3G/4G USIM卡的安全性分析

葛毅杰
上海交通大学 LoCCS实验室

目 录

目 录

1 背景

Edward Snowden reveals that NSA and GCHQ hacked SIM card manufacturer Gemalto: reports

BY ALEJANDRO ALBA / NEW YORK DAILY NEWS / Thursday, February 19, 2015, 4:12 PM

A A A

2

Share Tweet Reddit

SHARE THIS URL

nydn.us/1Dx3Je0 COPY

BRIAN JACKSON/GETTY IMAGES/ISTOCKPHOTO

The NSA and the Government Communications Headquarters targeted Gemalto, a multinational firm in the Netherlands that makes mobile phone SIM cards, to monitor mobile communications on respective SIMs without permission from telephone companies.

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 sold by Gemalto.

多种威胁

克隆

窃听

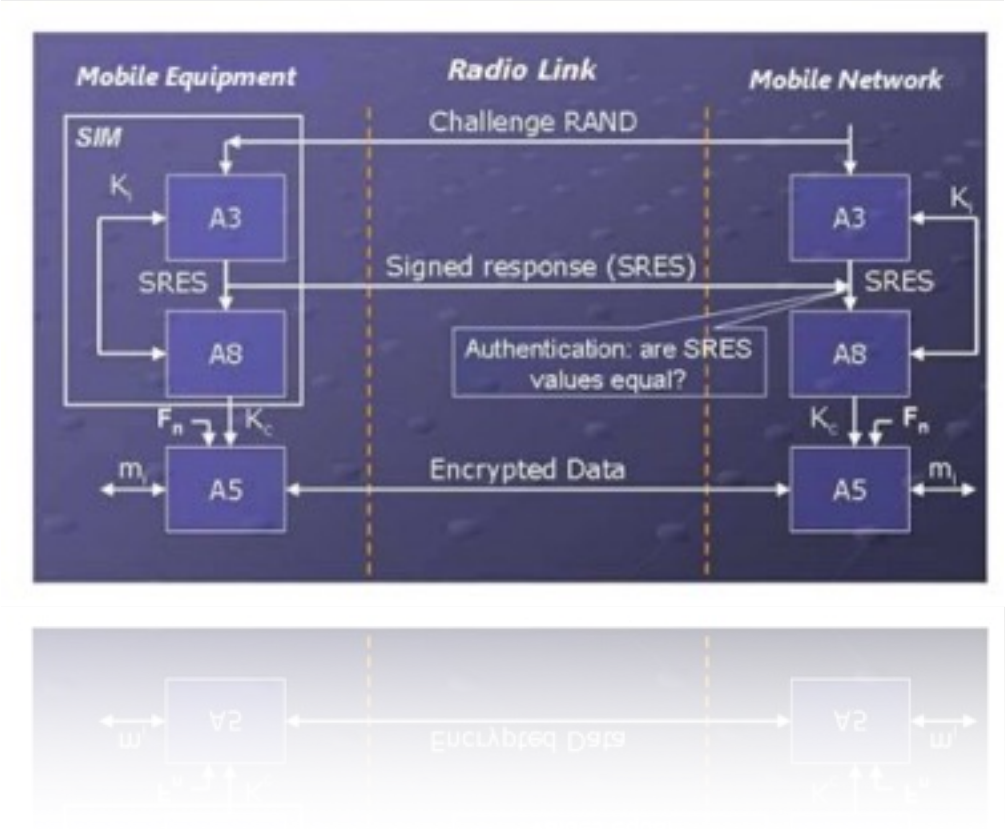
木马

几十亿的SIM卡面临着重大的安全威胁

目 录

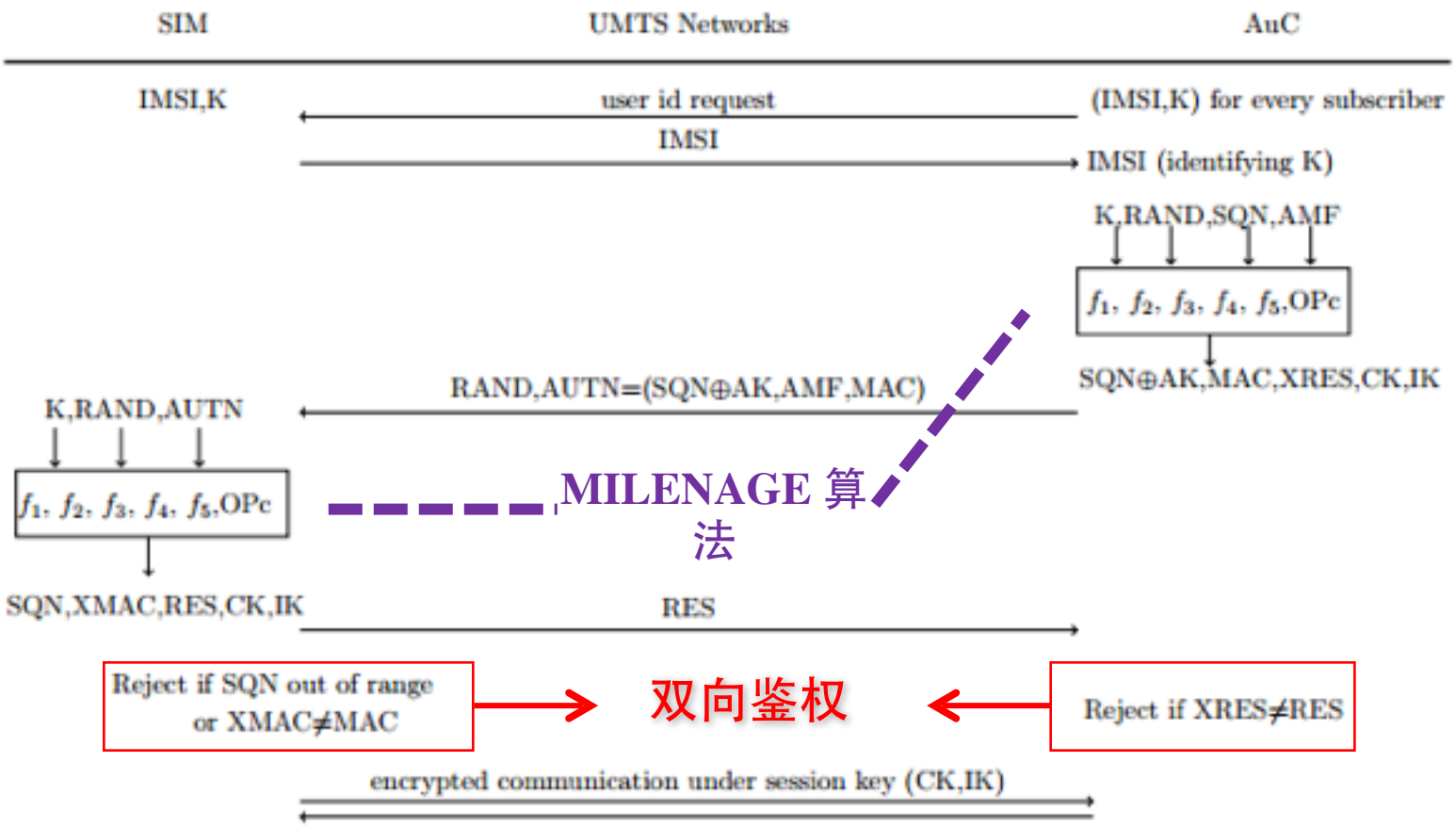
2G早已千疮百孔

2G鉴权



1. 单向鉴权无法辨别伪基站
2. 鉴权算法本身存在漏洞
3. 面对旁路攻击显得非常脆弱

3G/4G的鉴权流程

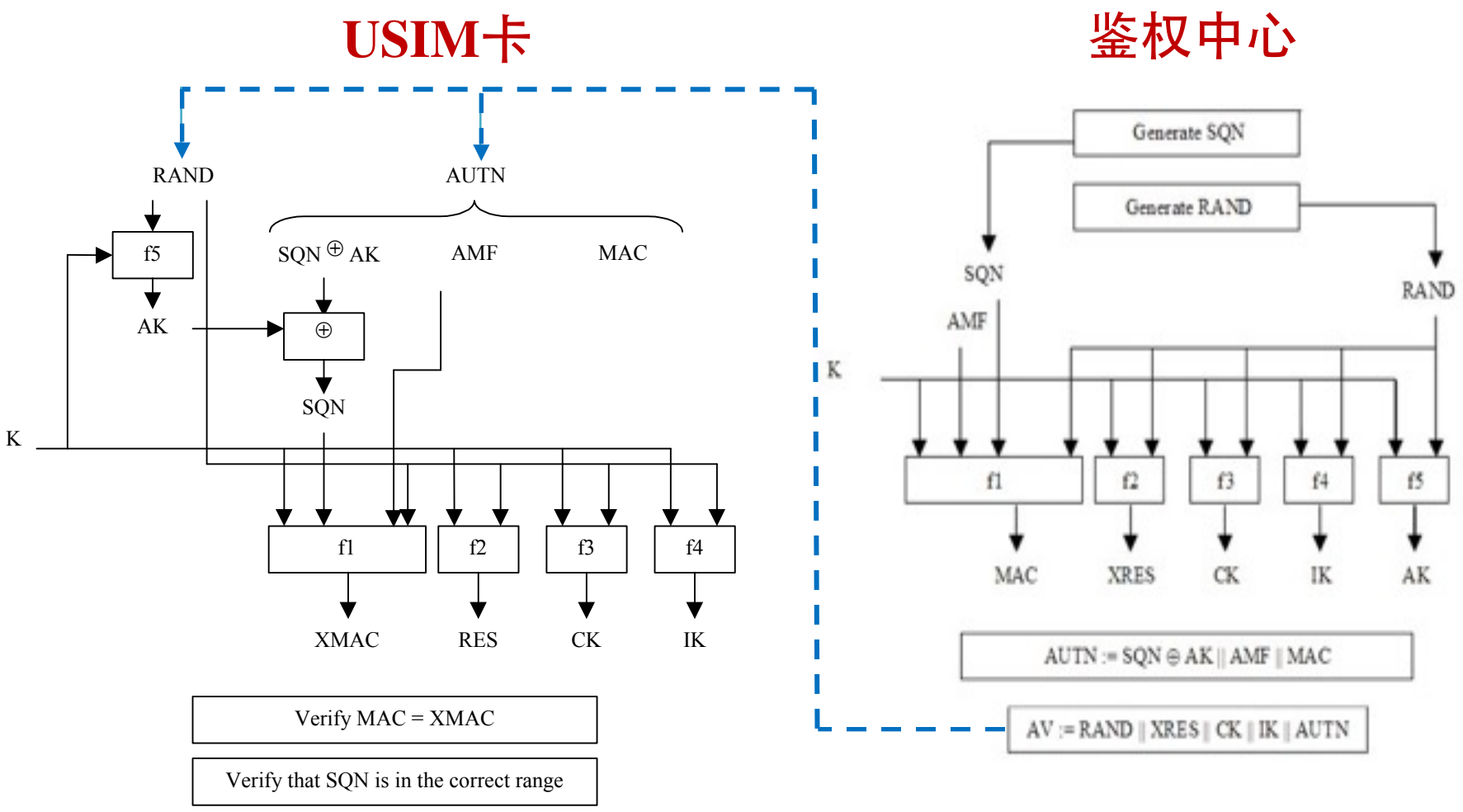

SIM
UMTS Networks
AuC
IMSI,K
user id request
(IMSI,K) for every subscriber
IMSI
IMSI (identifying K)
K,RAND,SQN,AMF
f_1, f_2, f_3, f_4, f_5,OPc
SQN⊕AK,MAC,XRES,CK,IK
RAND,AUTN=(SQN⊕AK,AMF,MAC)
K,RAND,AUTN
f_1, f_2, f_3, f_4, f_5,OPc
MILENAGE 算法
SQN,XMAC,RES,CK,IK
RES
Reject if SQN out of range or XMAC≠MAC
双向鉴权
Reject if XRES≠RES
encrypted communication under session key (CK,IK)

2G vs 3G/4G

	2G	3G/4G
鉴权算法	***Comp128 15***年前就被发现存在漏洞	***MILENAGE*** 算法基于***AES-128+***循环移位***+***异或， 没有明显漏洞
单向还是双向鉴权	单向鉴权，面临着伪基站的威胁	双向鉴权 可以识别伪基站
其它	没有对于同步性和完整性的考虑	采用***SQN***来保证同步性，并且采用许多其它策略来保证 ***UE***、 ***eNB*** 、***MME***间通信信息的完整性

但是这些改进够吗？

MILENAGE 算法

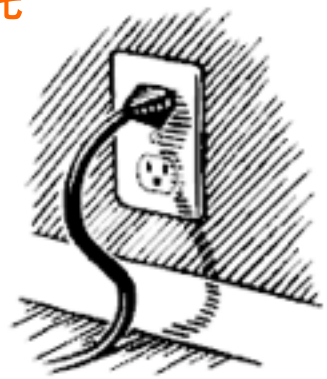

USIM卡
鉴权中心
RAND
AUTN
f5
AK
SQN ⊕ AK
AMF
MAC
⊕
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verify MAC = XMAC
Verify that SQN is in the correct range
Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

目 录

旁路攻击(Side Channel Attack)

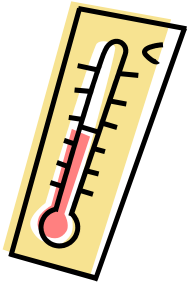
电磁

功耗



时间

声音



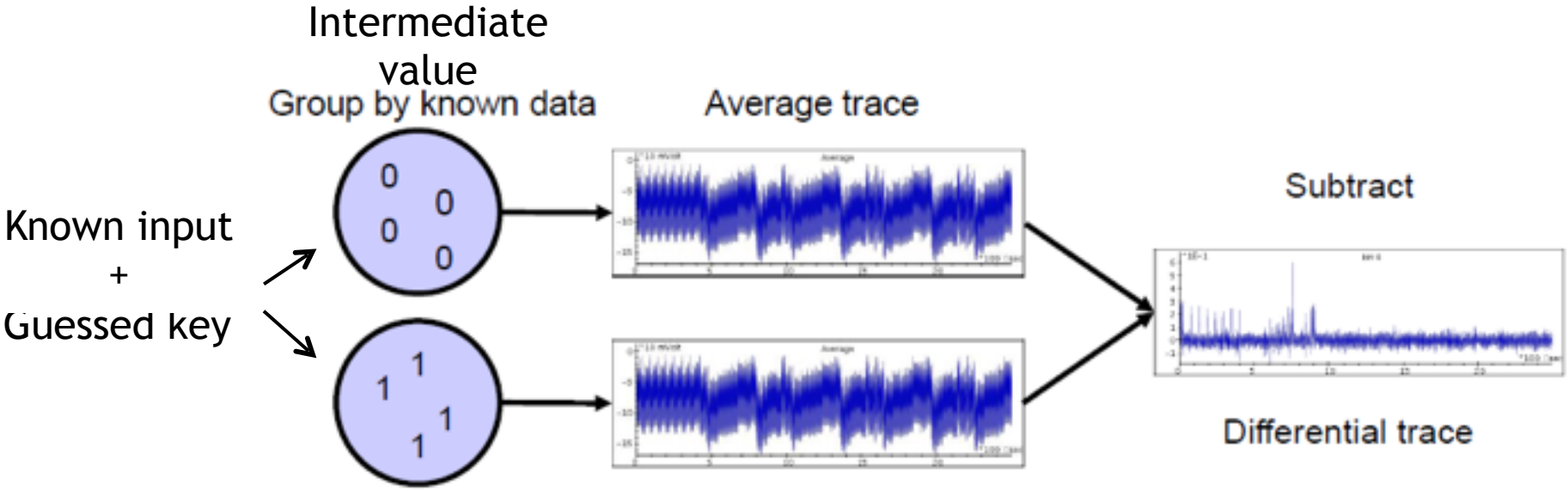
温度

功耗分析

- 简单能量分析SPA

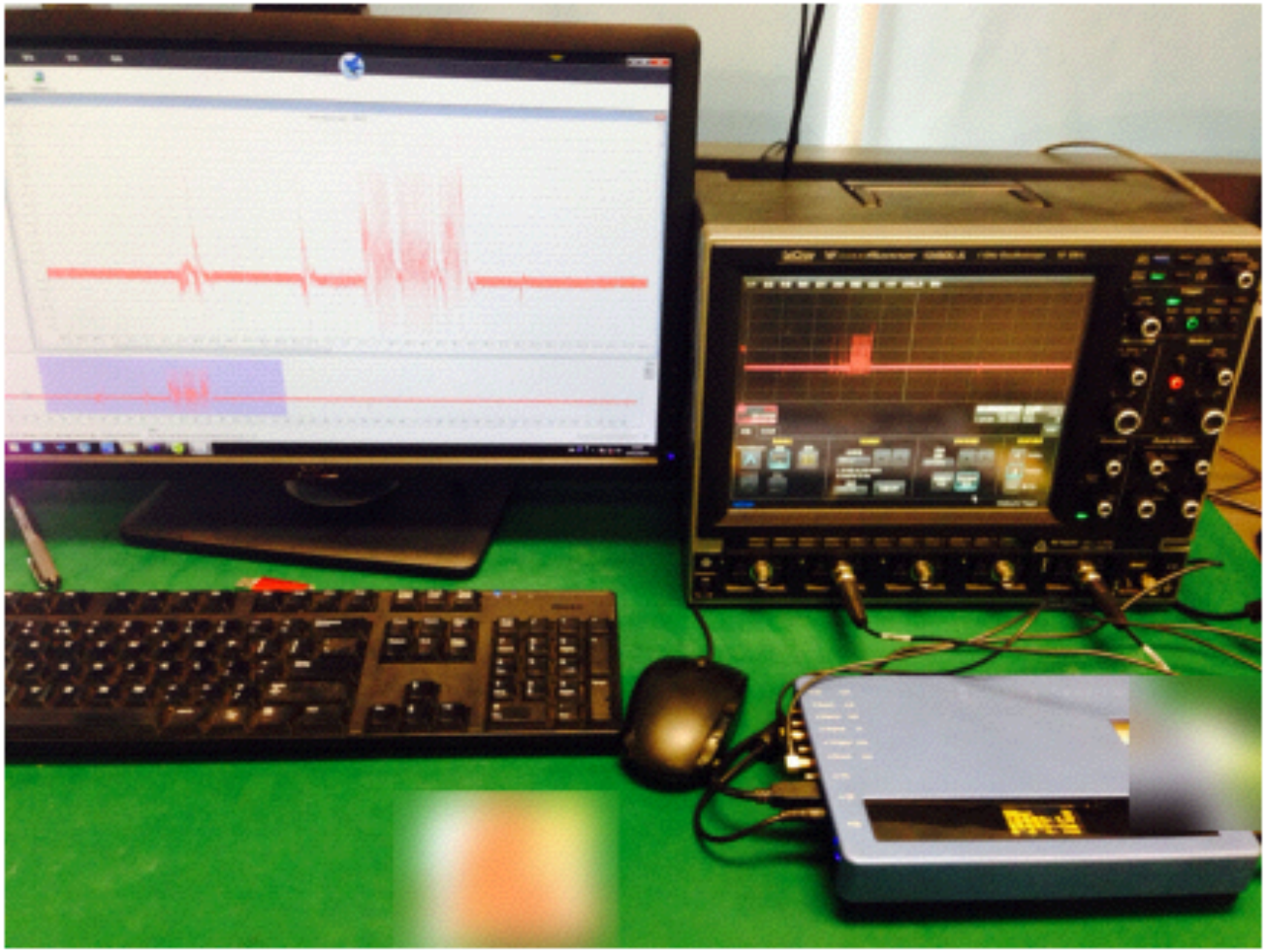
  根据观察一条或几条功耗曲线的特点，来推断出加密算法的相关信息。

- 差分能量分析DPA



实验环境

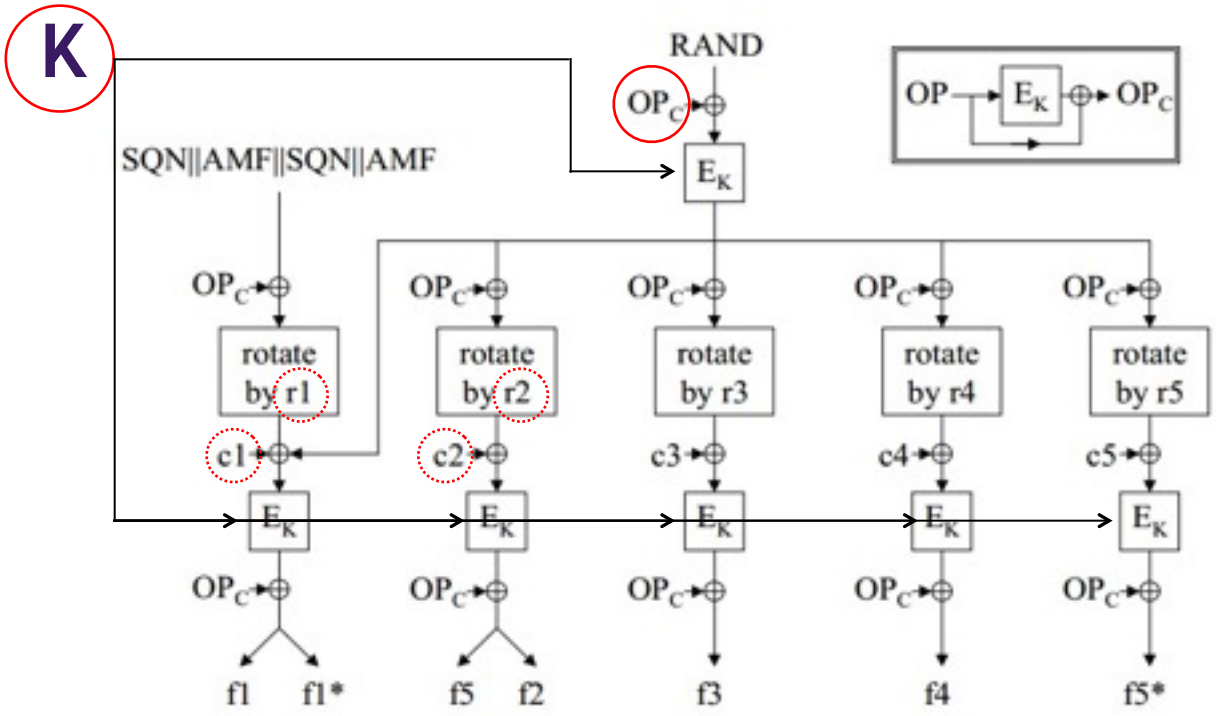
PC
+
SCAnalyzer



Oscilloscope

Power
Recorder

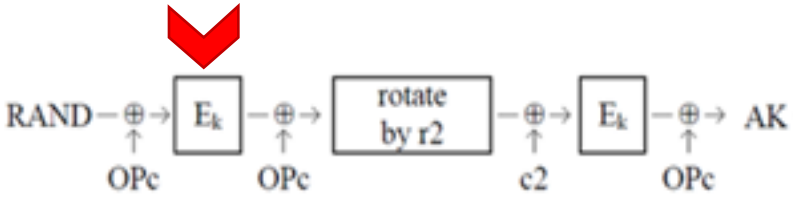
我们需要得到哪些信息?



K + OPc + r,c

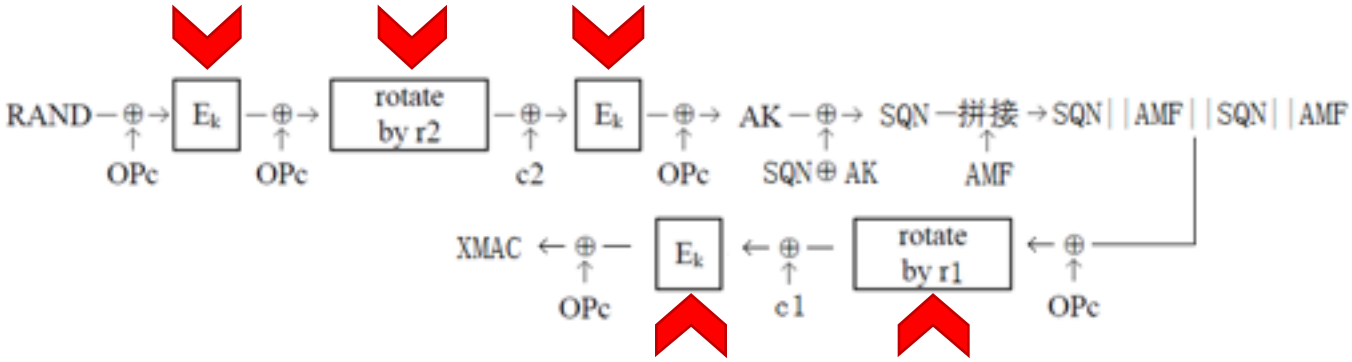
分析什么位置?

场景1:
采用的是标准的
r1~r5,c1~c5



f5

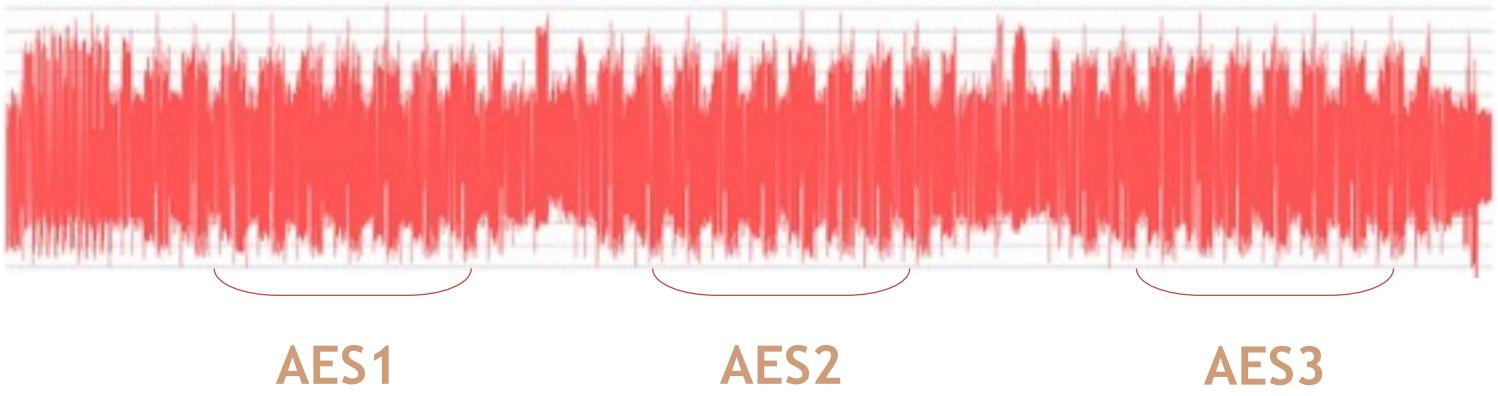
场景2:
自定义
r1~r5,c1~c5



f5+f1的流程

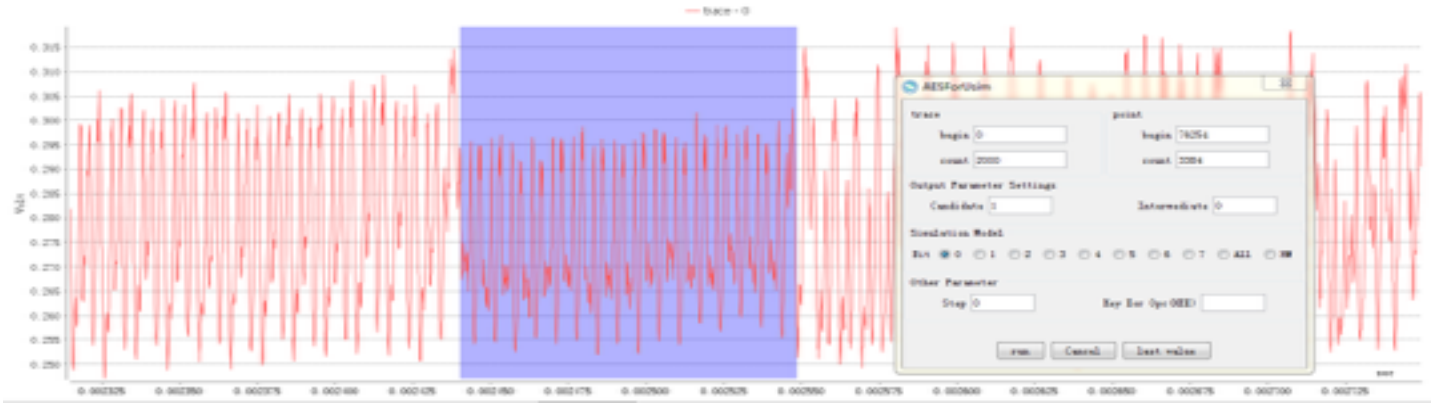
分析过程

第一步: 采集曲线

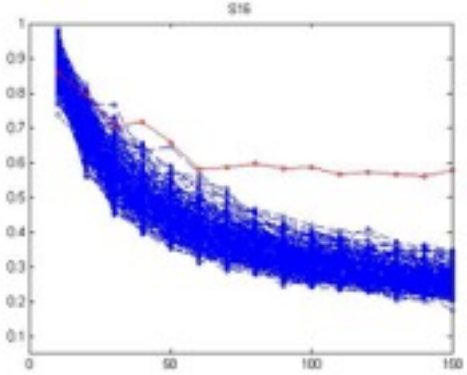


分析过程

第二步: 得到 K 和 OPC



分析第一轮



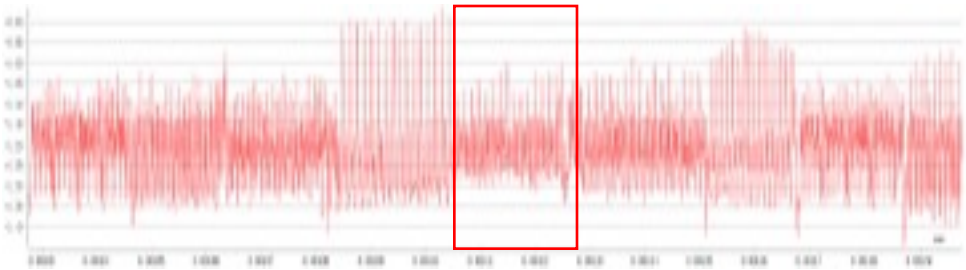
分析过程

第三步：验证通过？

自定义参数

Y

通过计算相关性来得到循环移位参数r

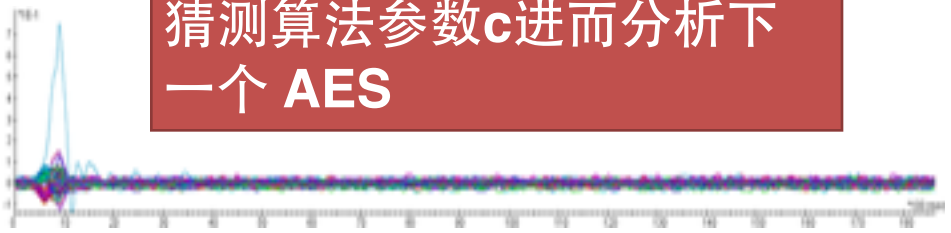


N

```
['INTERNAL AUTHENTICATE apdu: 00 88 00 81 22 10 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 10 00 00 00 00 00 00 00 00 A7 E1 8D EB 95 2E 6B 6F', 'sw1, sw2:
61 10 - normal processing: 16 bytes still available', (97, 16), []]
['GET RESPONSE apdu: 00 C0 00 00 10', 'sw1, sw2: 90 00 - normal processing: conn
and accepted: no further qualification', (144, 0), [220, 14, 248, 108, 88, 4, 23
0, 197, 83, 241, 149, 189, 255, 123, 111, 35]]
```

验证通过

猜测算法参数c进而分析下一个 AES



最后我们得到需要的参数r和c

我们的研究结果

target USIM	operator	manufacturer	technology	secrets
#1	AP-1	AP-I	3G UMTS	K,OPc
#2	AP-1	AP-II	3G UMTS	K,OPc
#3	AP-1	AP-III	3G UMTS	K,OPc
#4	AP-2	AF-I	3G UMTS	K,OPc, r_1, c_1, ...,r_5, c_5
#5	EU-1	EU-I	3G UMTS	K,OPc, r_1, c_1, ...,r_5, c_5
#6	AP-3	AP-IV	4G LTE	K,OPc, r_1, c_1, ...,r_5, c_5
#7	AP-3	AP-II	4G LTE	K,OPc, r_1, c_1, ...,r_5, c_5
#8	EU-2	EU-II	4G LTE	K,OPc, r_1, c_1, ...,r_5, c_5

目 录

结论

1. USIM卡的安全性相比前一代SIM卡有着更高的安全性要求，不仅是因为数量巨大，而且也因为如今手机的应用场合多种多样。

2. 基于AES128的MILENAGE算法，即使运营商可以选择自定义参数r1~r5和c1~c5，但是面对旁路功耗分析仍旧显得脆弱。

3. 我们的运营商可以考虑为USIM卡增加抗功耗分析的设计并且进行专业的安全性测试。

Thank you !»