3G/4G SIM卡安全分析与防护

郁昱
上海交通大学 密码与计算机安全实验室
(谷大武 刘军荣 郭筝 葛毅杰 等)

年初Citizenfour的一则报道

www.digitaltrends.com/mobile/nsa-gchq-sim-card-hack-snowden-leak-ne

THE NSA HAS HACKED YOUR PHONE: WHAT YOU NEED TO KNOW, AND HOW TO PROTECT YOURSELF

By **Malarie Gokey** — February 25, 2015

3 1.1K 268 103

"When the NSA and GCHQ compromised the security of potentially billions of phones (3G/4G encryption relies on the shared secret resident on the SIM), they not only screwed the manufacturer, they screwed all of us, because the only way to address the security compromise is to recall and replace every SIM."

报告提纲

- 背景
  1) 2G/3G/4G SIM 安全
  2) 密码学简介, 2G/GSM 的密码认证协议
- 我们的工作
  1) 3G/4G 密码认证协议和 MILENAGE算法
  2) 旁路攻击 / 差分功耗分析
  3) 策略、演示与结果
- 经验教训

第一部分
背景

移动通信技术 (1-4G)

- 1G: 模拟信号

- 2G: GSM vs. CDMA
  数字信号

- 3G/4G: UMTS/LTE
  高速数据传输

什么是 (U)SIM 卡?

- (U)SIM = (Universal) Subscriber Identity Module
- (U)SIM卡是一类智能卡 (迷你计算机系统).
- SIM卡上存储了
  - ICCID (序列号)
  - IMSI (E.g. 310 150 123456789)
    USA+AT&T +id number
  - 保密信息

- 2G SIM卡: 主密钥K
- 3G/4G USIM卡:
  主密钥K, 运行商保密参数 OPc, r1, …, r5, c1, …, c5.

保密信息窃取/破解后带来的安全隐患

CLONING

TAPPING

TROJAN

FRAUDULENT CALLS
OTP AUTHENTICATION

(U)SIM上实现了哪些密码功能?

Cryptology(密码技术) in a nutshell

Cryptology = “Cryptography” + “Cryptanalysis”

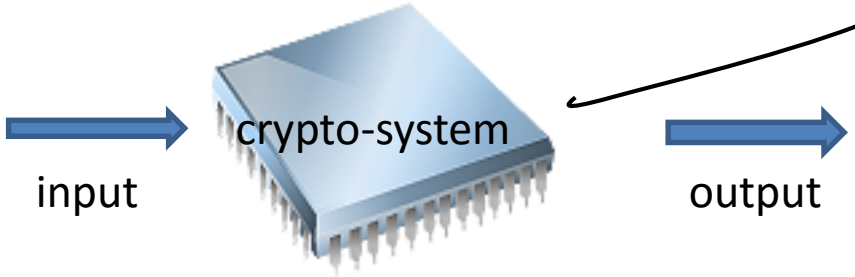
- Cryptography (密码学)

保护各种信息安全属性的密码算法设计，如AES分组加密(保密性)、HMAC（完整性）、SHA-3(防碰撞函数)、RSA数字签名(不可抵赖性)等

- Cryptanalysis (密码分析)

1. 数学密码分析: 数学上破解密码算法本身
2. 物理密码分析: 破解密码算法的物理实现

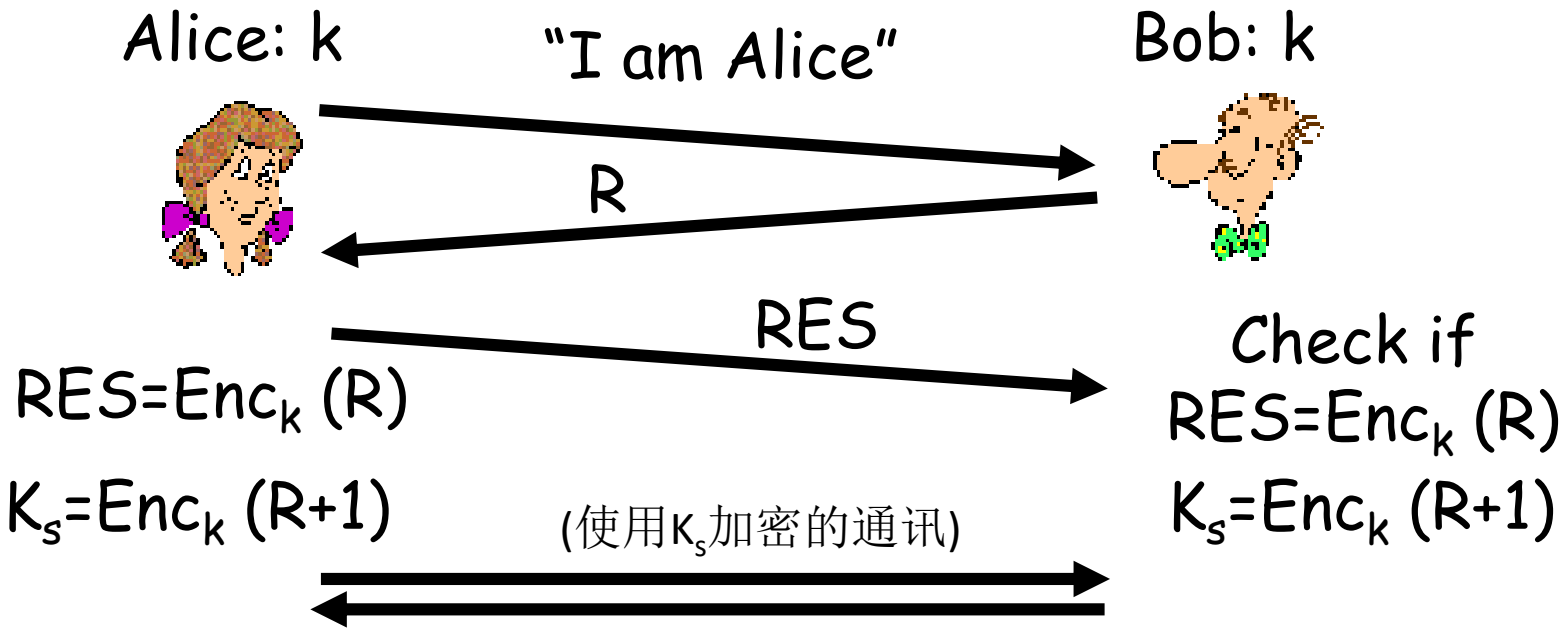
物理密码分析方法通常更为强大



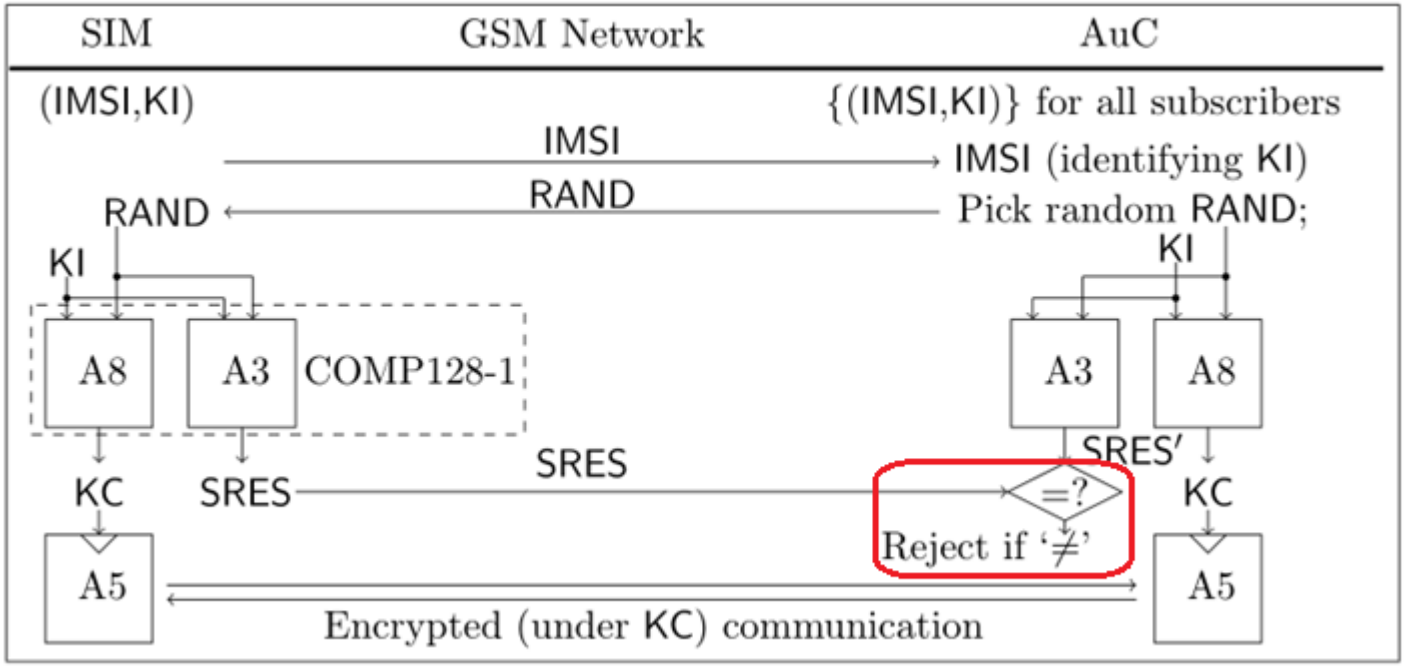
(U)SIM上实现的密码算法/协议

- AKA: Authentication & Key Agreement
- Authentication(认证/权鉴/鉴权): 确认用户的合法身份.

  例： Bob 对Alice进行认证： **Challenge-and-Response**.
- Key Agreement (密钥协商, 用词不准确): 生成session key



2G GSM AKA 协议



2G GSM 使用的AKA 算法: COMP128-1 (A3+A8)

2G GSM 使用的加密算法 : A5

安全性:

1. COMP128-1 算法有致命缺陷 (narrow pipe attacks [BGW98])
2. 单向认证 的局限性 (伪基站攻击, DEFCON 2010)
3. 旁路攻击 (差分功耗攻击 [RRST02,ZYSQ13])

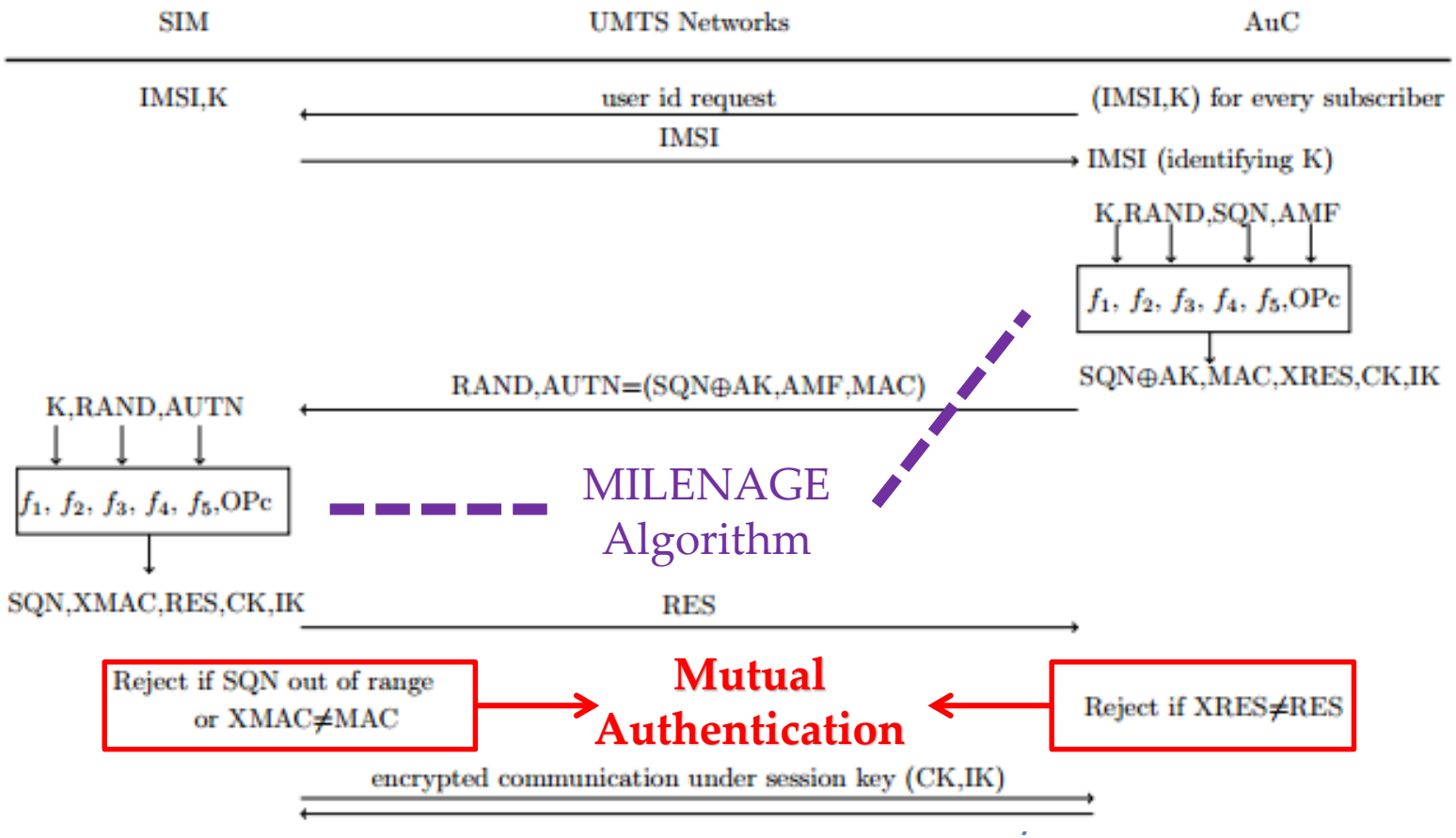
第二部分
我们的工作

3G/4G相对于2G
安全措施的提升

	2G	3G/4G
认证算法	COMP128-1 设计上致命缺陷	MILENAGE, 基于 AES-128 加密算法, 目前公认 数学安全
认证机制	单向认证 (基站认证SIM卡)	双向认证(防止伪基站攻击)
保密信息	主密钥K	主密钥 K tweak value OPc 更多运行商自定义参数: r1, …, r5, c1, …, c5 (更多保密信息 = 更好的安全性?)

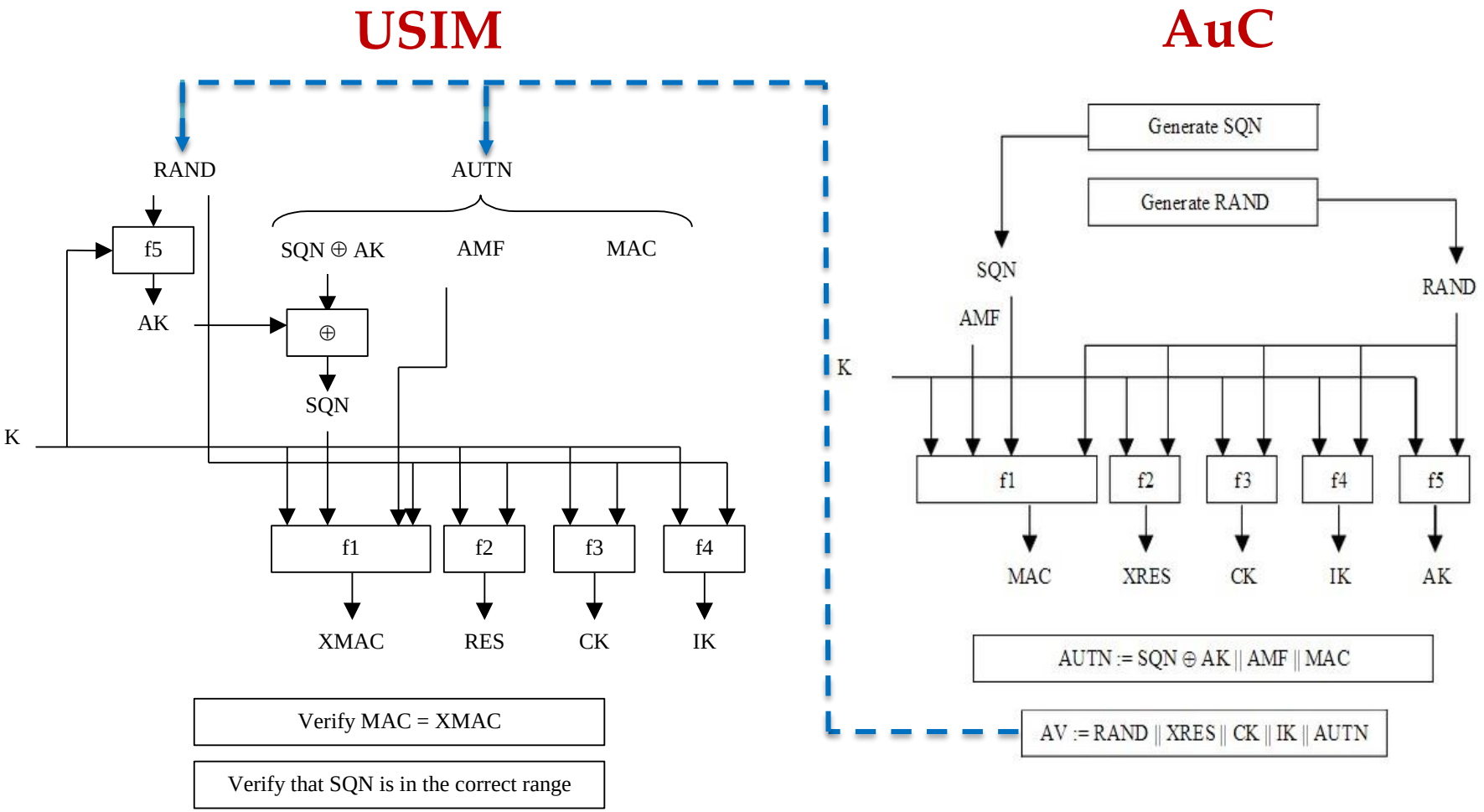
3G/4G USIM 认证是否 *物理* 安全?

3G/4G AKA 协议（简化版）

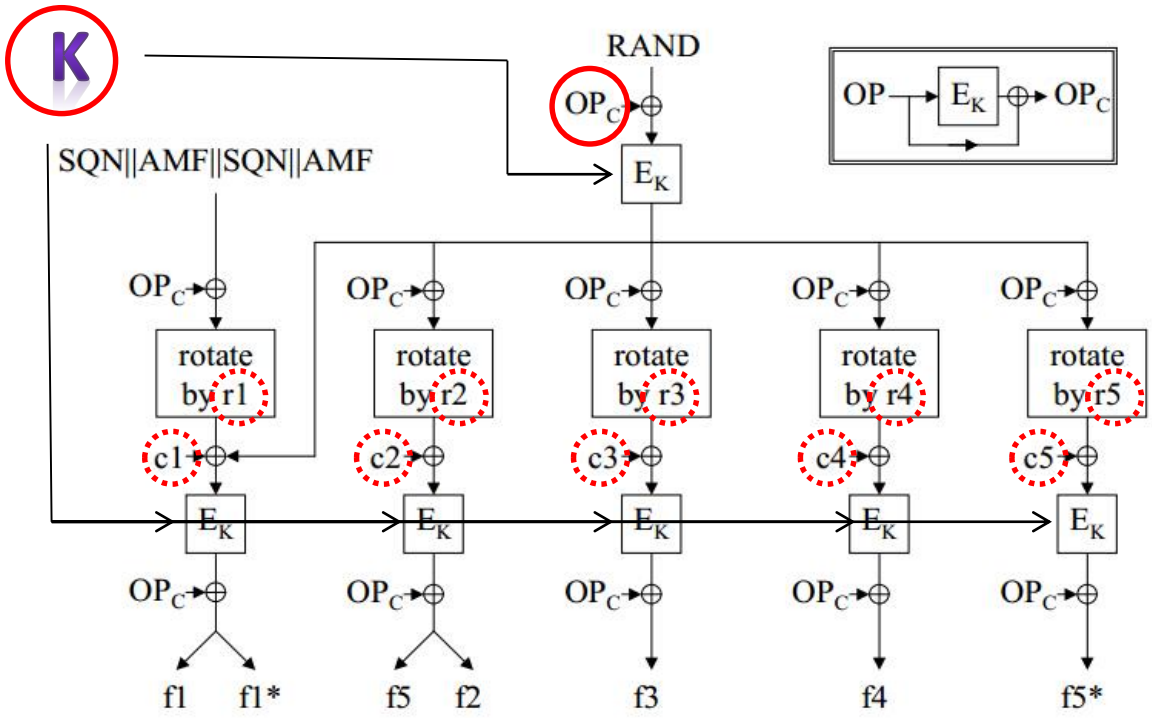


3G 与 4G 的AKA协议并不完全相同，但不同之处与其安全性无关

MILENAGE 算法


USIM
AuC
RAND
AUTN
f5
SQN ⊕ AK
AMF
MAC
AK
⊕
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verify MAC = XMAC
Verify that SQN is in the correct range
Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

USIM卡上进行的计算



K + OPc (+ r1,c1, r2,c2, r3,c3, r4,c4, r5,c5)

如何恢复卡上的保密信息?

- 策略: “分而治之(Divide et impera)”

破解密码组合是困难的

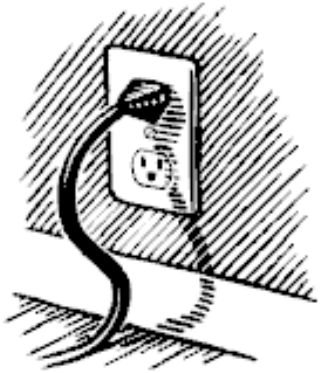
如果能将单个困难问题拆分成多个**独立**的子问题，情况将会大大不同

- 我们的工作: 利用功耗分析将 K, OPc, r1,c1, …, r5, c5 逐一恢复
  - 对于secret ∈{K, O*P*c, c1, c2, …, c5 }
    进行差分功耗分析(Differential Power Analysis)
  - 对于secret ∈{r1, r2, …, r5 }
    进行(非标准) 相关功耗分析 (Correlation Power Analysis)

旁路攻击 (Side Channel Attack)

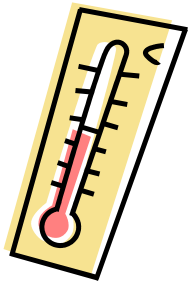
电磁辐射

（简单/差分）功耗



时间

声音



温度

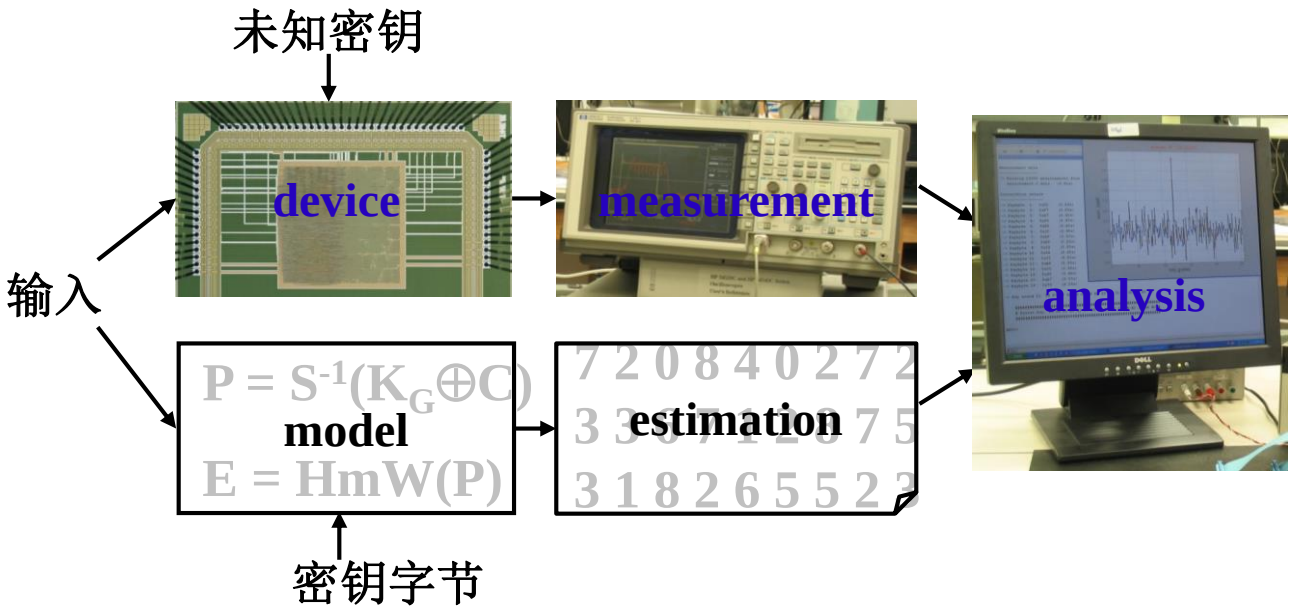
实验环境

电脑
+
旁路分析软件
SCAnalyzer

示波器

功耗采集平台
Power
Recorder

差分功耗分析 (Differential Power Analysis)

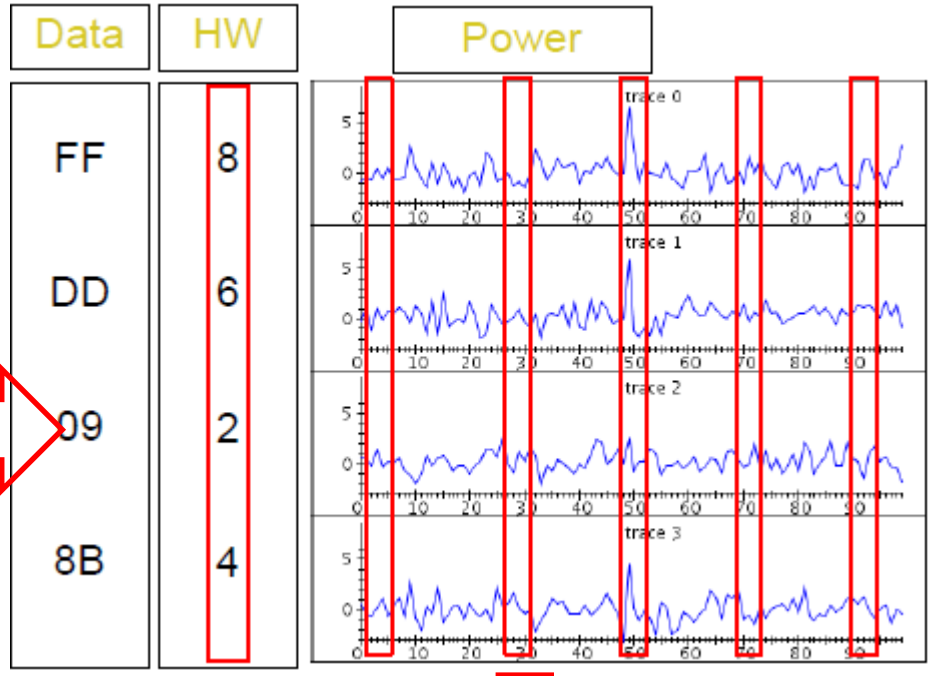


- AES: 128-bit 密钥 暴力穷举 几乎不可能
- 穷举单个密钥字节（256种可能） 容易
- 验证猜测是否正确 正确值与功耗有较高相关性
- 对每个密钥字节独立地进行搜索、验证和恢复

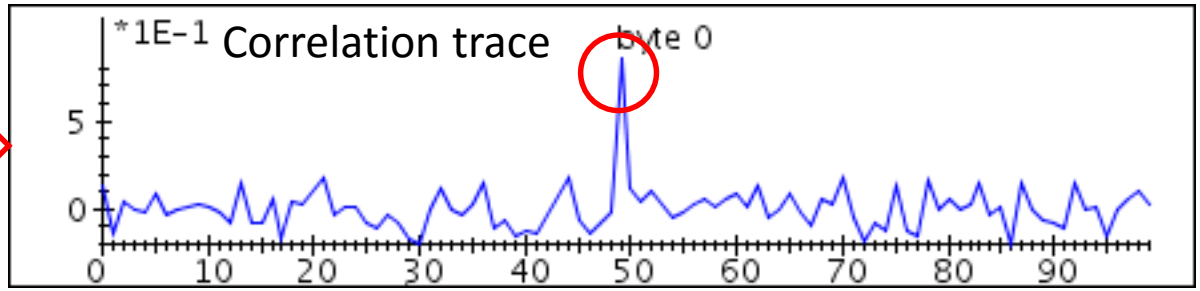
差分功耗分析 (续)

如何测试一个密钥字节的猜测正确与否?

计算(基于猜测密钥值)中间变量值与功耗曲线之间的相关性

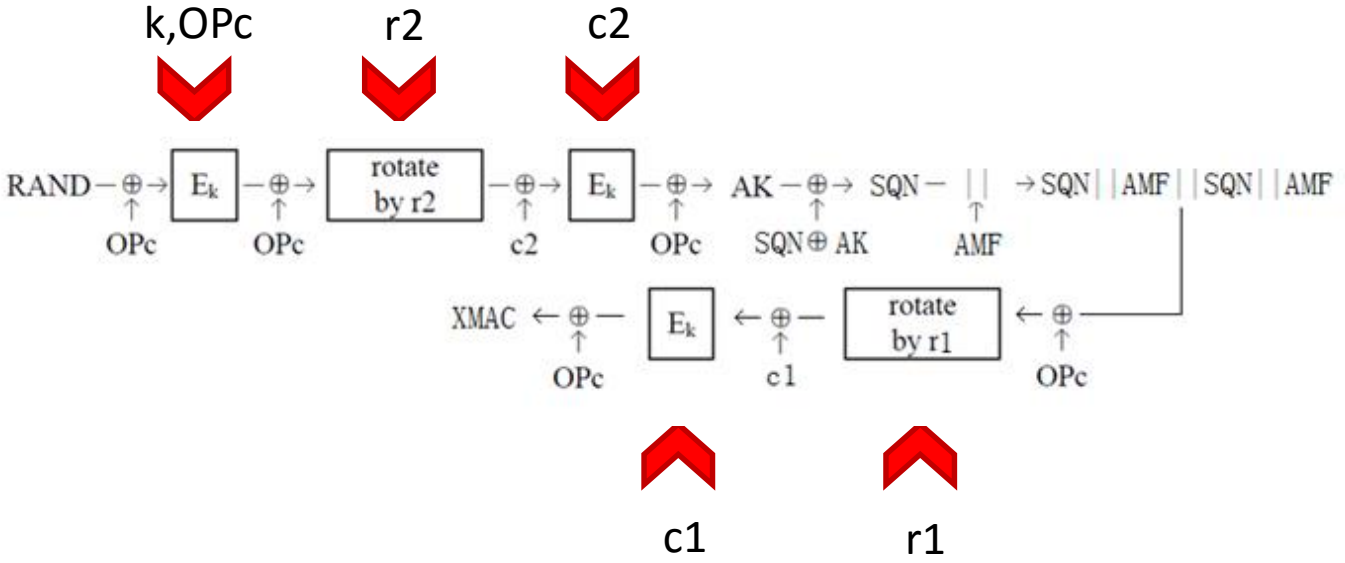


猜对的密钥值：相关性出现峰值



攻击哪些部位？

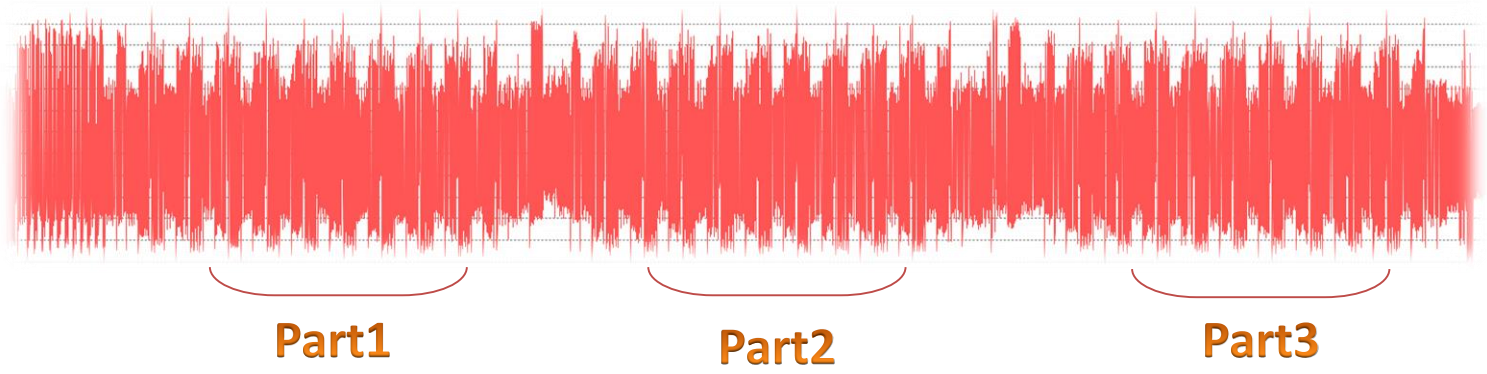
保密信息: k, OPc, r1~r5,c1~c5



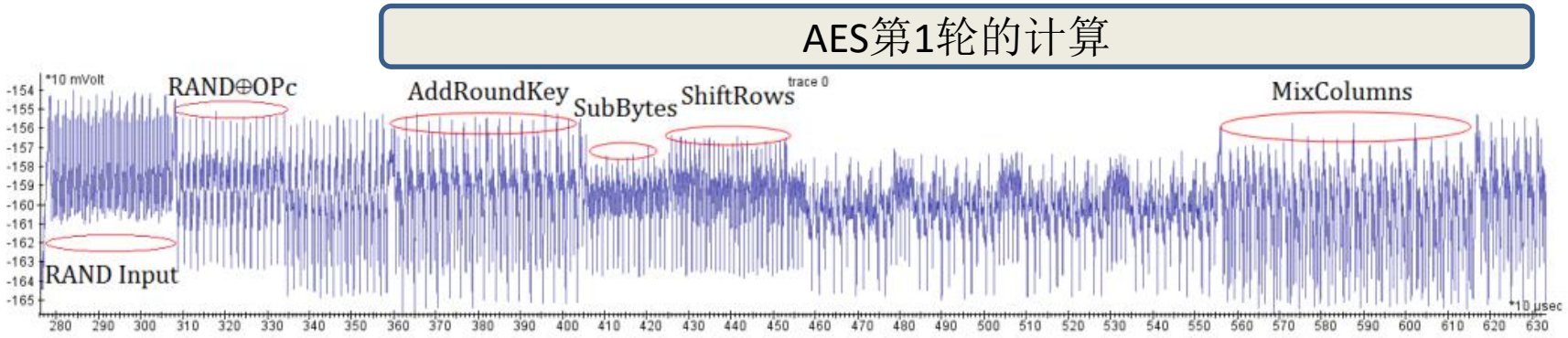
子函数 **f5+f1**

分析过程

第一步：采集功耗曲线



在整条曲线上找到兴趣点 (simple power analysis)
放大后进行相关的分析

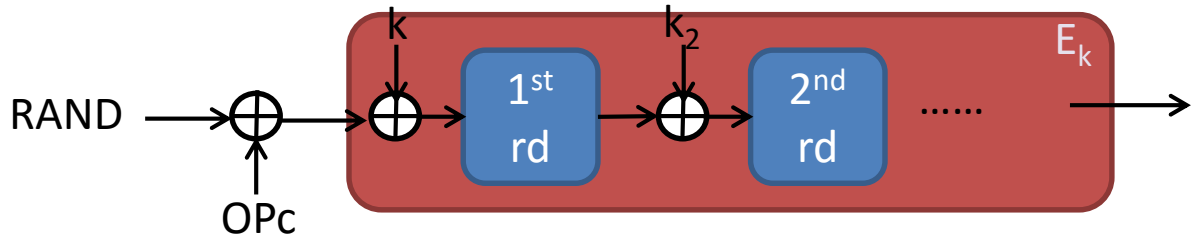


分析过程

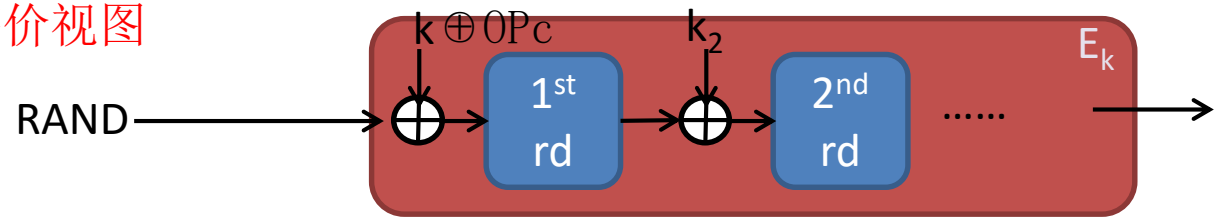
第二步: 恢复 K 和 OPc

已知的差分功耗分析：从 RAND → E_k → 恢复密钥 k

如何利用差分功耗分析从 RAND → ⊕ ← OPc, ⊕ → E_k 恢复 k 和 OPc ?



等价视图



攻击AES 第1轮: (视作密钥为k'=k⊕OPc) 恢复k⊕OPc

攻击AES 第2轮: 恢复第二轮的轮密钥 k_2 (进而恢复主密钥 k)

分析过程

第三步：恢复 $r_1, \ldots, r_5$

- 将 r 写作 $r = 8i + j$

$$v_0 v_1 \ldots v_{127} \xrightarrow{\text{right cyclic shift by } r \text{ bits}} \underbrace{(v_j v_{j+1} \ldots v_{j+7})}_{\text{byte 0}} \cdots \underbrace{(v_{j+120} \ldots v_{127} v_0 \ldots v_{j-1})}_{\text{byte 15}}$$

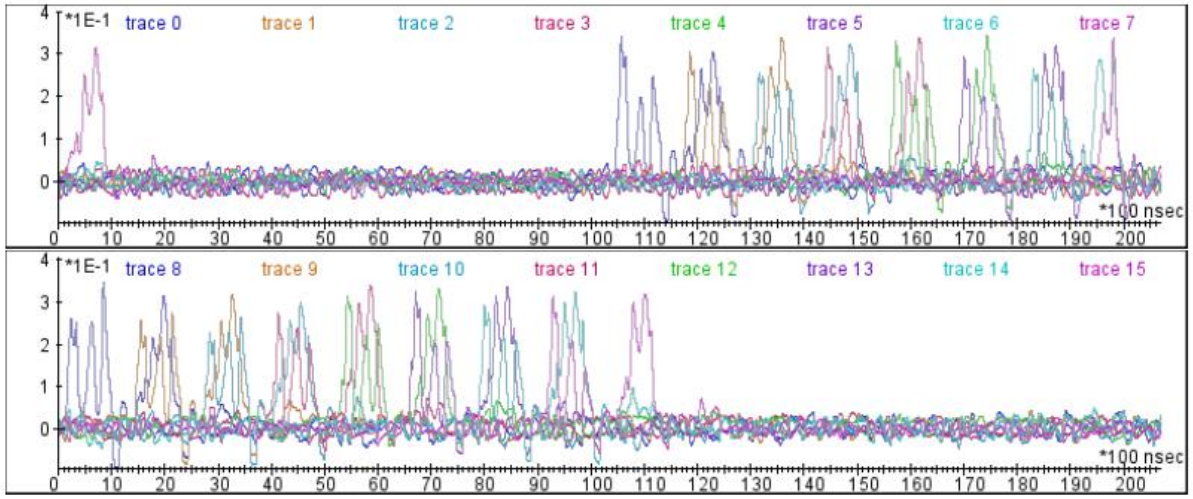
1. **恢复 j** (不妨假设 $i = 0$)

   对 j 进行猜测(8种可能) 并逐一进行假设验证(hypothesis testing)

   (计算 byte 0 与功耗曲线之间的相关性)

2. **恢复 i** 计算所有字节 bytes 0 ~15 与功耗曲线的相关性,

   那么 i 即为相关性曲线在时域上的平移



分析结果

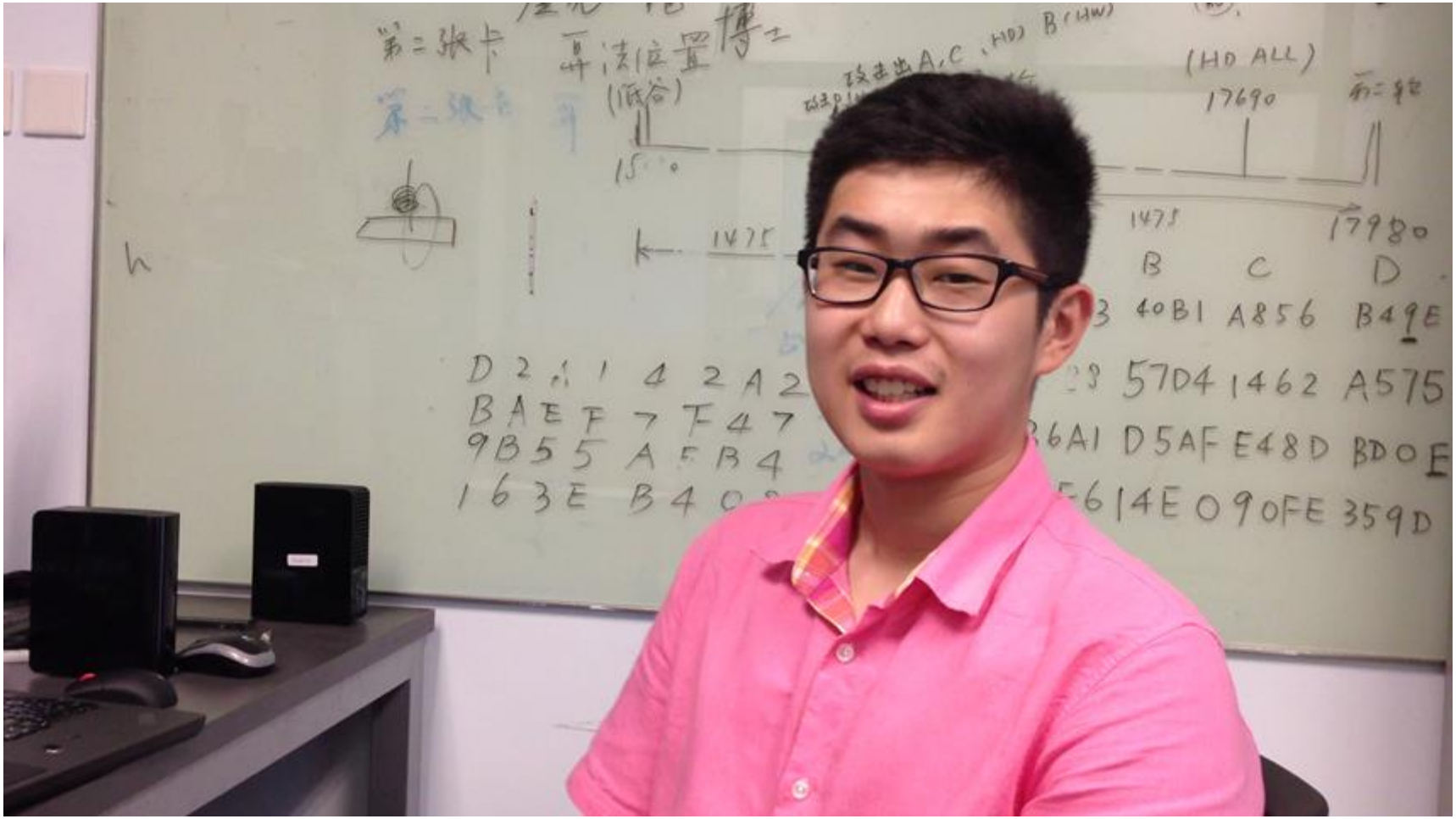
Target USIM	operator	manufacturer	technology	secrets
#1	C1-1	C1-I	3G UMTS	K, OPc
#2	C1-1	C2-II	3G UMTS	K, OPc
#3	C1-1	C1-III	3G UMTS	K, OPc
#4	C1-2	C3-I	3G UMTS	K, OPc, r1,c1,…,r5,c5
#5	C2-1	C2-I	3G UMTS	K, OPc, r1,c1,…,r5,c5
#6	C1-3	C1-IV	4G LTE	K, OPc, r1,c1,…,r5,c5
#7	C1-3	C1-II	4G LTE	K, OPc, r1,c1,…,r5,c5
#8	C2-2	C2-II	4G LTE	K, OPc, r1,c1,…,r5,c5

恢复所有保密信息需要的时间和数据量：10到80分钟不等

200到1000条功耗曲线

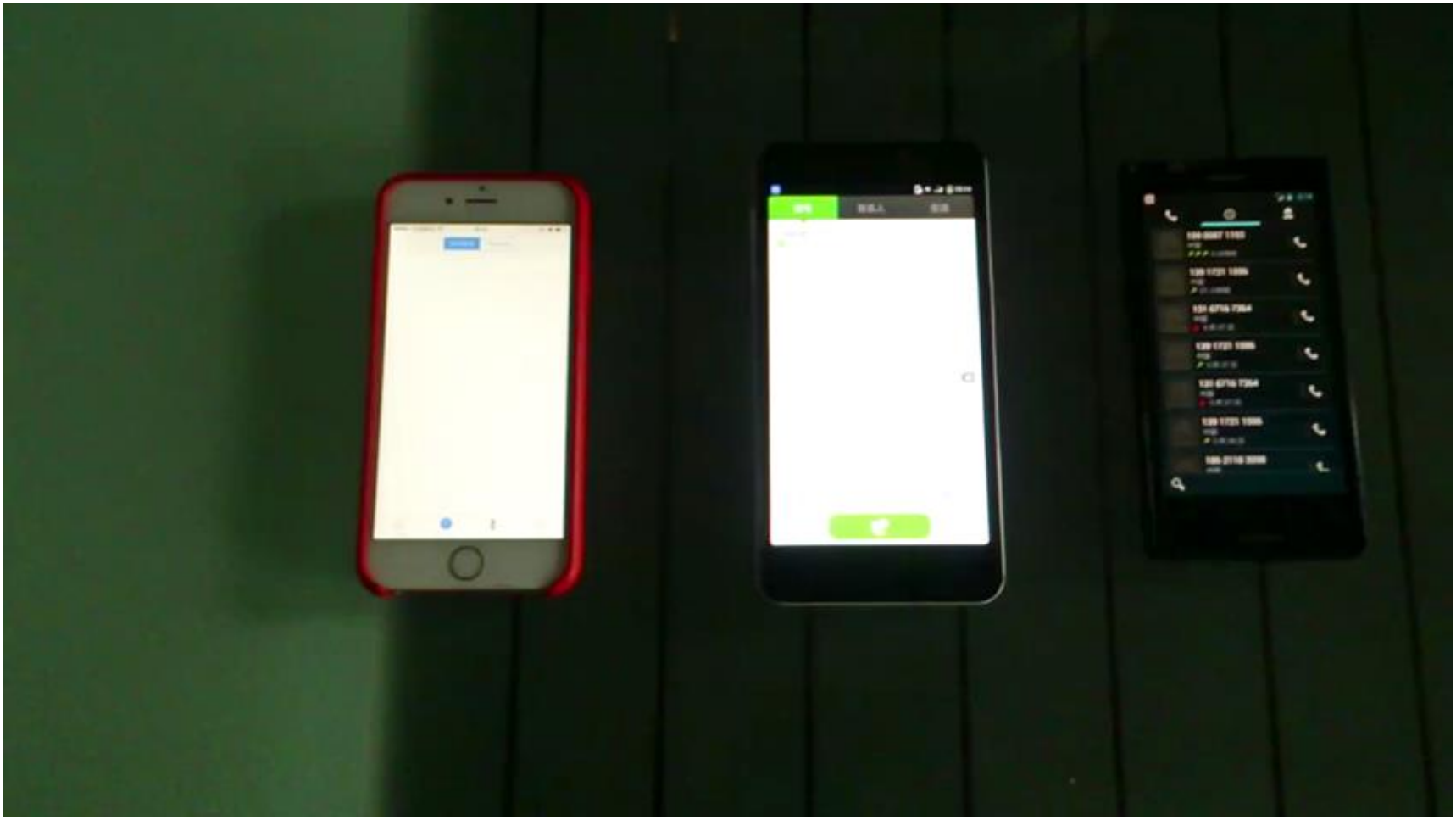
对运行商和制造商做了匿名处理

演示 1


(HD ALL)
17690
B C D
40B1 A856 B4?E
57D4 1462 A575
D5AF E48D BD0E
614E 090FE 359D

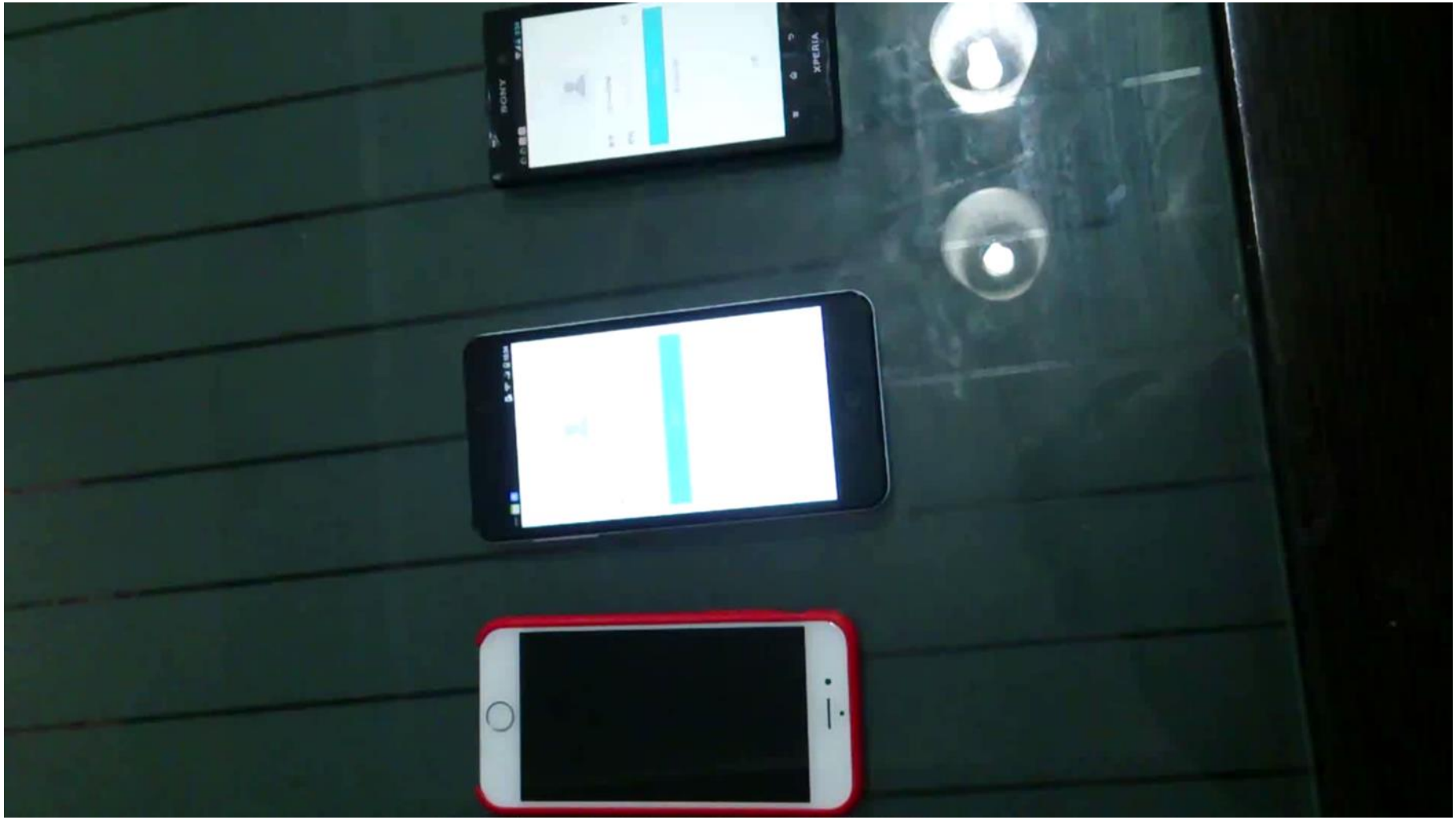
演示 2

原卡、克隆卡分别拨打电话



演示 3

移动客户端APP：绕过基于手机OTP的身份认证



第三部分 经验教训

1. 密码学. 对于加密算法，引入密钥以外保密信息并不额外增加算法的安全性。

2. 现实中的矛盾:
   - ➢低成本芯片 ≈ 没有预算进行 CC/EMVCo/FIPS 等安全评估测试
   - ➢低成本 × 巨大的发行量 = 重大的安全隐患

3. 嵌入式芯片物理安全的重要性

   现实的安全性:
   - ➢不仅需要数学设计上安全(且公开)的加密算法.
   - ➢也需要足够的物理安全防护措施

Thanks

更多技术细节，参见论文 *Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards*