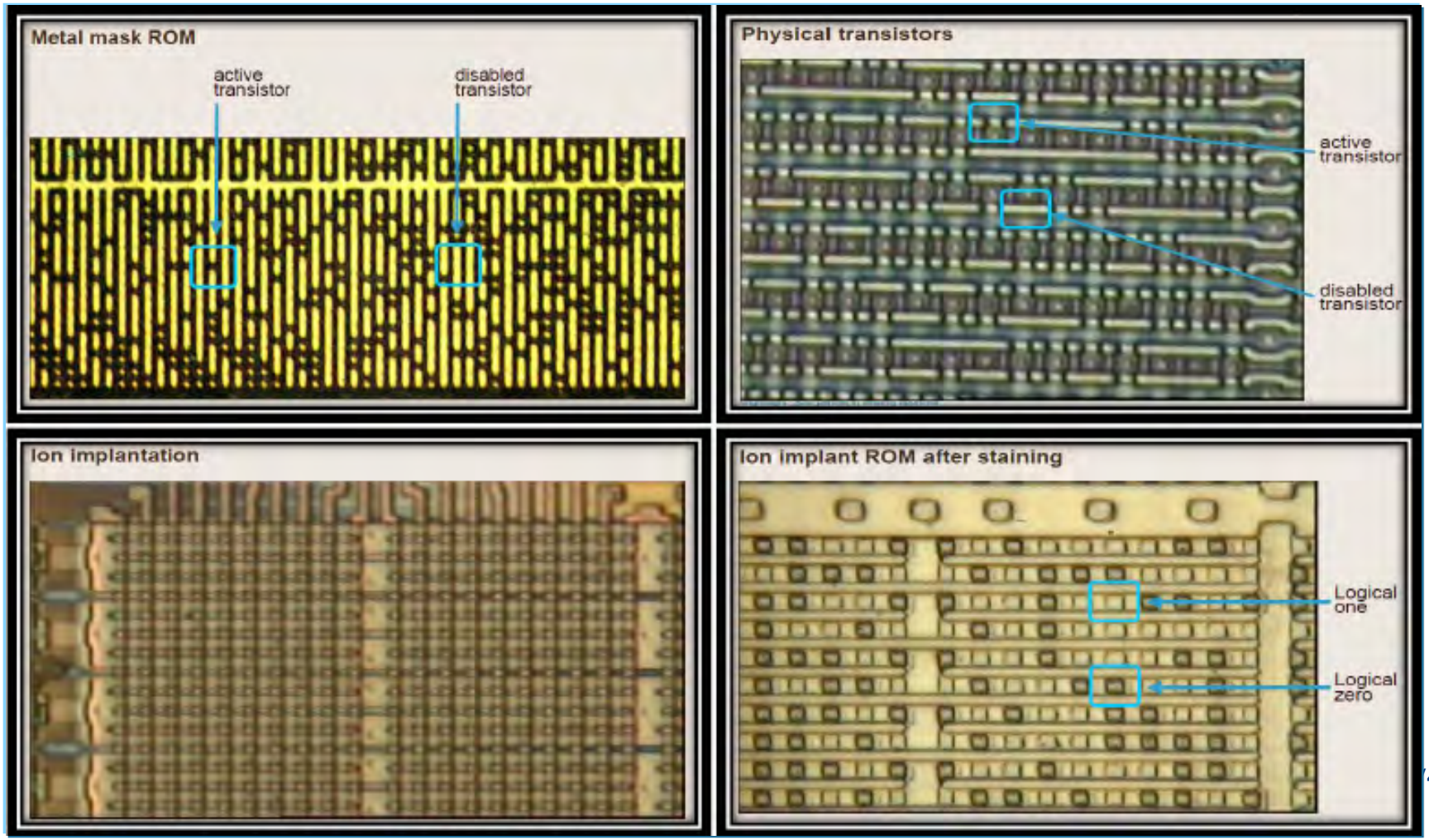
金属覆盖层

- 层数
- 覆盖率
- 形状
- 间距

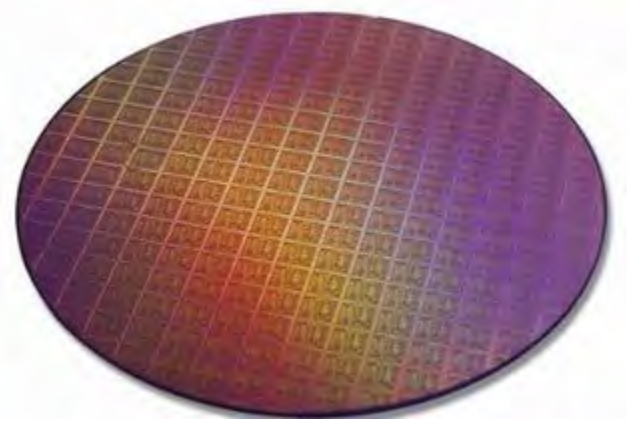


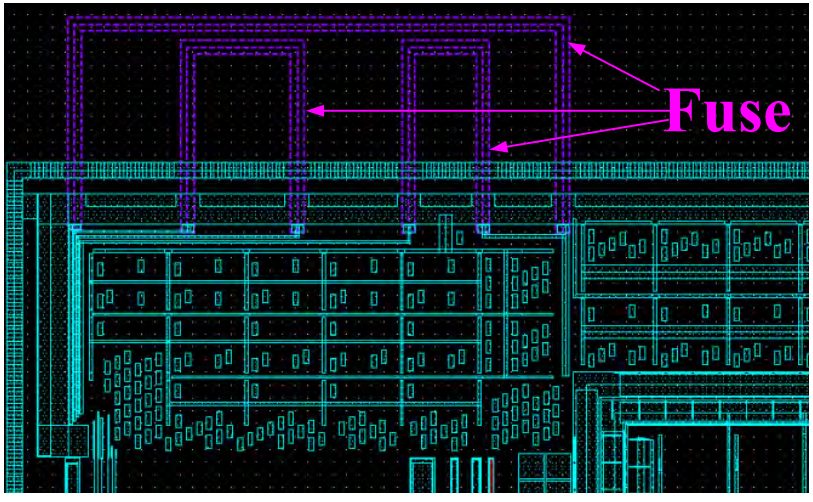
■ 物理保障

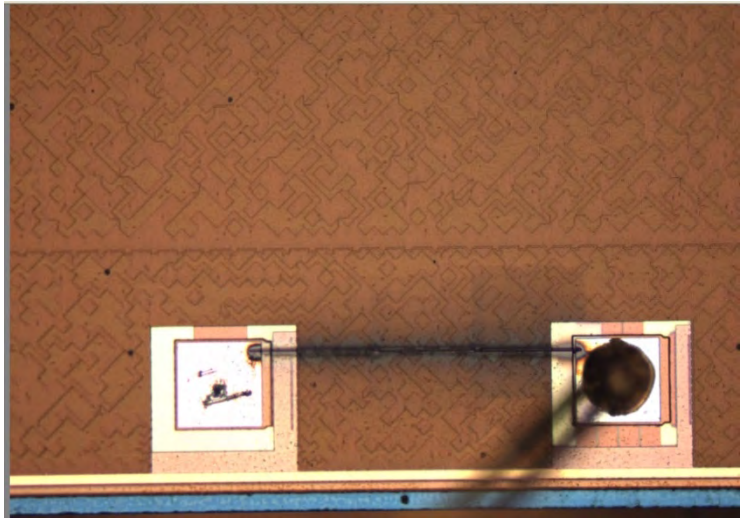
✓ 防止智能卡存储器被读取

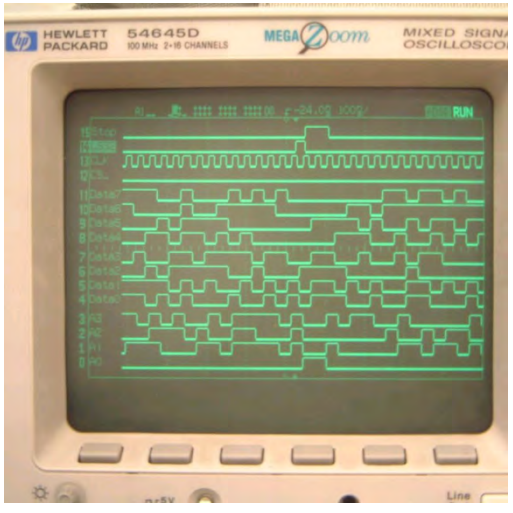


■防止生命周期功能滥用

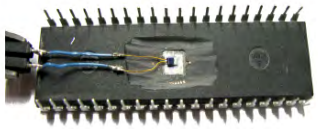


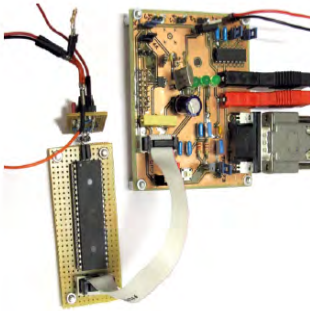


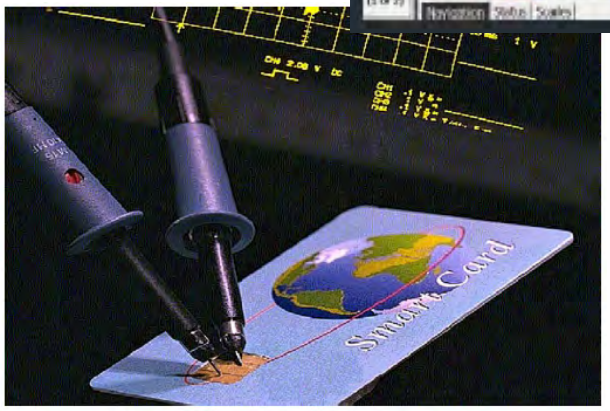


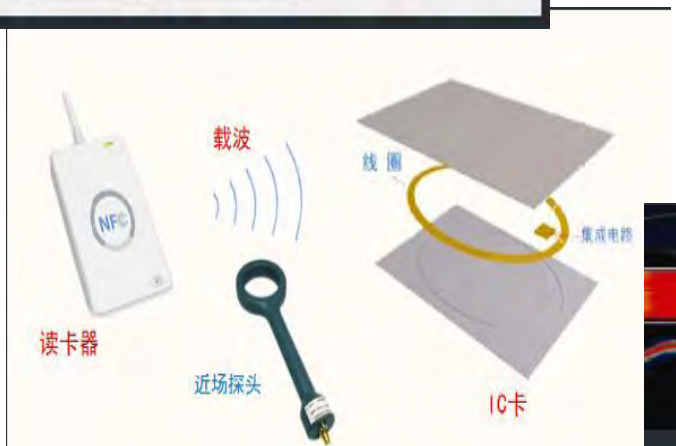


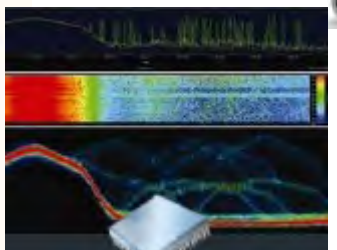
■ 防止信息泄露









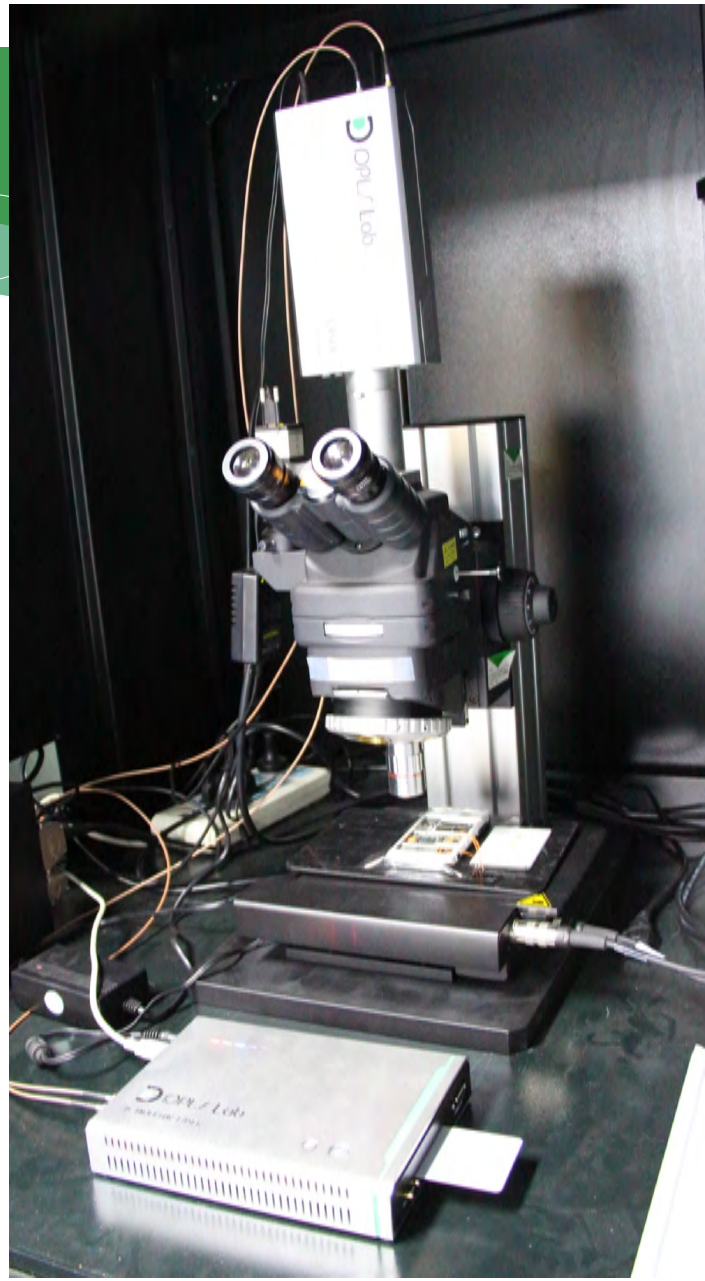


■ 算法安全性保障

算法	金融里的应用
RSA /SM2	签名验签，脱机密文pin加密，
DES/3DES/SM4	计算pin block，应用密文算mac，报文部分数据加解密
AES	同上
SHA256/SM3	签名算hash，摘要验证

目录

密码算法	破解手段
RSA/(国密SM2)	侧信道功耗分析，激光错误注入
AES	侧信道电磁分析，侧信道功耗分析，电磁错误注入，等
DES/3DES(国密SM4)	侧信道电磁分析



目录

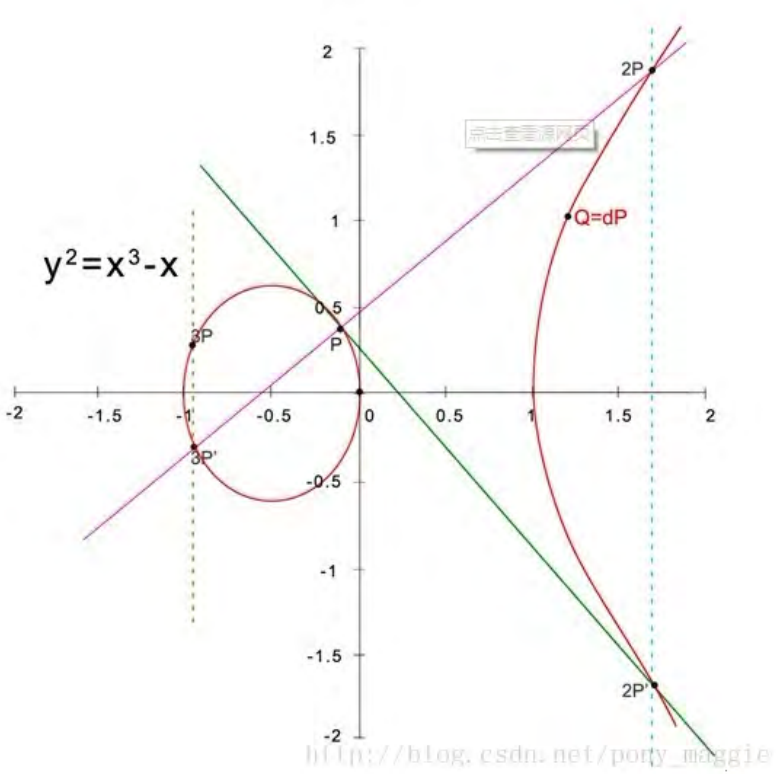
SM2算法

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

椭圆曲线并不是椭圆，之所以称为椭圆曲线是因为它们是用三次方程来表示的，并且该方程与计算椭圆周长的方程相似。

基于这种离散椭圆曲线原理的SM2算法一般有三种用法：

- 签名验签
- 加解密
- 密钥交换



芯片攻击

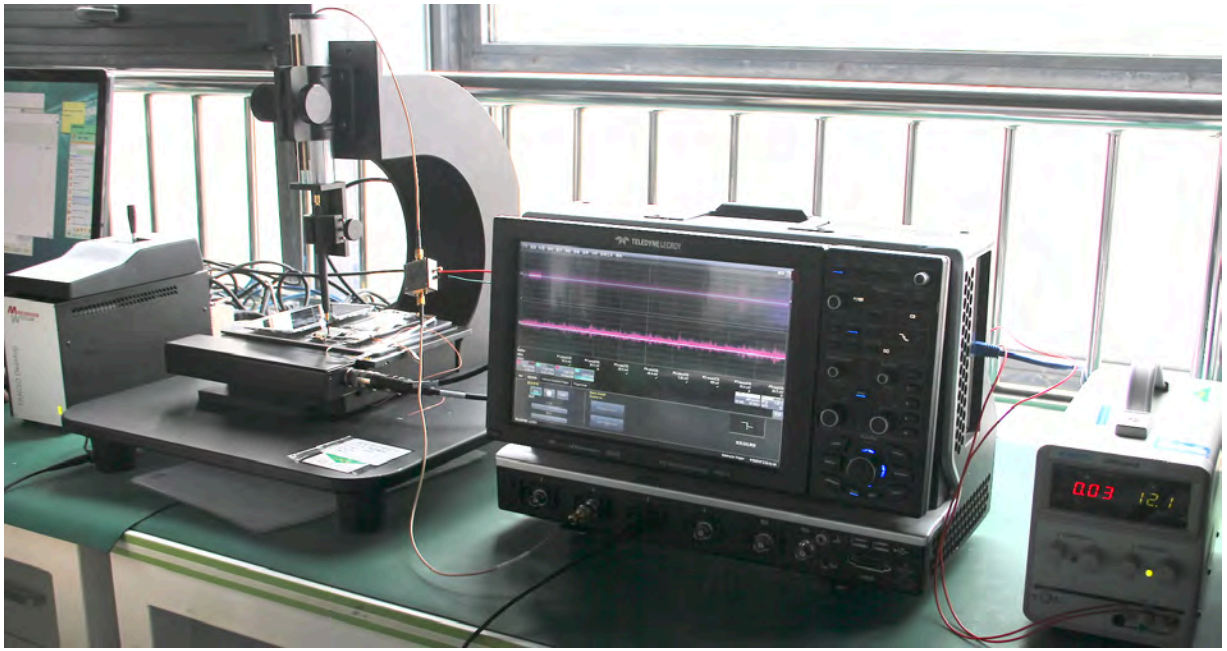
■ 攻击对象

某市面流通的智能卡

- 智能卡芯片：XXXX
- 攻击算法：SM2

■ 攻击平台

D-Observer



■ 攻击代价

时间	• 4小时
曲线数	• 1条
设备	• 功耗采集设备、示波器 • 算法分析软件
样本	• 智能卡1张
人员知识	• 侧信道技术

■ 攻击结论

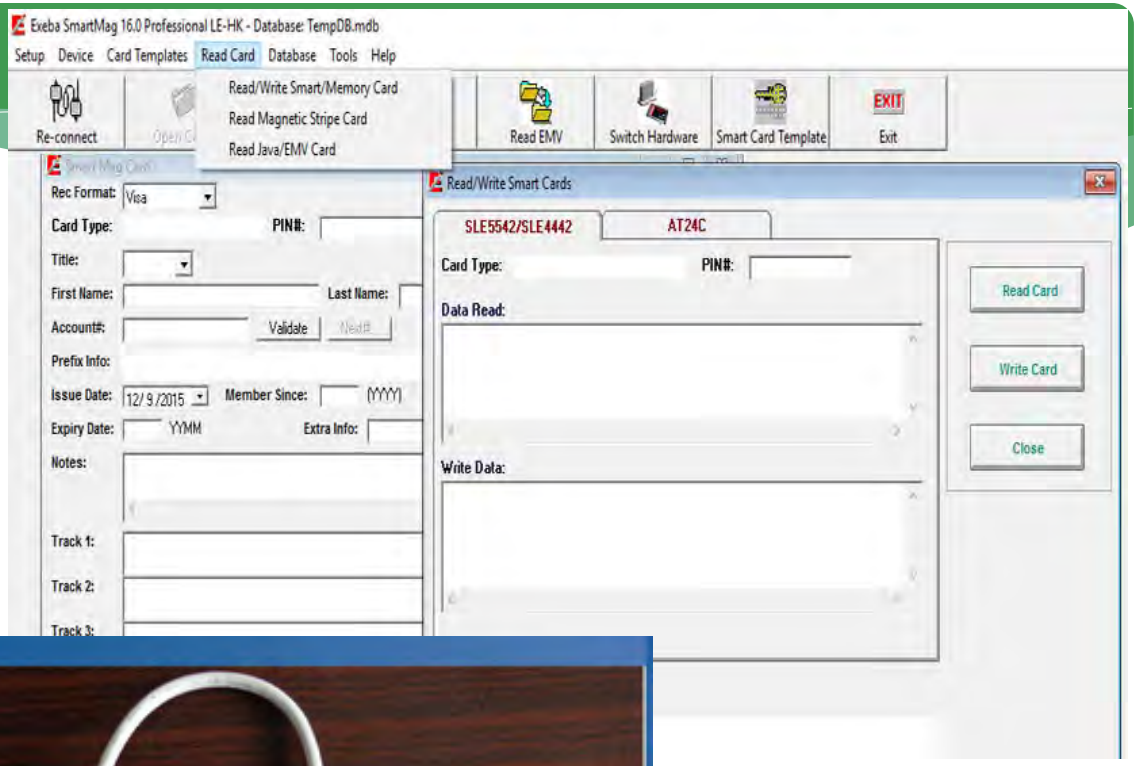
安全威胁较大： 无需对智能卡进行任何破坏

攻击实施难度： 需要软件分析能力强大，攻击人员需经验丰富

目录

伪卡的制作

- ✓ 通过软件直接写入破解得到的秘钥（SM2私钥）进入到智能卡中。
- ✓ 写入其他智能卡配套信息，如：卡号，UID等。



目录

作为实验室，我们现在只尝试了一种SM2算法，可以推测其他SM算法的实现也存在同样的风险。

今后几年，SM算法将会用到交易中的各个环节，比如：在线交易，动态认证，签名验签，等等。

安全算法的实现还需产业界各方共同努力，不断精进。

我们提供的安全咨询服务可以先于真正的黑客之前找到这些漏洞。

这是我们实验室对产业界的责任。

Secure Your Life

*谢谢！

黄天宁

联系电话：18610887190

邮箱地址： huangtn@dplslab.com

公司地址：北京市石龙经济开发区莲石湖西路98号院7号楼701室