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

blackhat USA 2015

观源信息

SHANGHAI JIAO TONG UNIVERSITY

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

Some updates from Citizenfour

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) Strategy, results and demos
- Lessons learned

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 (E.g. 310 150 123456789)
    USA+AT&T +id number
  - Secrets

- Secret on 2G SIM: master key K.
- Secrets on 3G/4G USIM:
  master key K, and OPc, r1, r2, …, r5, c1, …, c5.
- What if secrets are stolen/compromised?

Part1

Security compromised by revealed/stolen secrets

CLONING

TAPPING

TROJAN

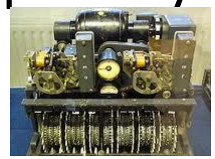
FRAUDULENT CALLS
OTP AUTHENTICATION

Any cryptography in (U)SIM?

Part1

Cryptology in a nutshell

Cryptology = “Cryptography” + “Cryptanalysis”

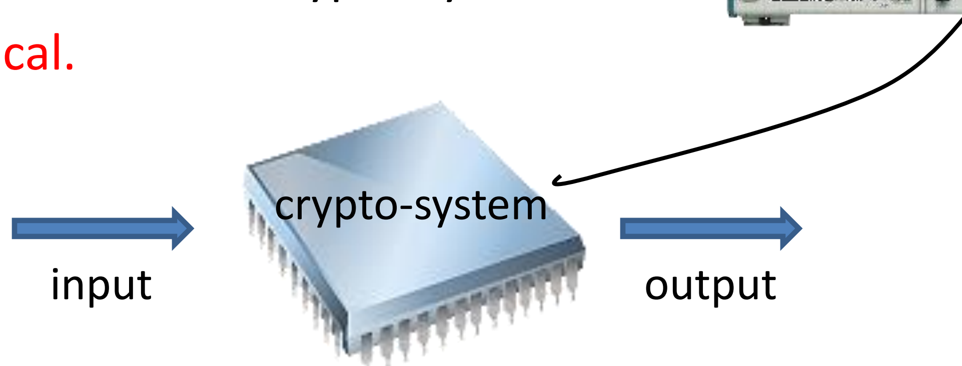
- Cryptography (design of )

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.

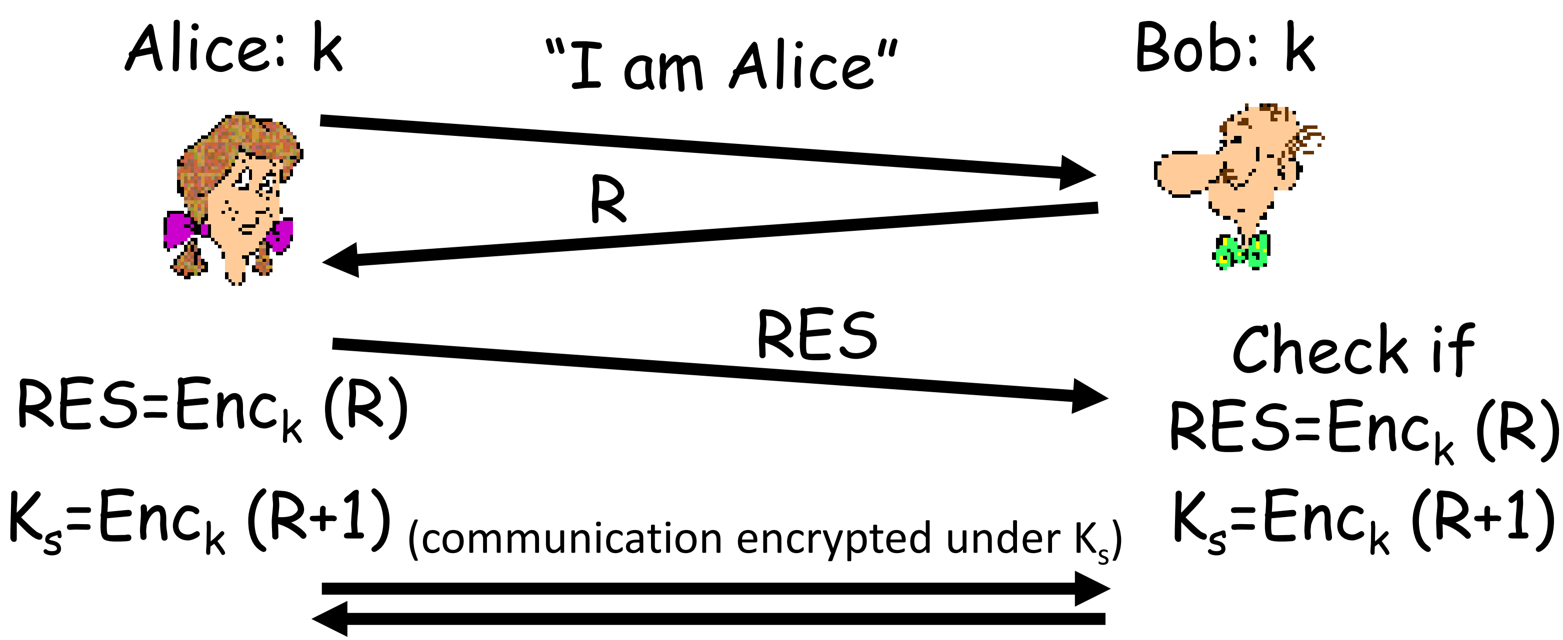


Part1

What cryptography is needed for (U)SIM?

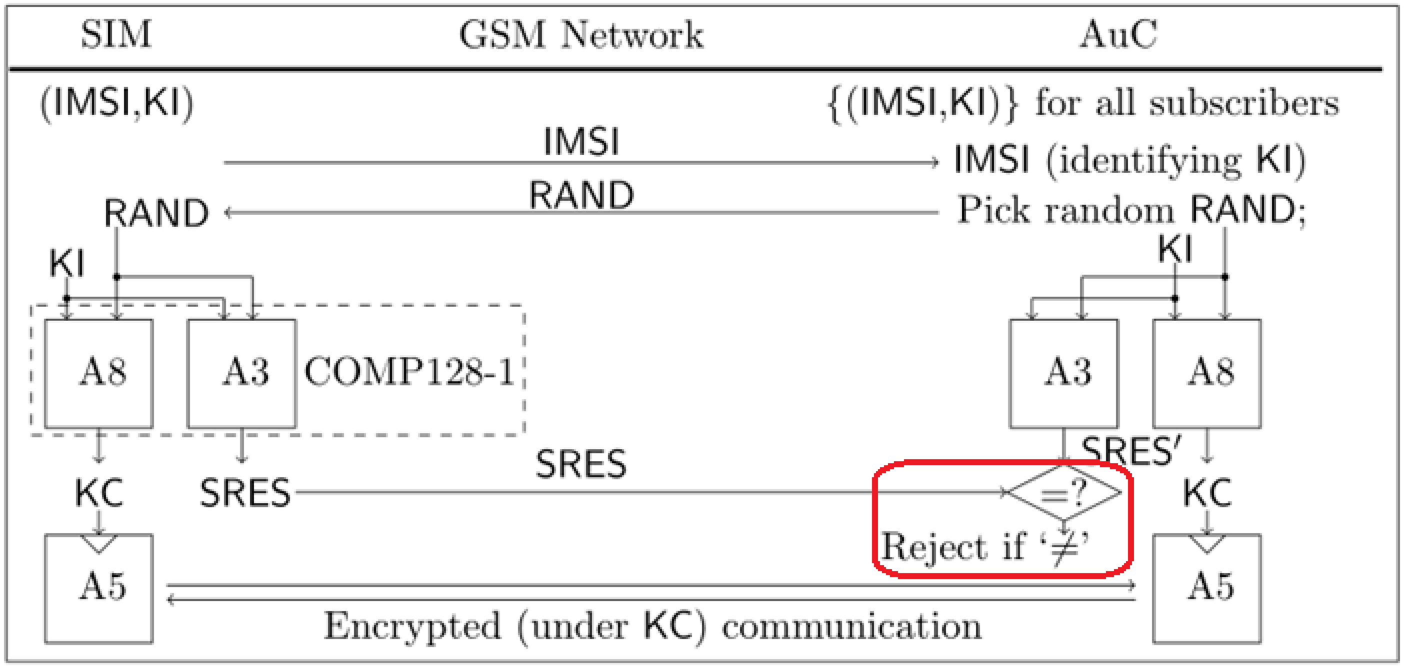
- AKA (Authentication & Key Agreement)
- Authentication: a process that ensures and confirms a user's identity.

  E.g., Bob authenticates Alice by **Challenge-and-Response**.
- Key Agreement (wrong term though!): session key derivation



Part1

The 2G GSM AKA Protocol



AKA algorithm of GSM: COMP128-1 (A3+A8)

Encryption algorithm : 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])

Security improvement of 3G/4G over 2G

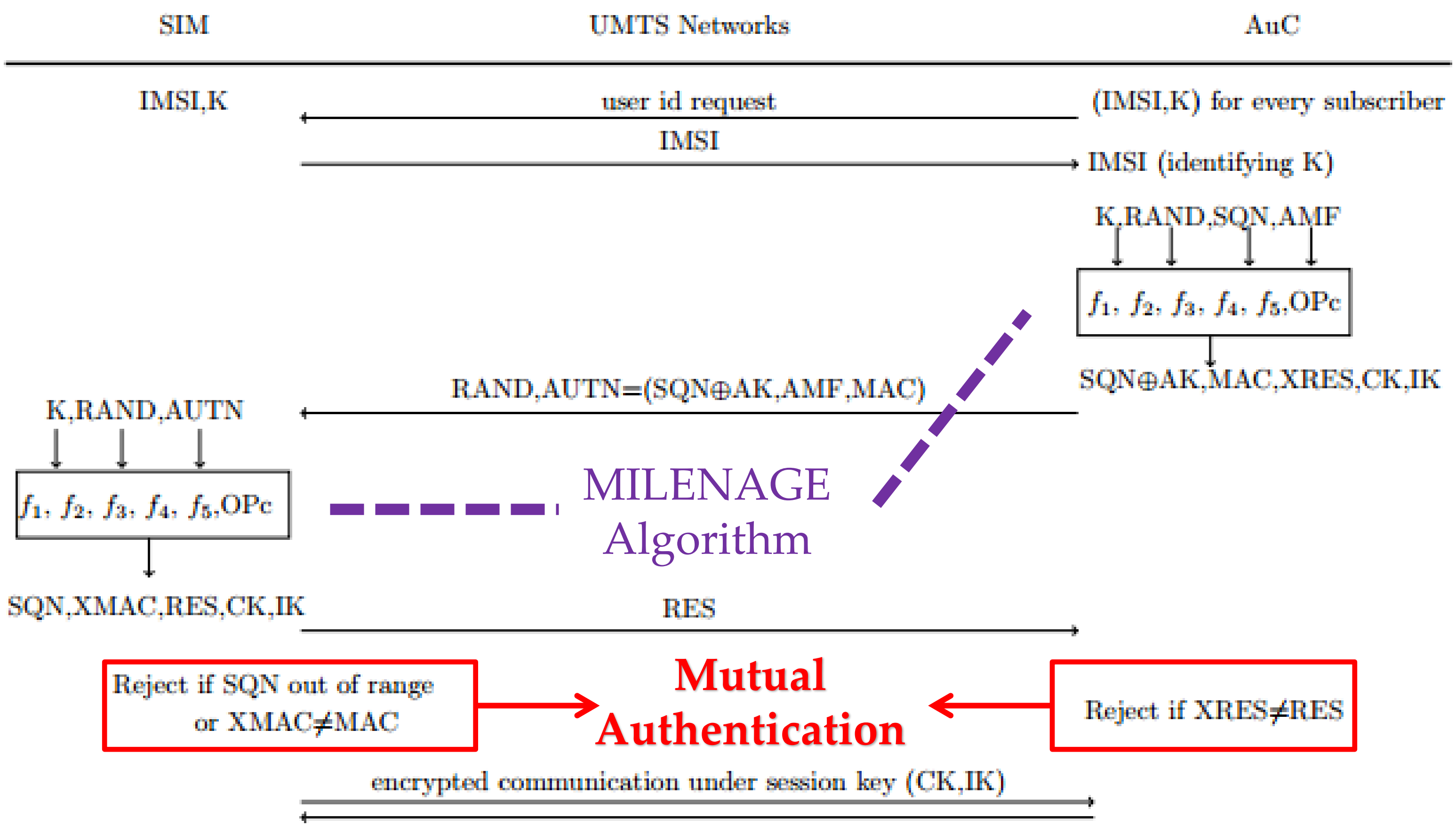
Part2

	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 USIM authentication *physically* secure?

Part2

3G/4G AKA Protocol



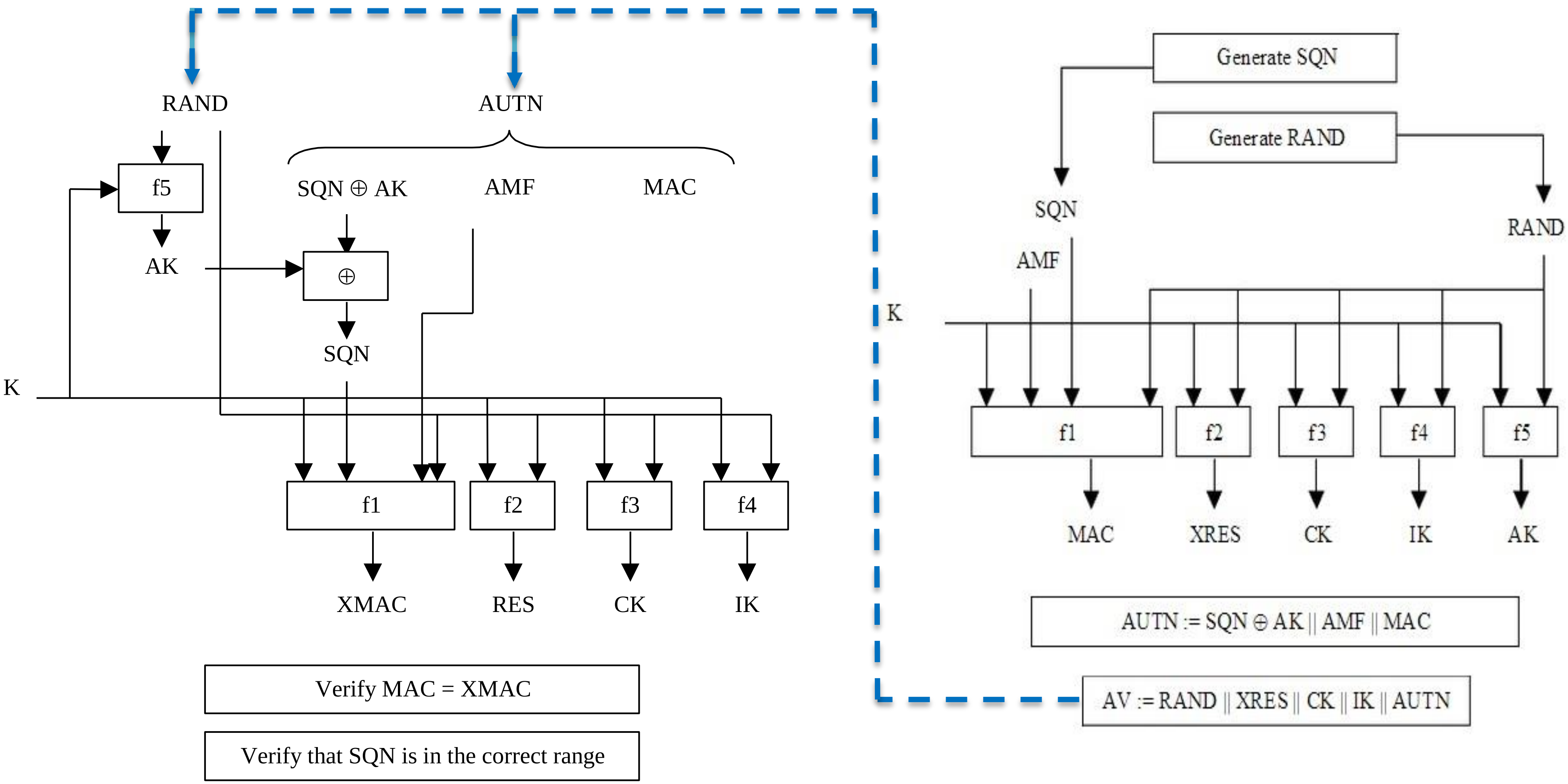
The different between 3G and 4G is not security-relevant

Part2

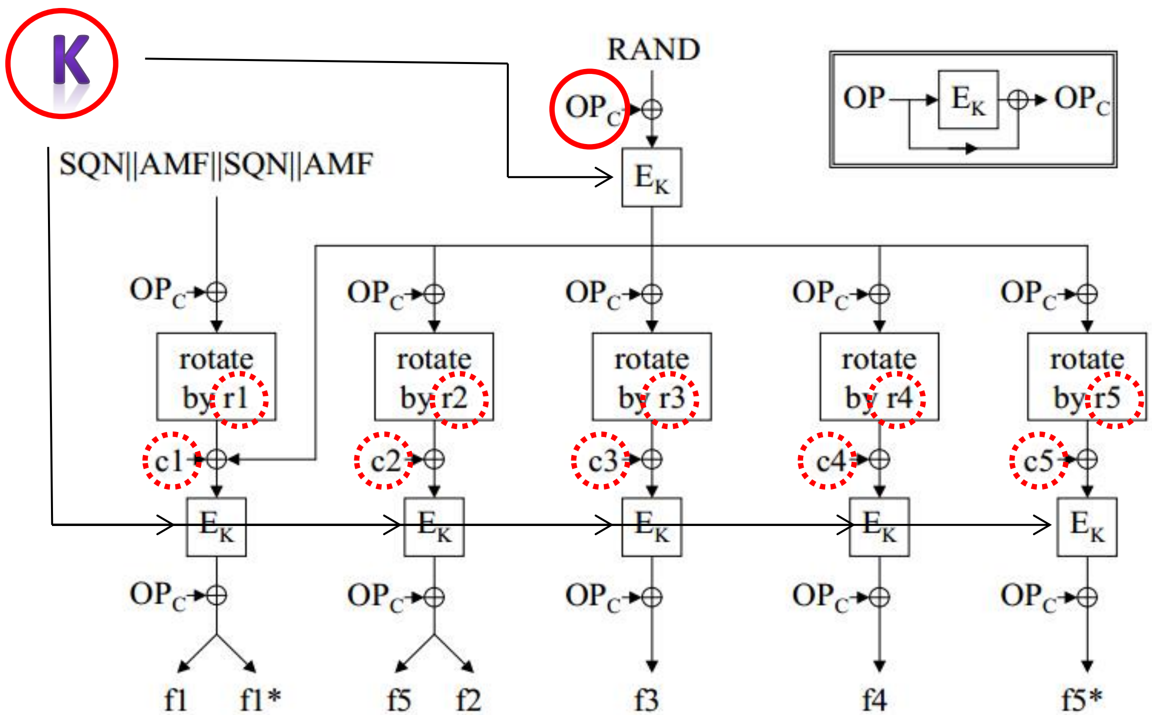
MILENAGE Algorithm

USIM

AuC



Secrets in USIM?



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

Part2

How to recover them?

- The strategy: "Divide et impera"

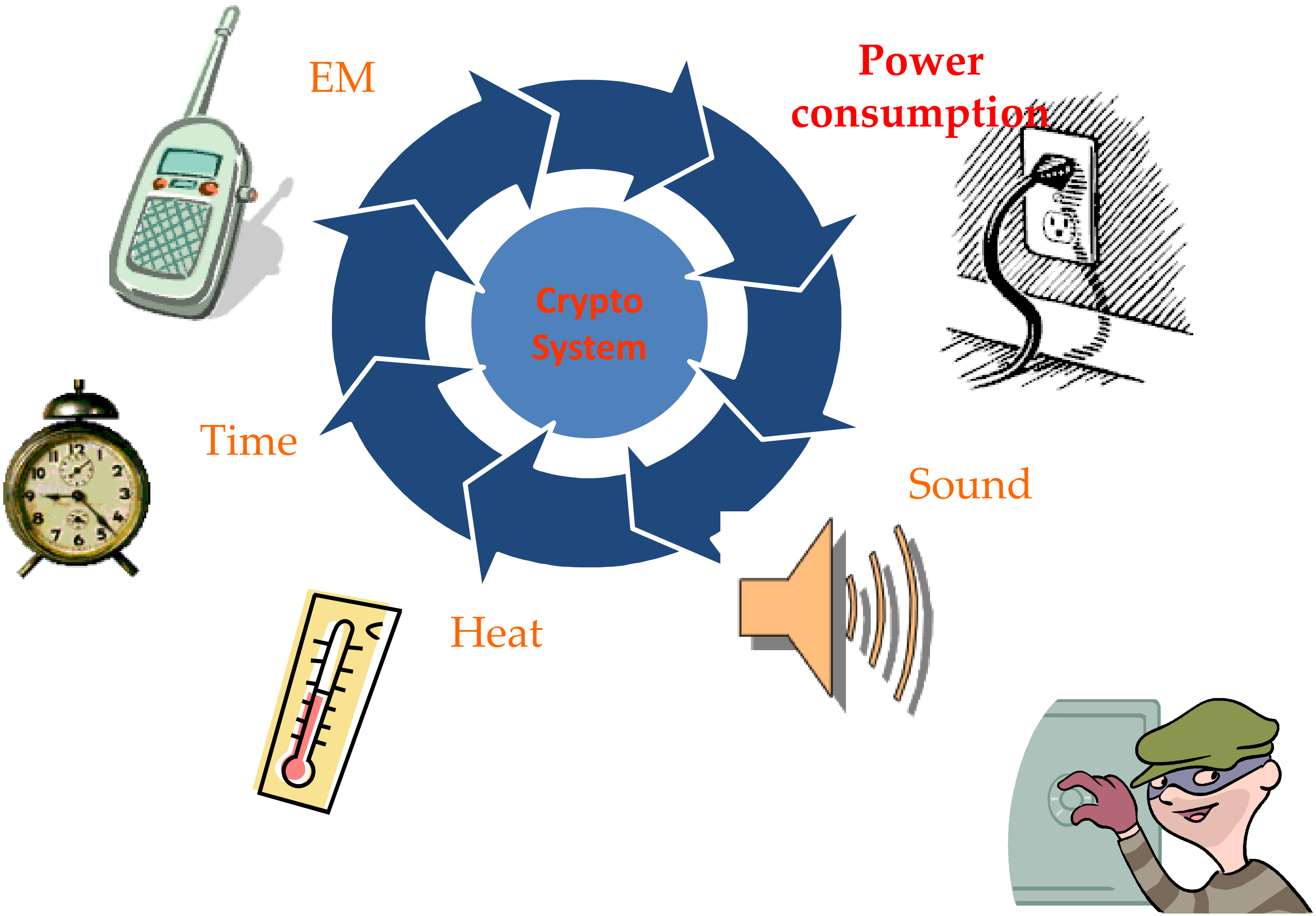
Breaking into a vault is hard.

Things are different if it can be divided into independent sub problems

- Our job: recover the secrets K, OPc, r1,c1, …, r5, c5 one at a time using power analysis.
  - ➢ for secret ∈{K, OPc, c1, c2, …, c5 } do a Differential Power Analysis (DPA)
  - ➢ for secret ∈{r1, r2, …, r5 } do a (non-standard) Correlation Power Analysis (CPA)

Part2

SCA (Side Channel Attack)



Measurement Setup

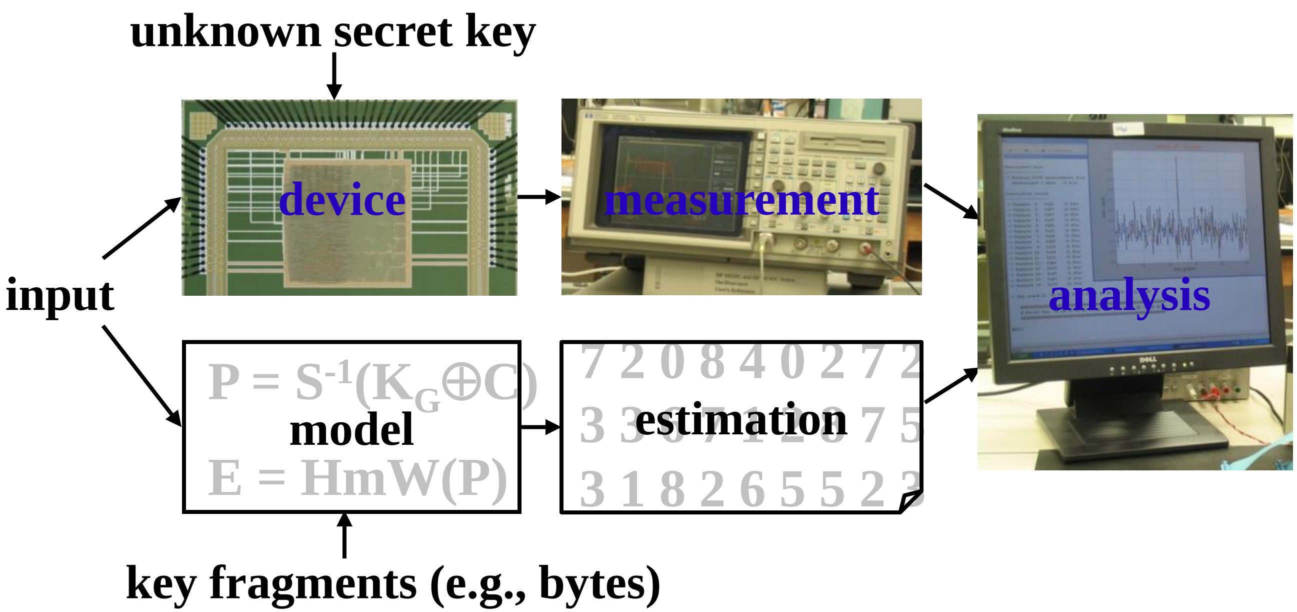
PC
+
Software
SCAnalyzer

Oscilloscope

Power
Recorder

Part2

Differential Power Analysis (DPA)



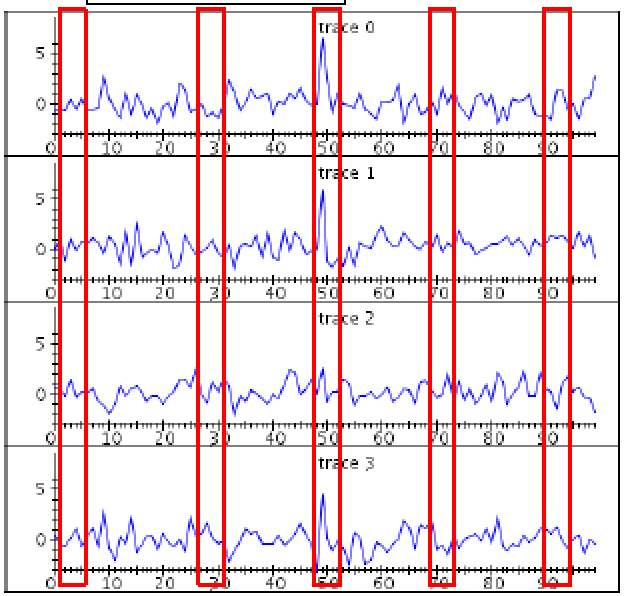
- **AES: 128-bit secret key brute force <u>infeasible</u>**
- **Exhaustive search for a key byte <u>easy</u>**
- **256 candidates (correct one highly correlates to traces)**
- **Do the above for every key byte <u>independently</u>**

Part2

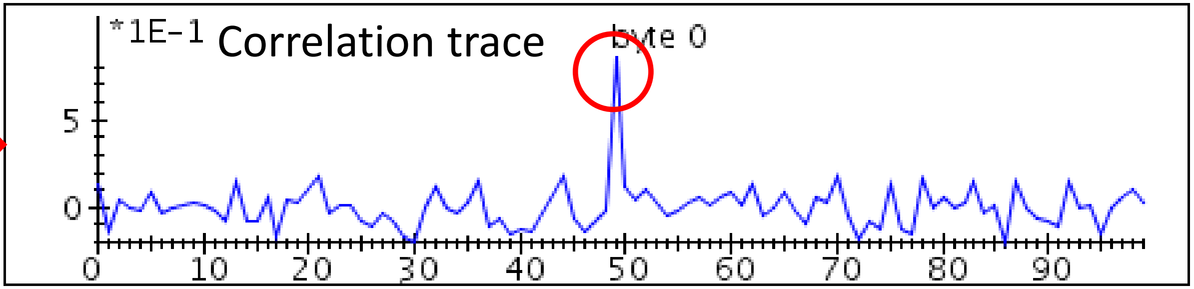
Differential Power Analysis cont'd
--- how to test if a key (byte) guess is correct or not?

Data	HW
FF	8
DD	6
09	2
8B	4

Power



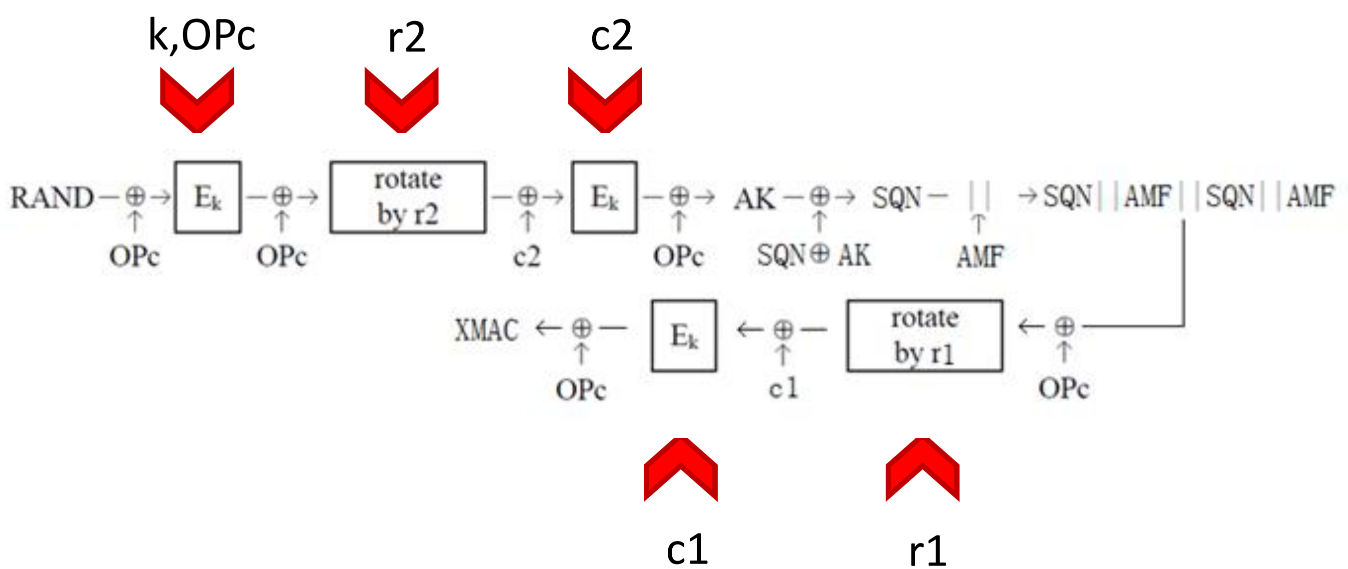
Correlate the hypothetical intermediate values to the power traces



Only the right key guess exhibits high peaks

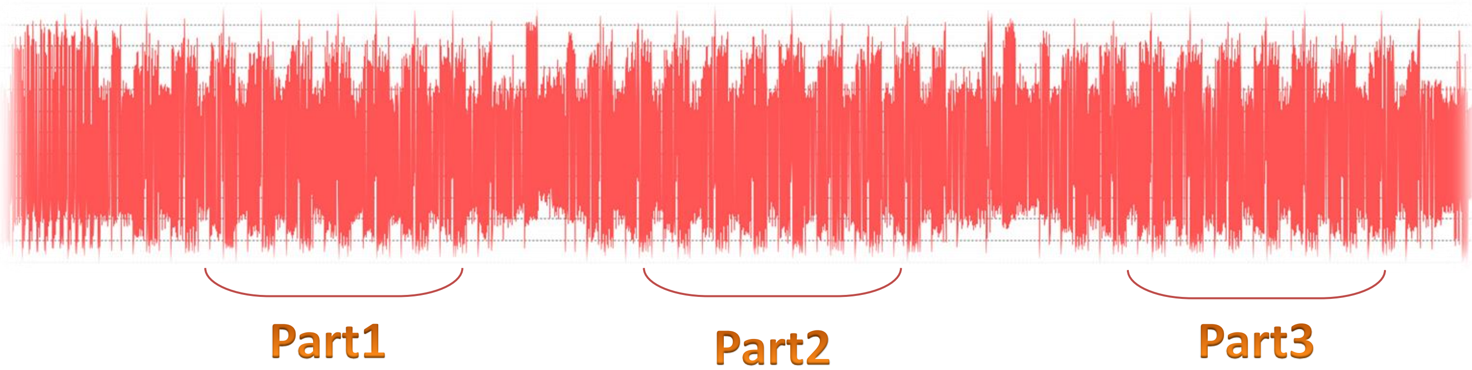
Where to Attack

Secrets: k, OPc, r1~r5,c1~c5



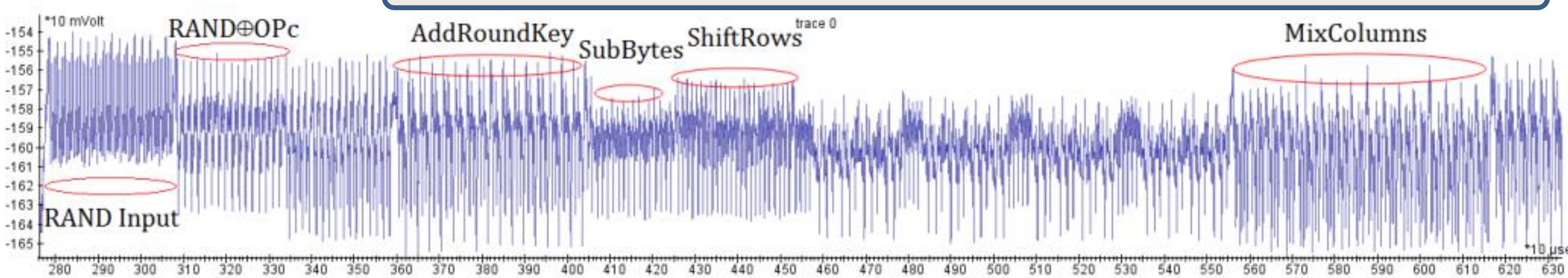
flow of f5+f1

Analysis Process
Step1: Collect Power Trace



Identify the segment of interest (simple power analysis) and zoom-in for further analysis.

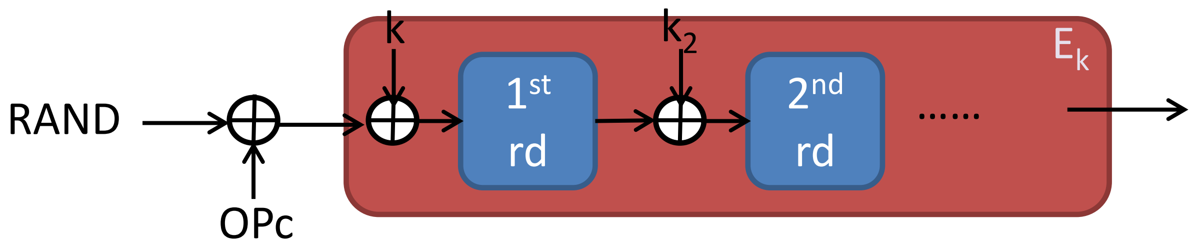
The first round of AES



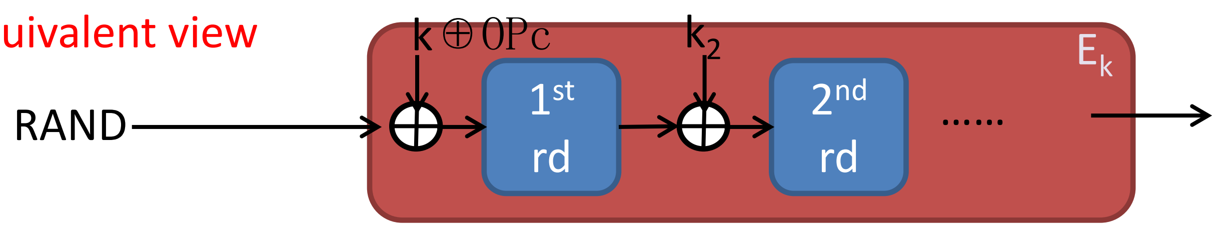
Analysis Process
Step2: Recover K and OPc

DPA recovers k from $\mathrm{RAND} \rightarrow \boxed{E_k} \rightarrow$

How to adapt the attack to $\mathrm{RAND} - \underset{\underset{\mathrm{OPc}}{\uparrow}}{\oplus} \rightarrow \boxed{E_k}$ with secrets k and OPc ?



Equivalent view



Attack 1st round: (viewing $E_{k'}$ with $k' = k \oplus \mathrm{OPc}$) recover $k \oplus \mathrm{OPc}$
Attack 2nd round: recover k_2 (and thus k)

Analysis Process

Step3: Recover $r_1, \dots, r_5$

- Consider r_2 and write $r_2 = 8i + j$

$$v_0v_1\dots v_{127} \xrightarrow{\text{right cyclic shift by } r_2 \text{ bits}} \underbrace{(v_jv_{j+1}\dots v_{j+7})}_{\text{byte } 0}\dots\underbrace{(v_{j+120}\dots v_{127}v_0\dots v_{j-1})}_{\text{byte } 15}$$

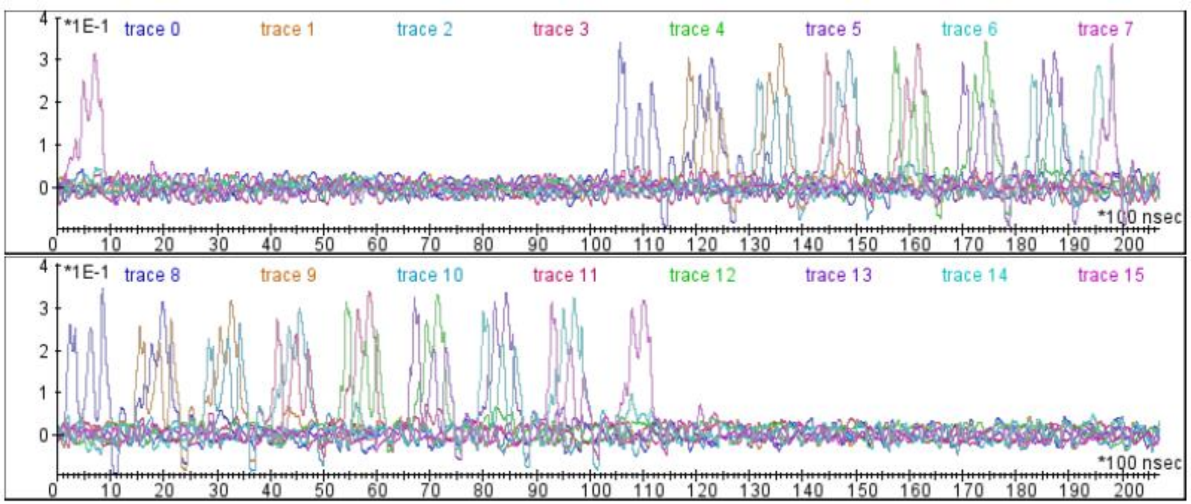
1. Recover j (assume WLOG $i = 0$)

   make a guess about j and do a hypothesis testing (8 possibilities)

   (correlate byte 0 to the power traces to test if which guess is correct)

2. Recover i . Correlate bytes 0 ~15 to the power traces, then

i is number of bytes shifted in the time axis (of the correlation trace).



Part2

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

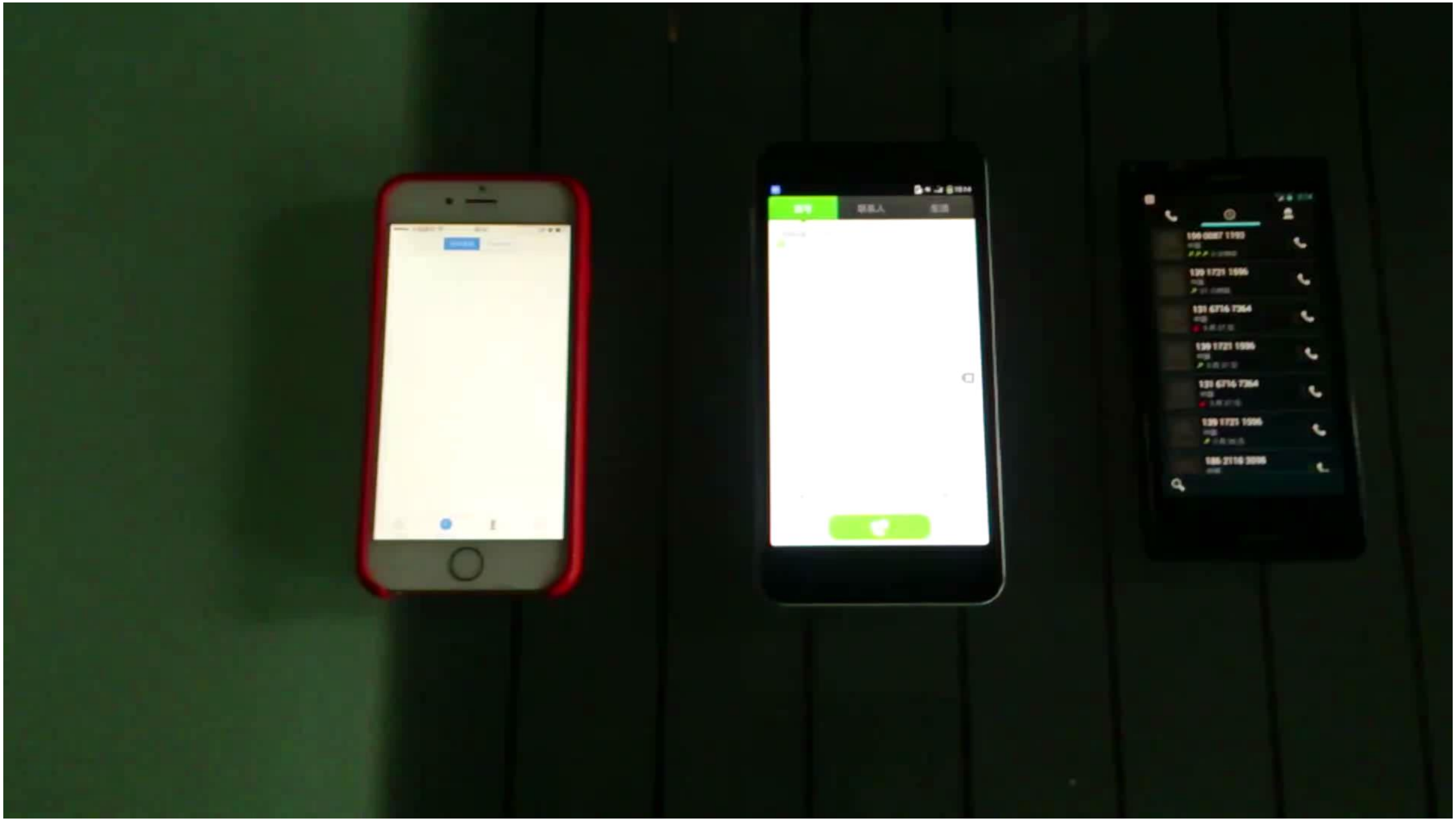
Time needed for recovering the secrets ranges from 10 to 80 minutes, using 200 to 1000 power traces.

Note: the operators and manufacturers are anonymized.

Part2

Demo 1

Making phone calls from a USIM and its duplicate to another phone.

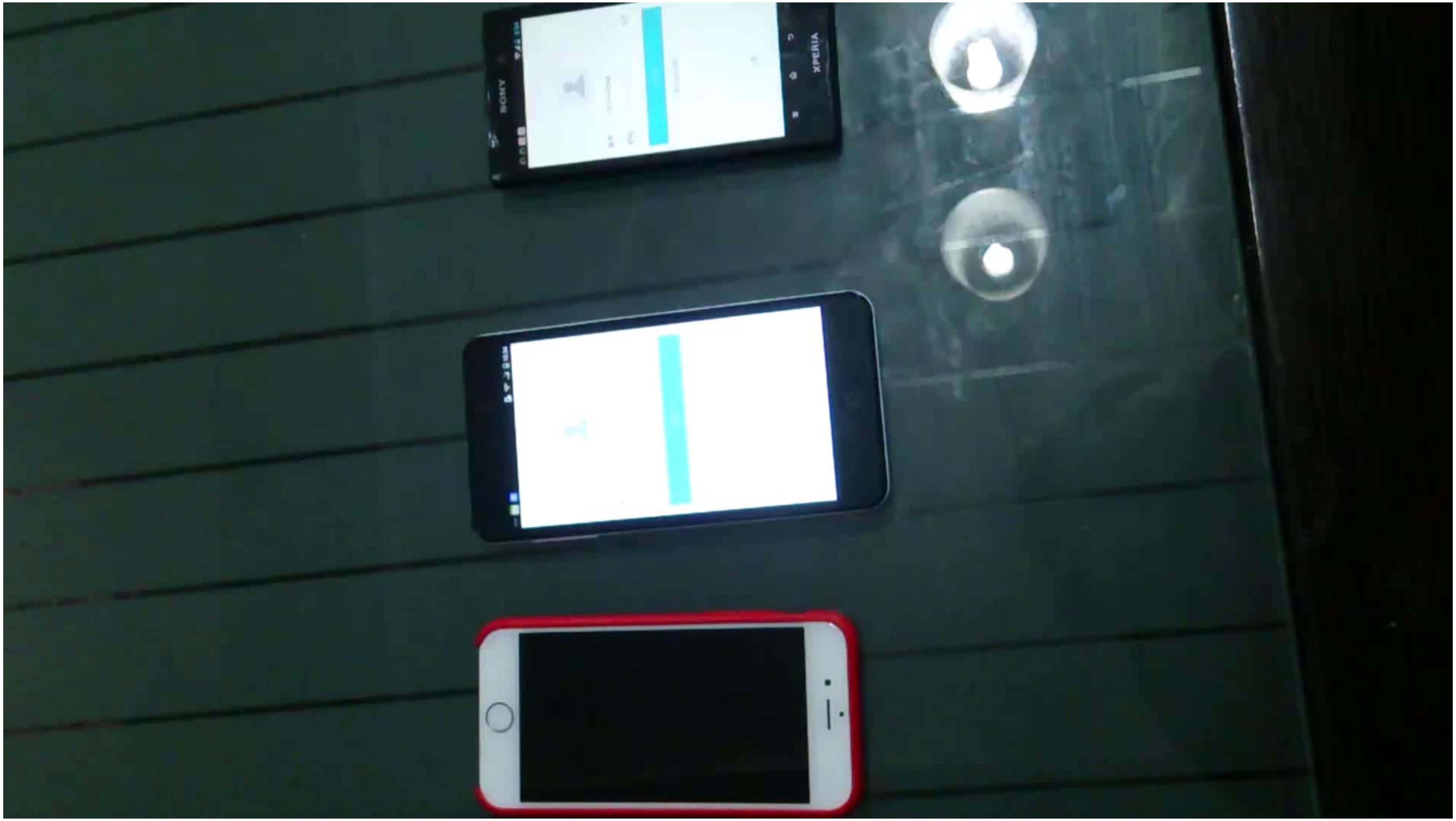


Part2

Demo 2

支付宝 Alipay.com

Resetting the password of Alipay app from a clone USIM.



Part3

Lessons Learned

1. Cryptography. Adding tweaks (secrets) 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!

For more technical details, check out our ESORICS 2015 paper: *Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards*