上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security

Yu Yu

joint work with Junrong Liu, F-X Standaert, Zheng Guo
Dawu Gu, Sun Wei, Yijie Ge, Xinjun Xie

black hat USA 2015

SHANGHAI JIAO TONG UNIVERSITY
LoCCS
密码与计算机安全实验室
Lab of Cryptology and Computer Security

Some recent updates

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."

Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Part1 Background

Cellular networks (1-4G)

- 1G: analogue signal

- 2G: GSM vs. CDMA

  digital signal

- 3G/4G: UMTS/LTE

high-speed data transmission

Part1

What is a (U)SIM card?

- (U)SIM = (Universal) Subscriber Identity Module
- (U)SIM is a smart card (a mini computer).
- SIM stores ICCID (serial number), IMSI (USER id), secrets, etc.
- Secret on 2G SIM: master key K.
- Secrets on 3G/4G USIM:

  master key K, and OPc, r1, r2, …, r5, c1, …, c5.
- Currently, 2G → 3G/4G → 5G
- Any cryptography in (U)SIM?

Part1

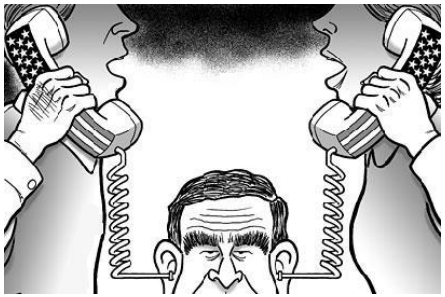
Security compromised by revealed/stolen secrets

CLONING

TAPPING

TROJAN

FRAUDULENT CALLS
OTP AUTHENTICATION



Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Part1

Cryptology in a nutshell

Cryptology = “Cryptography” + “Cryptanalysis”

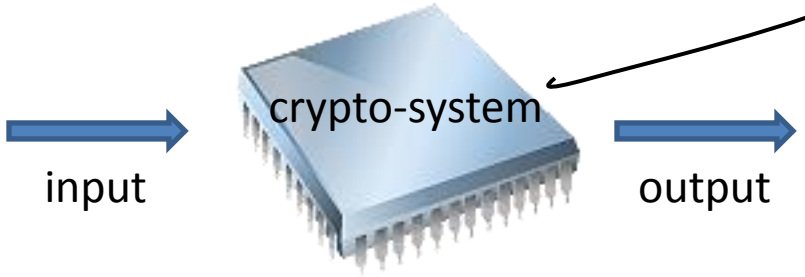
- Cryptography (designing )

The design of crypto-systems that help preserve various aspects of information security such as confidentiality, integrity, authenticity and non-repudiation.

- Cryptanalysis (code-breaking).

1. Mathematical: break a crypto-system mathematically.
2. Physical: break the implementation of a crypto-system.

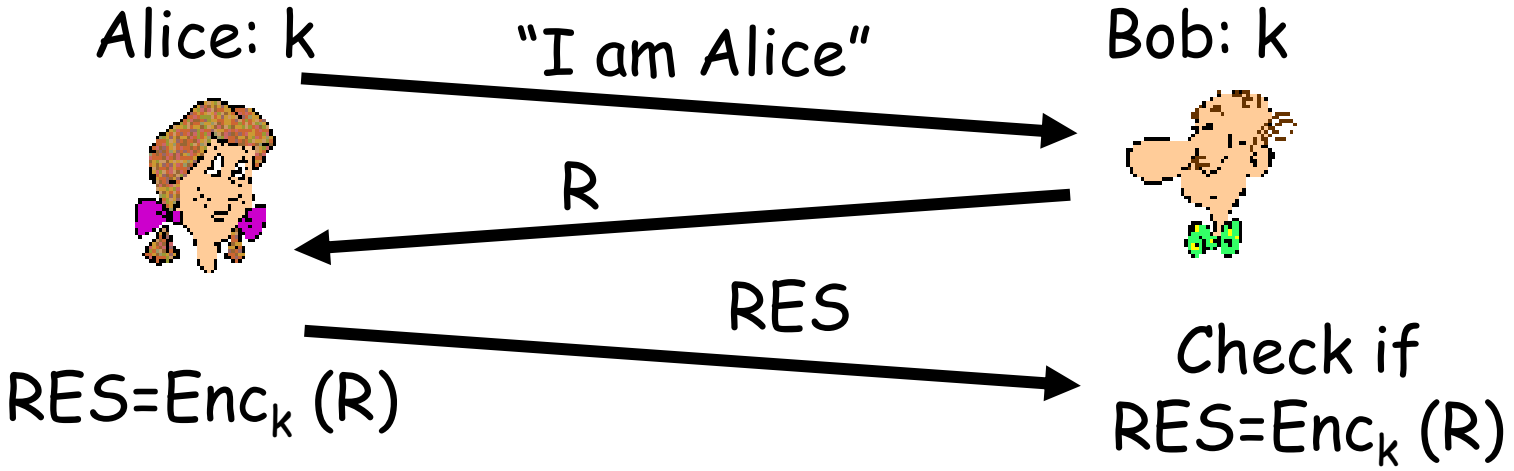
Attacks in real life are often physical.



Part1

What cryptography is needed for (U)SIM?

- AKA (Authentication and Key Agreement)
- Authentication is a process that ensures and confirms a user's identity.
- Bob authenticates Alice by **Challenge-and-Response**.

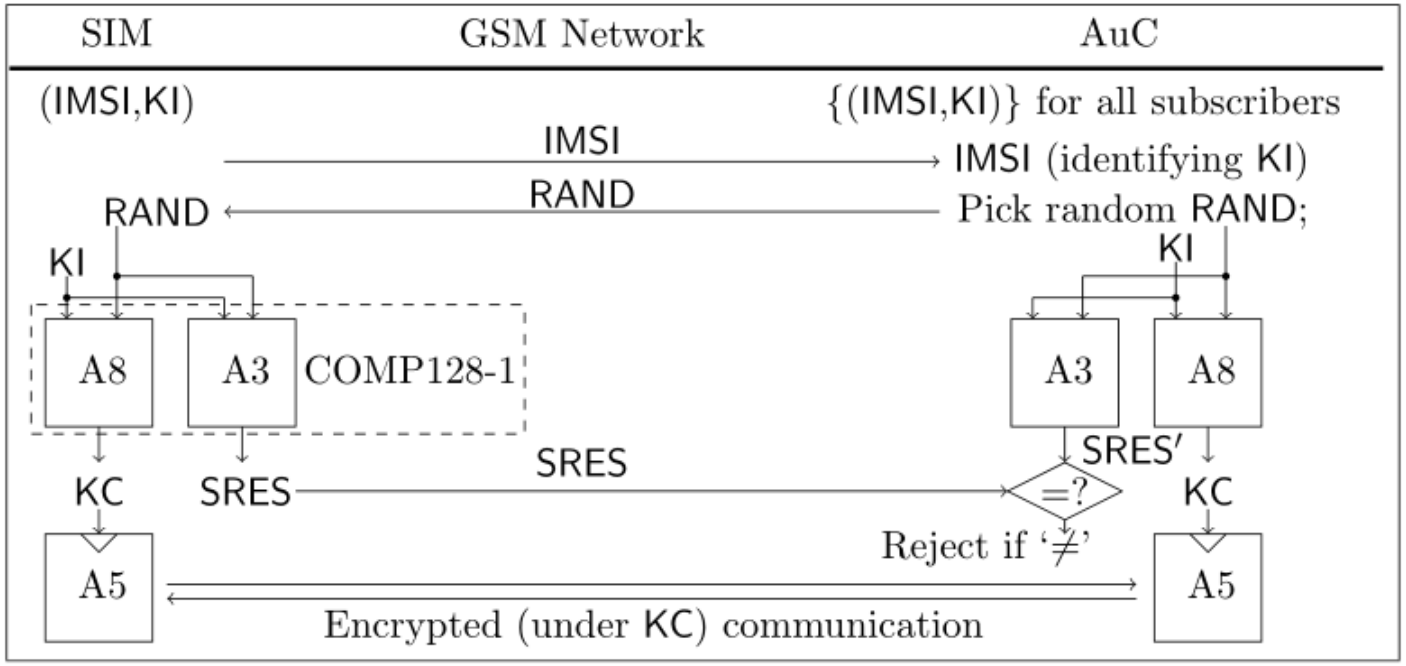


- Key Agreement (term not precise): deriving session key from master key.
- How to do Key Agreement: use same protocol above

  (use partial Enc$_k$(R) for RES and the rest as session key)

Part1

The 2G GSM AKA Protocol



AKA algorithm: COMP128-1 (A3+A8)
Encryption algorithm (optional) : A5
Insecurity:

1. COMP128-1 is fatally flawed (narrow pipe attacks [BGW98])
2. Only one-way authentication (spoofing base stations, DEFCON 2010)
3. Subject to side-channel attacks (DPA attacks [RRST02,ZYSQ13])

Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Part2

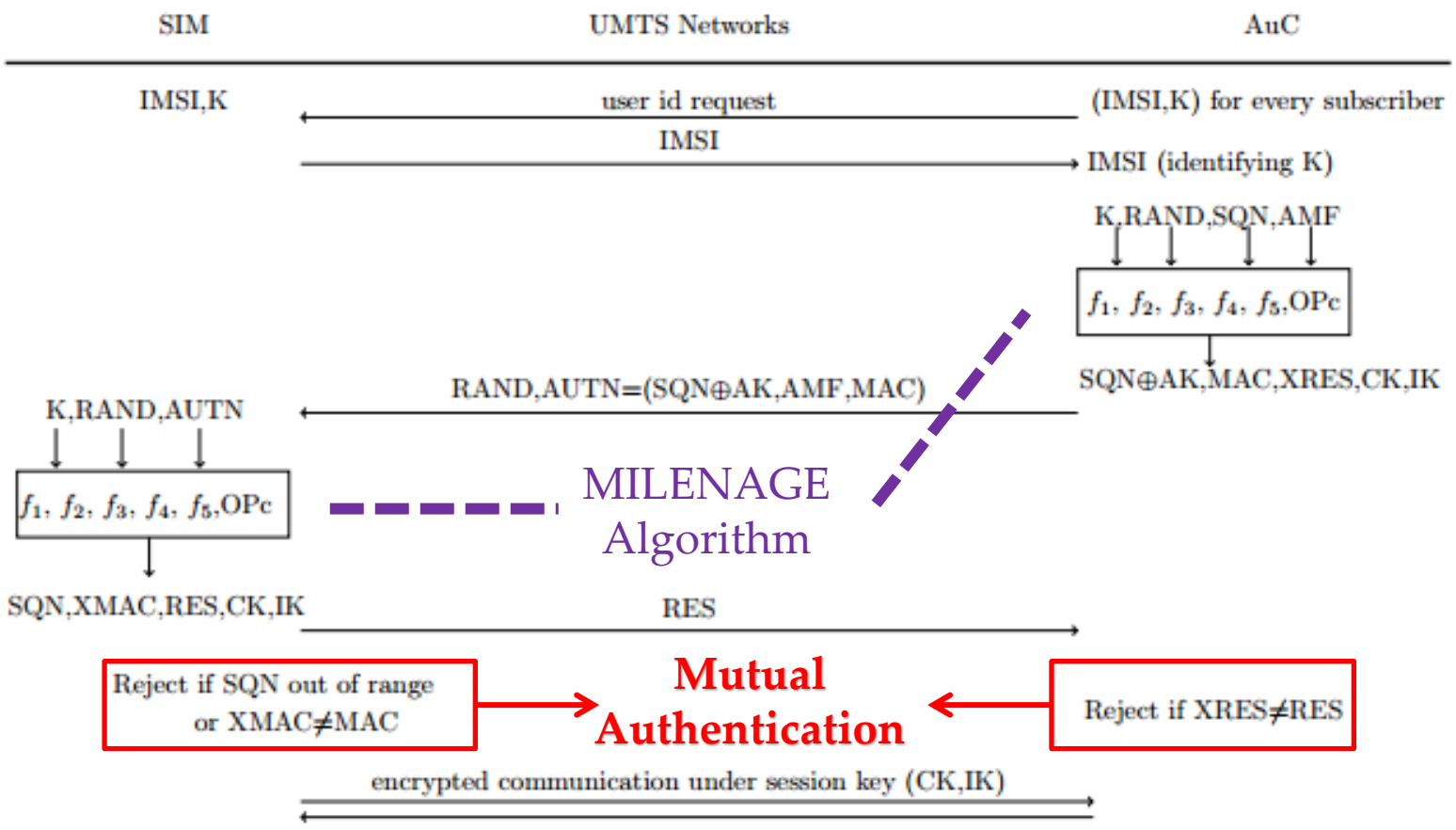
Security improvement of 3G/4G over 2G

	2G	3G/4G
Authentication Algorithm	flawed COMP128-1	MILENAGE, in turn based on AES-128, which is mathematically secure
Authentication mechanism	One-way (base station authenticates the SIM)	**Mutual authentication** (preventing spoofed base stations attacks)
Secrets	The master key K	The master key K The tweak value OPc More operator-defined values: r1, …, r5, c1, …, c5 (more secrets = better security?)

Is 3G/4G secure in practice?

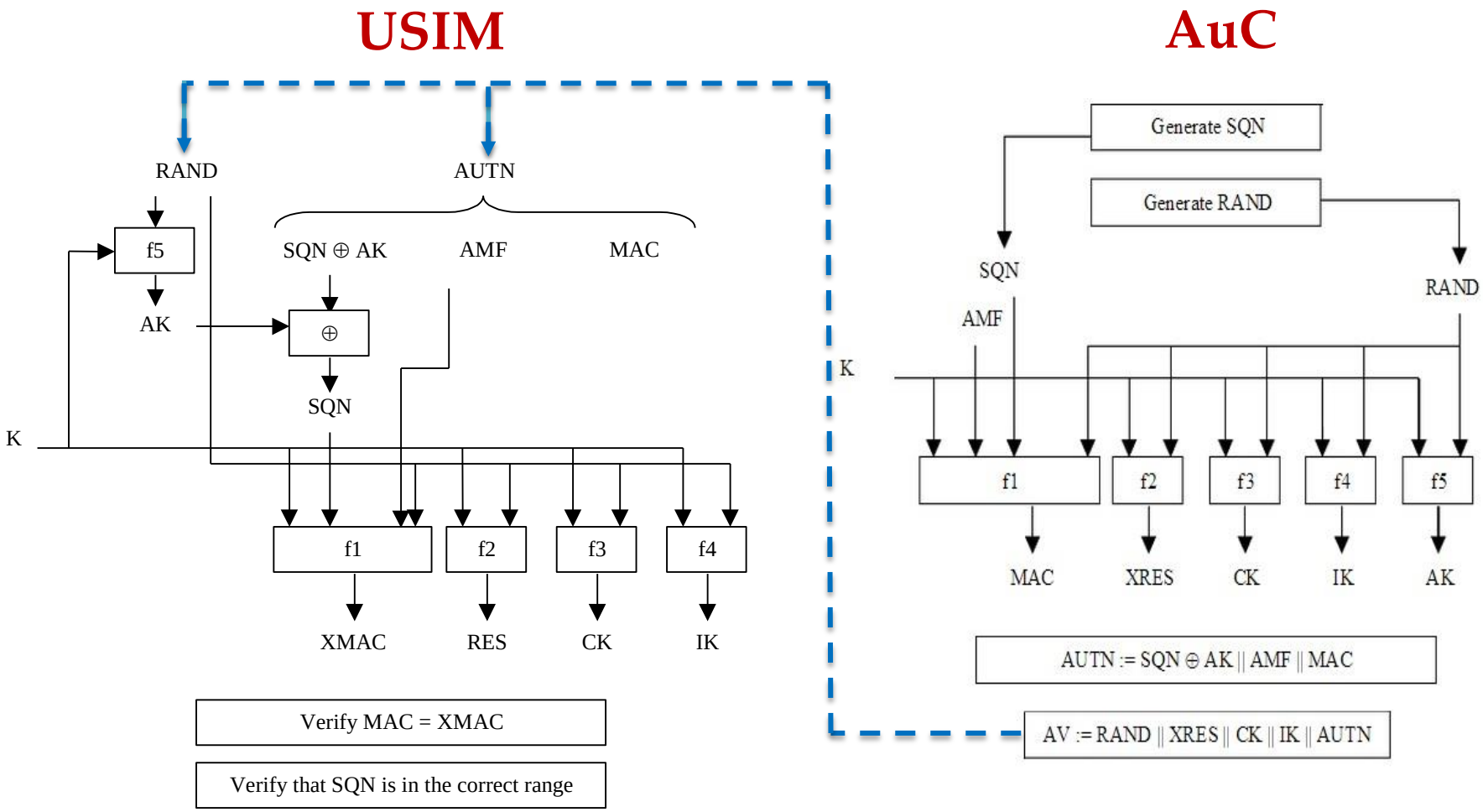
Part2

3G/4G AKA Protocol



Part2

MILENAGE Algorithm



Outline

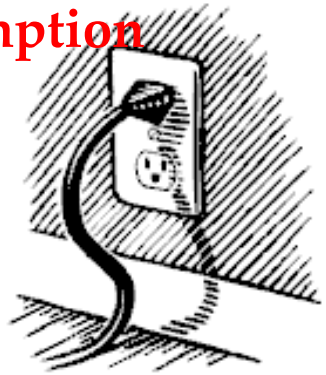
- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Part2

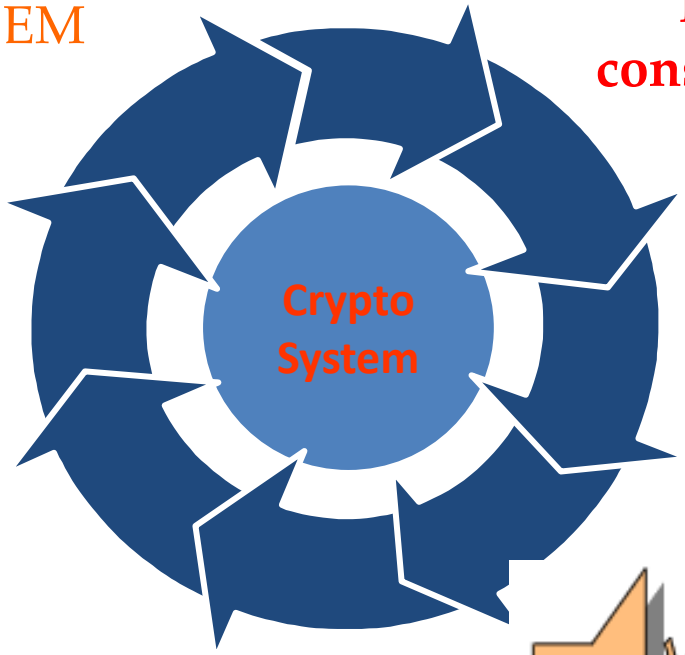
SCA (Side Channel Attack)

EM

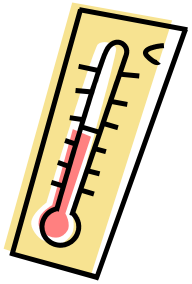
Power consumption



Time



Sound



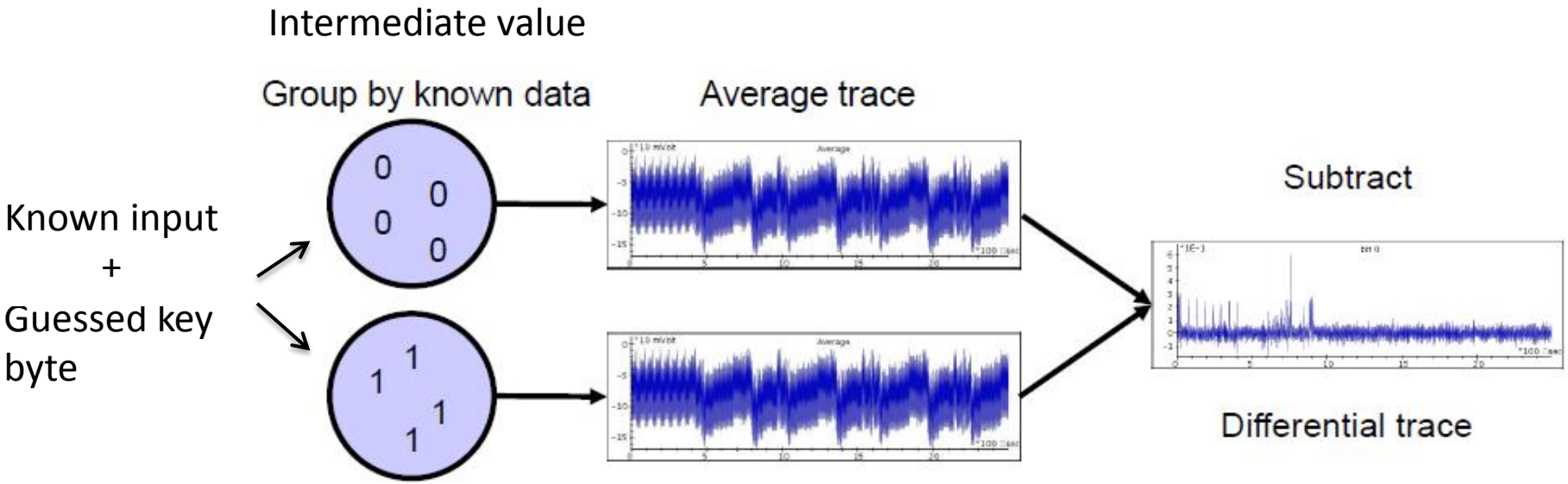
Heat

Power Analysis

- SPA (Simple Power Analysis)

  Deduce algorithm-related information by simply observing a single power trace.

- DPA (Differential Power Analysis)



Test if the guessed key byte is correct or not (hypothesis testing)

Part2

Measurement Setup

PC
+
Software
SCAnalyzer

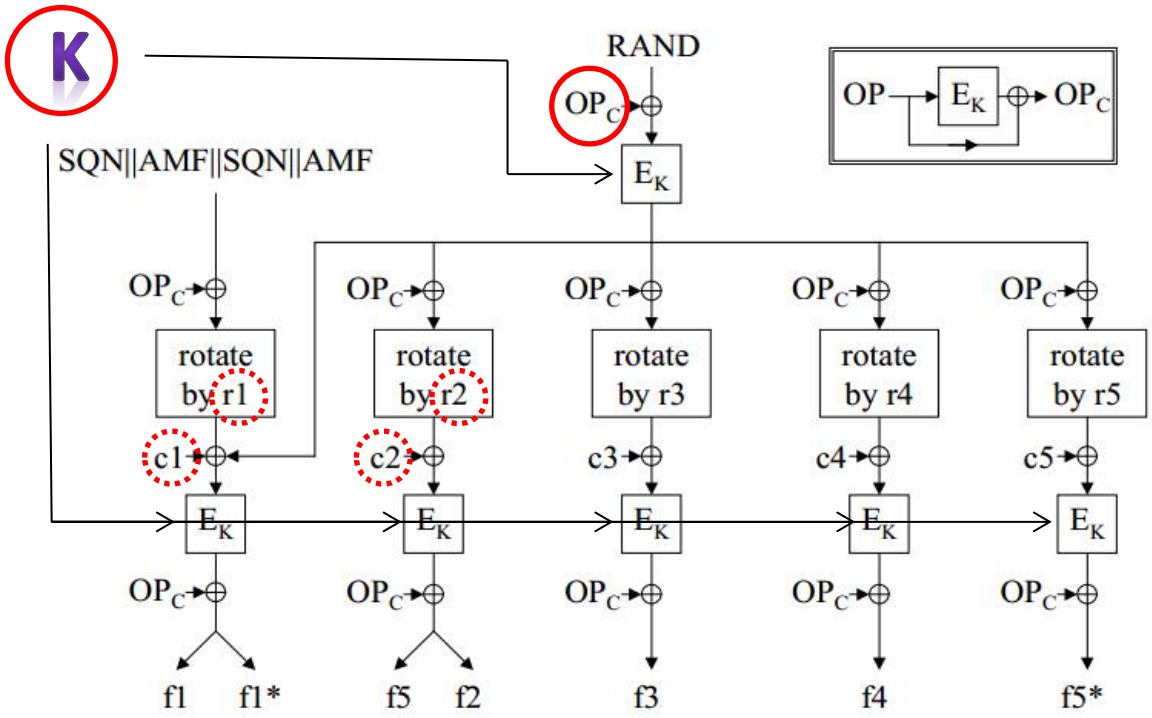
Oscilloscope

Power
Recorder

Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

What Do We Need



K + OPc + r1,c1, r2,c2

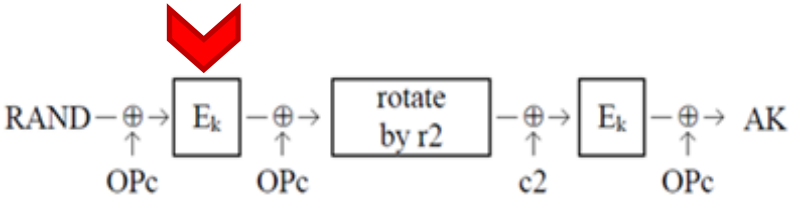
(recovery of r3,c3,r4,c4,r5,c5 is likewise)

How to recover them?

- The strategy: divide-and-conquer
- Recover the secrets K, OPc, r1,c1, …, r5, c5 one at a time using power analysis.
- For each secret, work on its key bytes independently and then combine.
  - for secret ∈{K, OPc, c1, c2, …, c5 }
    do a standard DPA
  - for secret ∈{r1, r2, …, r5 }
    do a divide-and-conquer PA

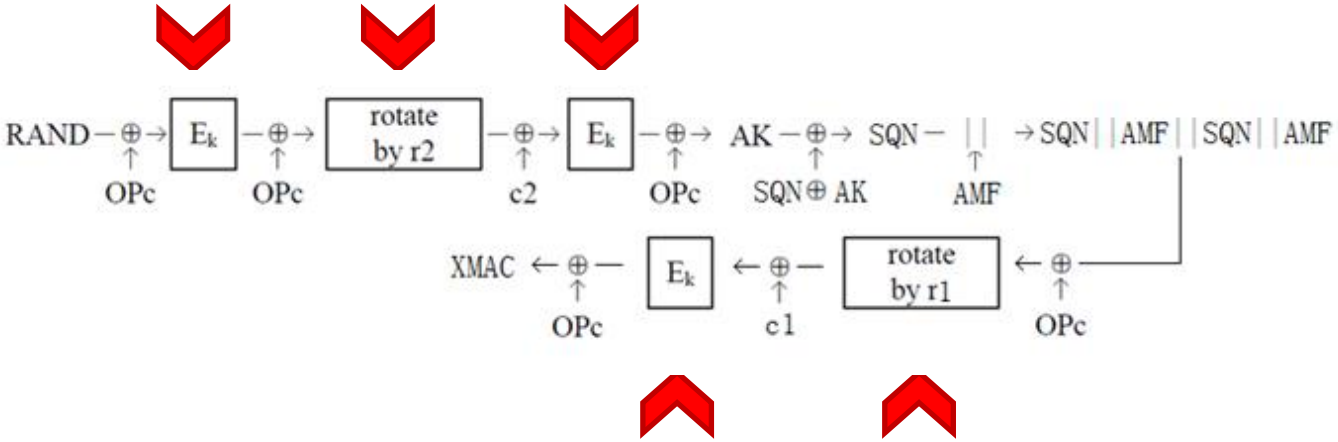
Where to Attack

Case 1:
Use standard (public) r1~r5,c1~c5



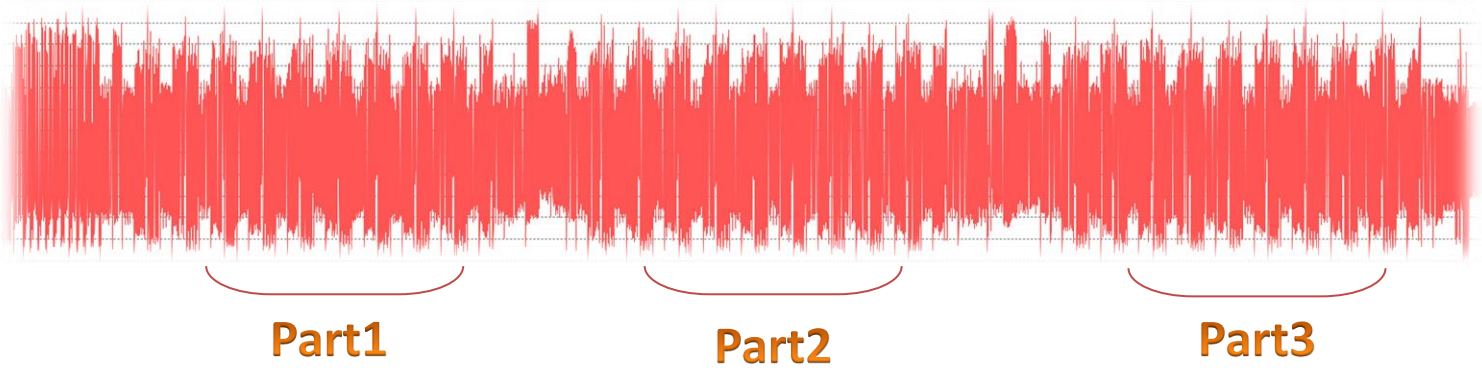
f5(function to generate AK)

Case 2:
Use customized (secret) r1~r5,c1~c5

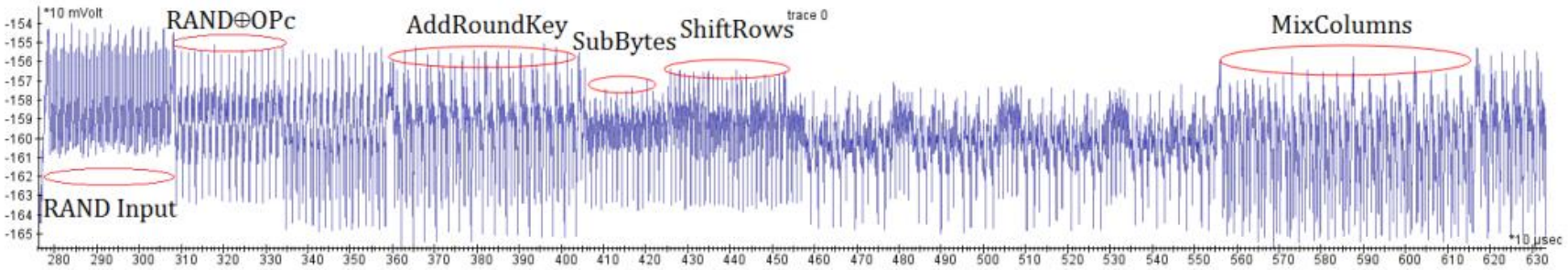


flow of f5+f1

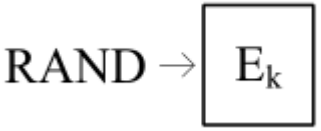
Analysis Process
Step1: Collect Power Trace



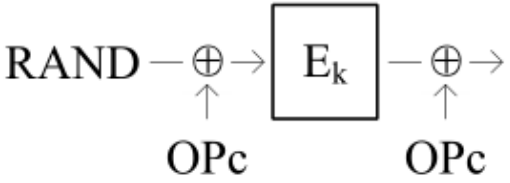
Identify the segment of interest using SPA and zoom-in for further analysis.



Analysis Process
Step2: Recover K and OPC

Standard DPA against AES only handles 

with secret k.

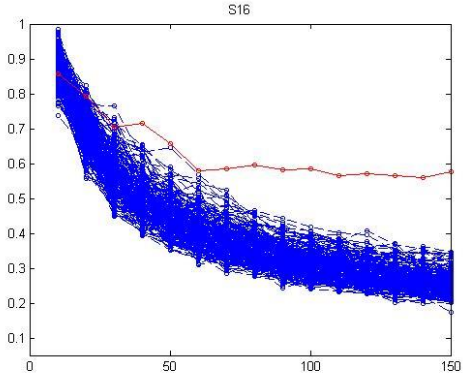
How to adapt the attack to 

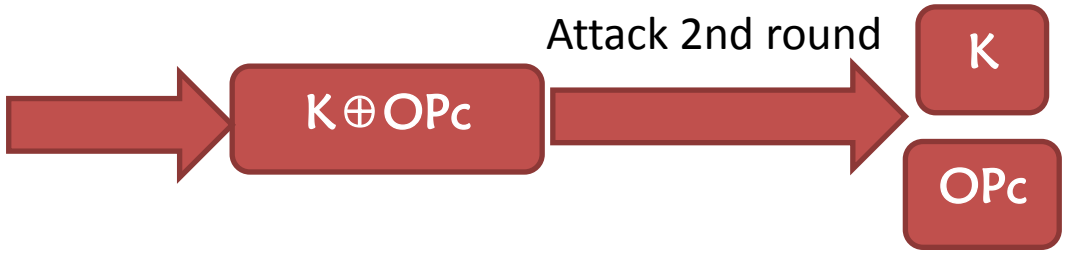
with secrets k and OPc ?

The trick: consider $E_{k'}$ with key $k'=k \oplus Opc$ and plaintext RAND.

(recall E_k first XORs its input with k due to AddRoundKey)

Attack 1st round





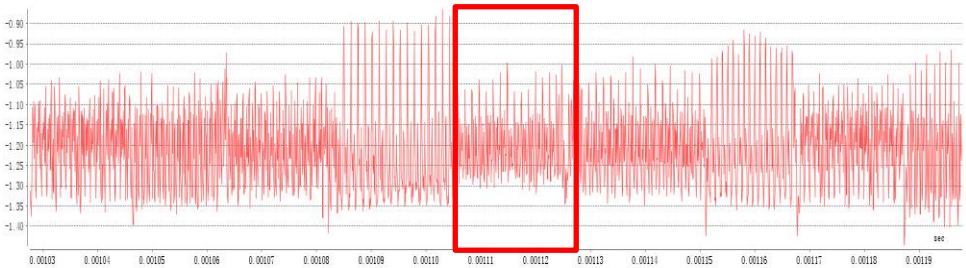
Part2

Analysis Process step3: Continue or Not?

Use standard Parameters for c1 r1 c2 r2

Y

Compute correlation to locate round shifts and recover parameter r1/r2

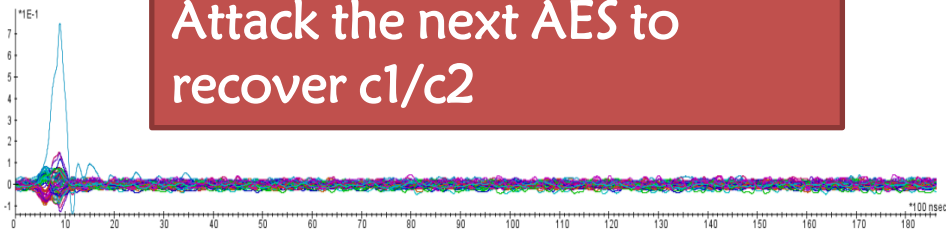


N

```
['INTERNAL AUTHENTICATE apdu: 00 88 00 81 22 10 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 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: comm
and accepted: no further qualification', (144, 0), [220, 14, 248, 108, 88, 4, 23
0, 197, 83, 241, 149, 189, 255, 123, 111, 35]]
```

VERIFICATION

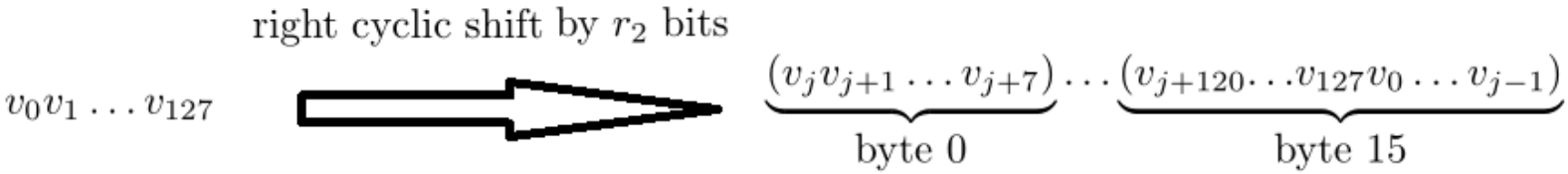
Attack the next AES to recover c1/c2



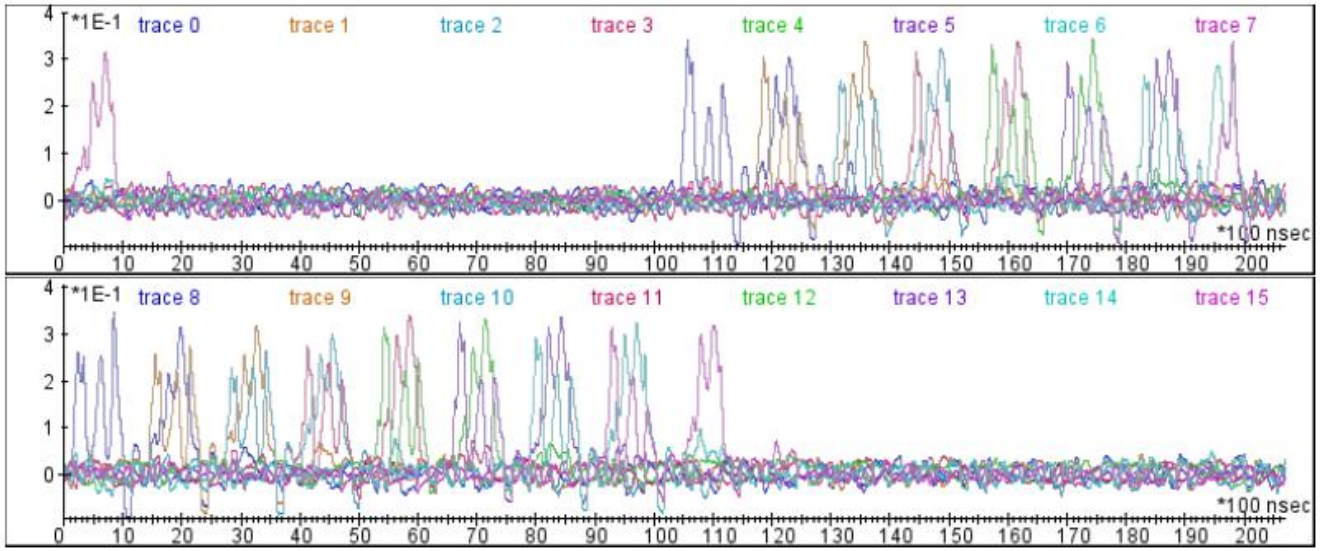
Finally we obtain c1、c2、r1、r2

How to recover the round shift parameter r?

- Consider $r2$ and write $r2 = 8i + j$



- First, assume $i = 0$, make a guess about j and correlate the resulting bytes to the power traces to test if the guess is correct or not.
- Second (when j is recovered), correlate the bytes to the traces again and identify the value of i from the sequence of correlations.



Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Results

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

Time needed for recovering the secrets ranges from 10 to 80 minutes,
using 200 to 1000 power traces.

Note: the operators and manufacturers are anonymized.

Outline

- Background
  1) 2G/3G/4G, (U)SIM Security
  2) Cryptology, 2G/GSM AKA protocol
- Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Our strategy
  4) Results
- Sound bytes

Part3

Sound bytes

1. Cryptography. Adding tweaks (secret values) to a block cipher in addition to the encryption key does not necessarily add more security.

2. The Dilemma:
   - Low cost devices ≈ limited budget for CC/EMVCo/FIPS security evaluations.
   - Low-cost × huge volume = great impact / loss

3. Awareness of physical security for small embedded devices.
   Practical security requires BOTH:
   - A mathematically secure (and publicly reviewed) algorithm.
   - Sufficient countermeasures in place against physical attacks.

Thank you!