On the Need of Physical Security for Small Embedded Devices: A Case Study with COMP128-1 Implementations in SIM Cards

Ryan Zhou, Yu Yu, F-X Standaert, Jean-Jacques Quisquater

Brightsight
Tsinghua University and East China Normal University
UCL Crypto Group

Financial Cryptography and Data Security 2013

Outline of the Talk

- Cryptography and Physical Security
- GSM and COMP128-1 (A3/A8) SIM cards
- Weakness and Attacks: Algorithmic vs. Physical
- A Case Study on COMP128-1 Implementations
- Lessons Learned

How cryptography works?

- Typical Assumptions:

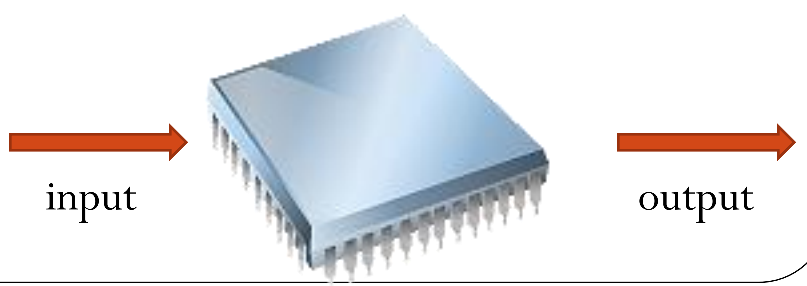
(1) A computational hard problem (RSA, AES).

(2) Black-box: attacker ONLY sees input-output.

- Provable Security: Reductionist approach.

  If one breaks the crypto-system (in polynomial-time), then it leads to efficient solution to the assumptions .

- Security guarantee voided if either assumption is not met.



Are these assumptions safe?

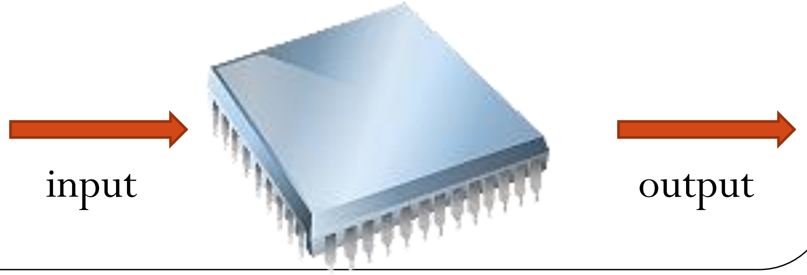
- Typical Assumptions:

(1) A computational hard problem (RSA, AES).

(2) Black-box: attacker ONLY sees input-output.

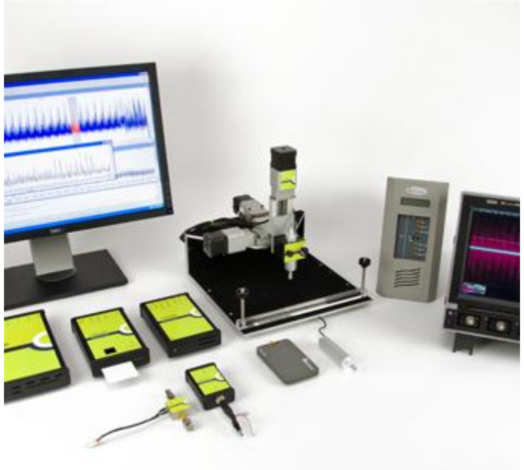
- Provable Security: Reductionist approach.
- Assumption #1 is ok (otherwise a breakthrough).
- Assumption #2 is not always respected.

The implementation of a cryptographic algorithm might be leaking in many forms.



Side-channel attacks and beyond

- Definition: Any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms.
- It takes many forms:
  - Timing Attacks
  - Power Analysis (PA)
  - Electro-Magnetic Analysis (EMA)
  - Acoustic Analysis
  - etc.
- More invasive physical attacks exist.



Cryptographic Products in Real World

Smart cards equivalents, banking tokens, and other small embedded devices.

Cellular networks (1-4G)

- 1G: analogue signal (last 90's)

- 2G: digital signal

  GSM vs. CDMA

- 3G: UMTS vs. CDMA2000

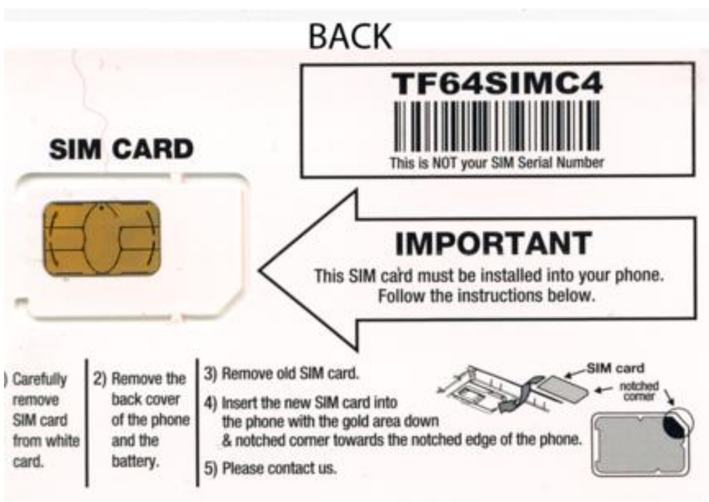
  high-speed data transmission
- 4G: LTE Advanced vs. WiMAX (IEEE 802.16e)

Despite the migration to 3G/4G, GSM remains the current dominant technology for mobile communications, especially in many developing countries.

SIM cloning： the main threat to phone security

- SIM card is a smart card.
- SIM stores： ICCID(serial number), IMSI (USER id)， secret key K, contacts (optional).

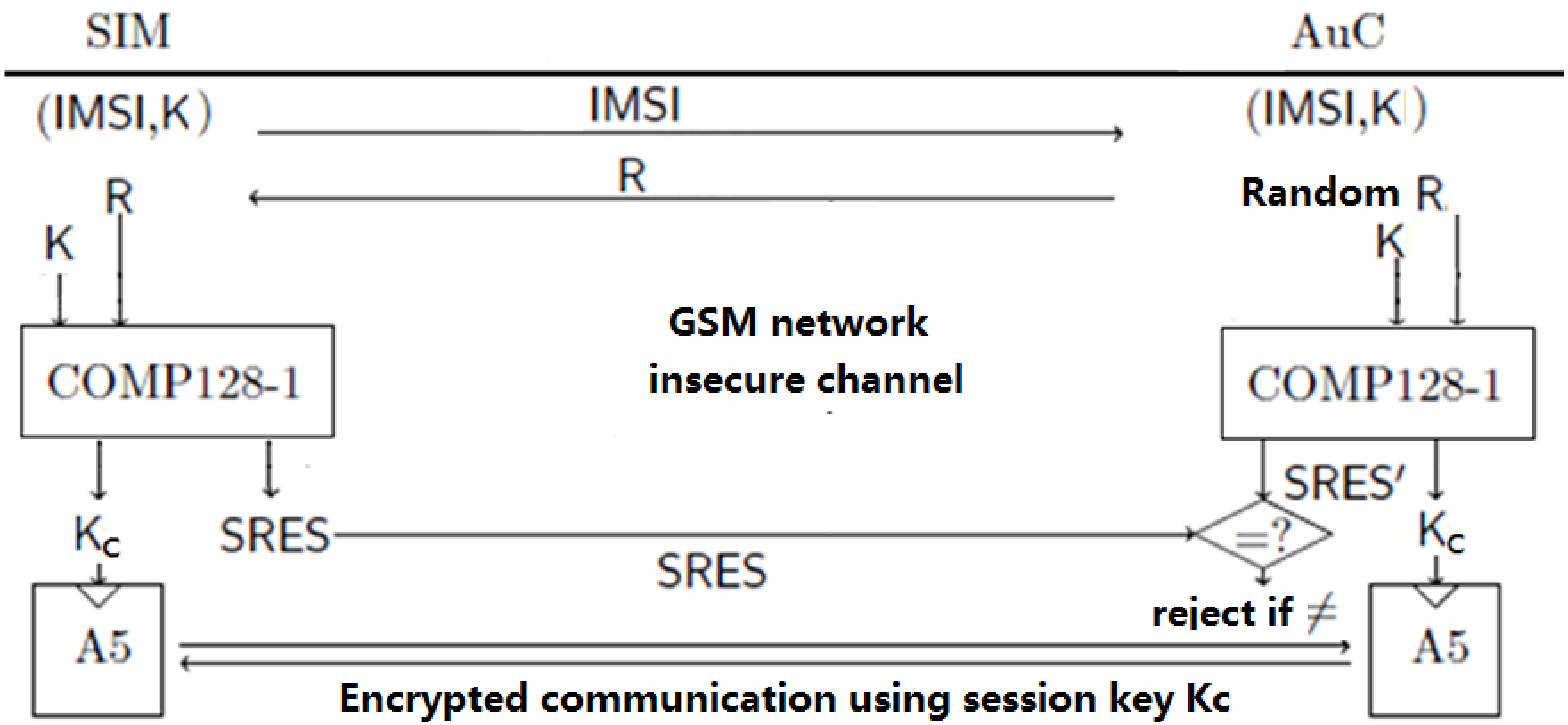
  knowing IMSI and K allows one to clone the SIM card
- SIM Cloning： making fraudulent calls、 impersonation、 privacy breach、 internet banking security。



- The key of cloning a SIM card： recover the key K

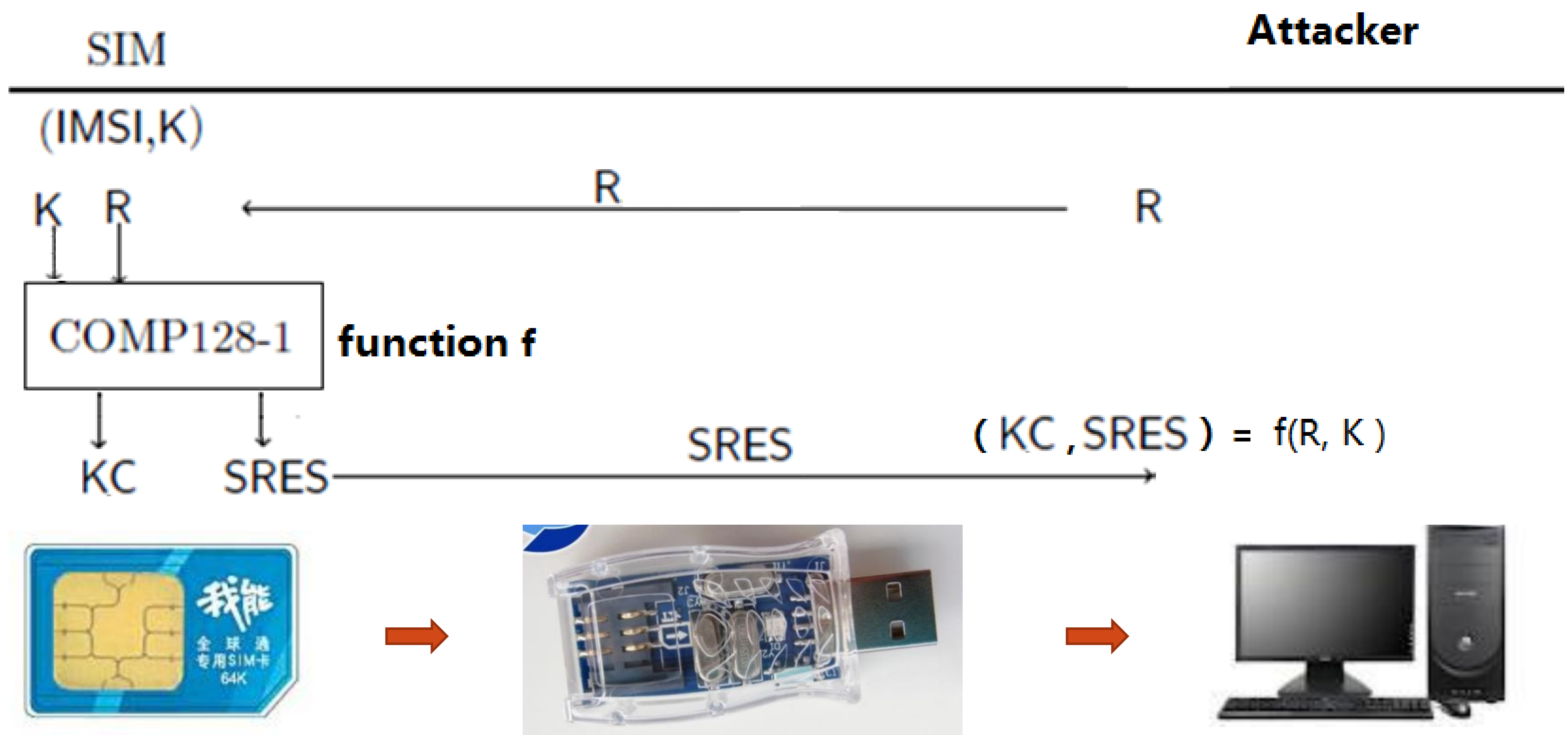
Authentication between SIM card and base station (AuC)

GSM SIM uses the COMP128-1 algorithm for the authentication.



Mathematical vs. physical attacks

- Mathematical attack： Attacker (impersonates the AuC), sends (possibly malicious) inputs R and observes output s accordingly, and try to recover K.



- Side-channel attack： In addition, attackers can capture some physical information such as power consumption.

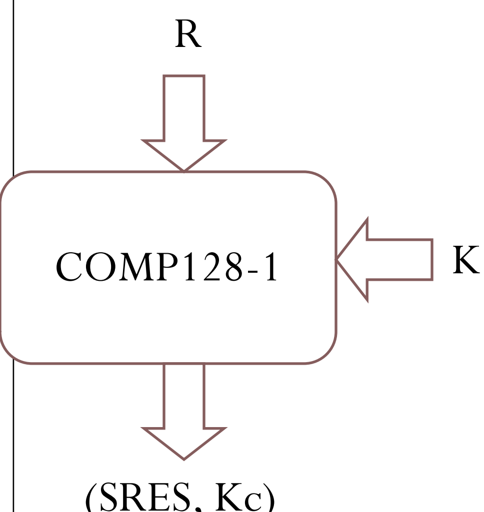
History COMP128-1

- COMP128-1, as part of the GSM specification, drafted in1987 and kept secret.
- In 1998, a research group at UC Berkeley (led by David Wagner) reversed engineered COMP128-1, and release it on the internet.
- COMP128-1 is a cryptographic hash function with a butterfly structure (FFT-HASH) .
- Targets of this work: a few SIMs cards from several (anonymized) manufacturers and operators.

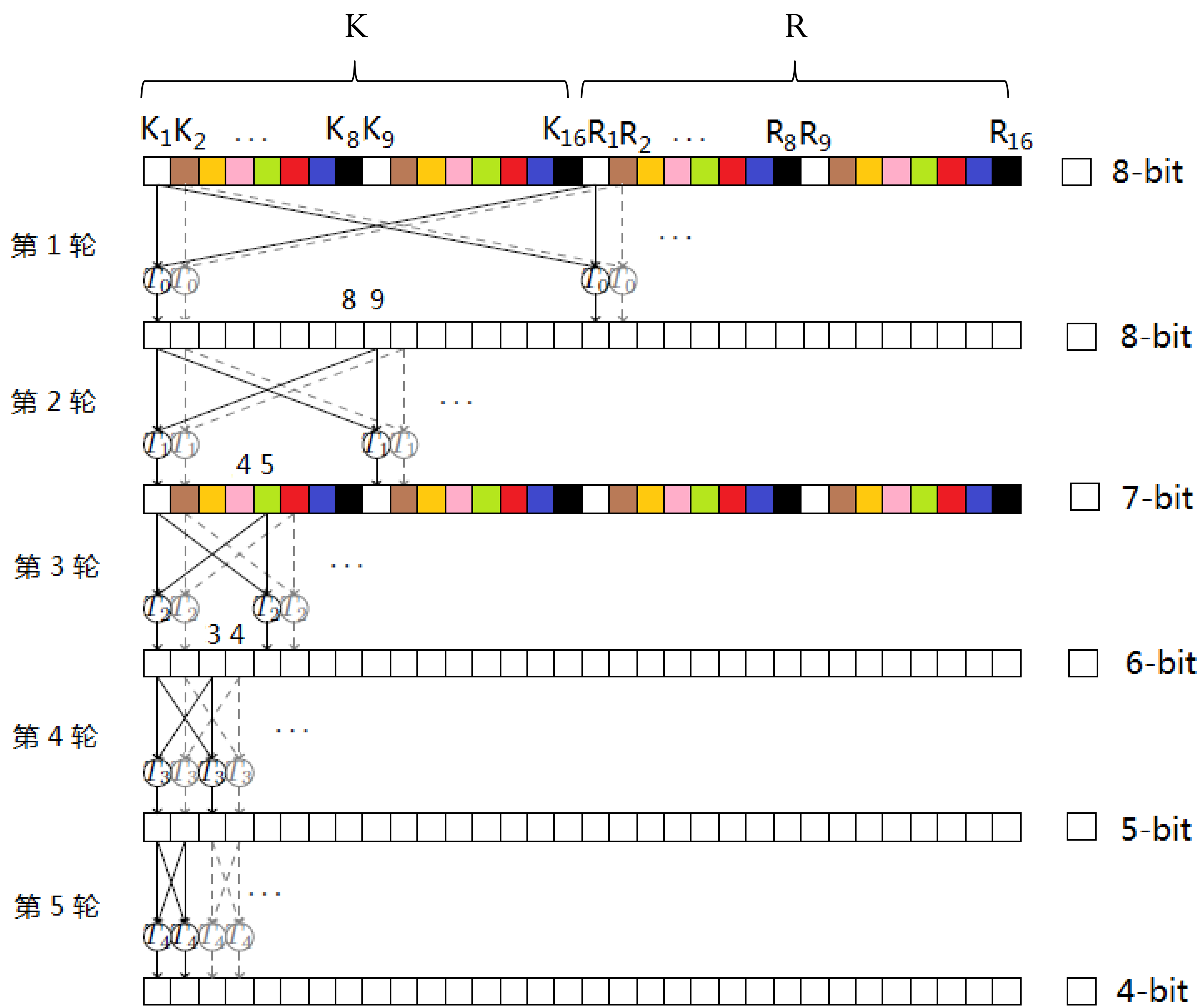
Pseudo-code of COMP128-1

- COMP128-1 is cryptographic hash function.
- Input： 32-byte (i.e. 16-byte random R, 16-byte secret K)
- Output： 12-byte(i.e. 4-byte SRES 和 8-byte Kc).
- Pseudo-code：

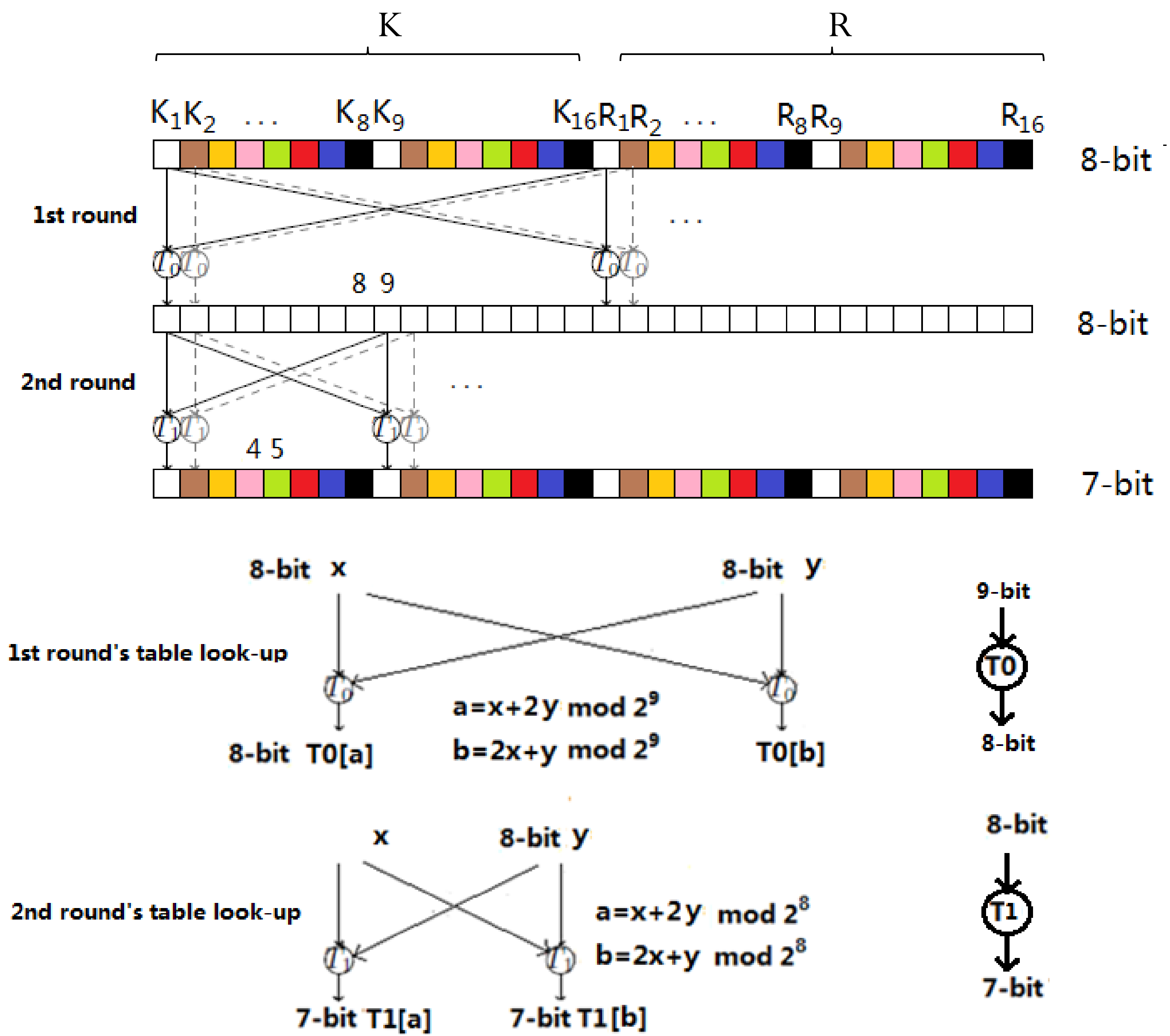
```
function COMP128-1(R, K)
begin
    for j=16 to 31 do              {* 调入随机数 R *}
        X[j] := R[j − 16];
    for i=0 to 7 do                {* 8次循环 *}
    begin
        for j=0 to 15 do           {* 调入密钥 K *}
            X[j] := K[j];
        call Compress;             {* 压缩函数 *}
        call FormBitsFromBytes;    {* 格式转换 *}
        if i < 7 then              {* 置换 *}
            call Permute
    end;
end;
```



Compression subroutine

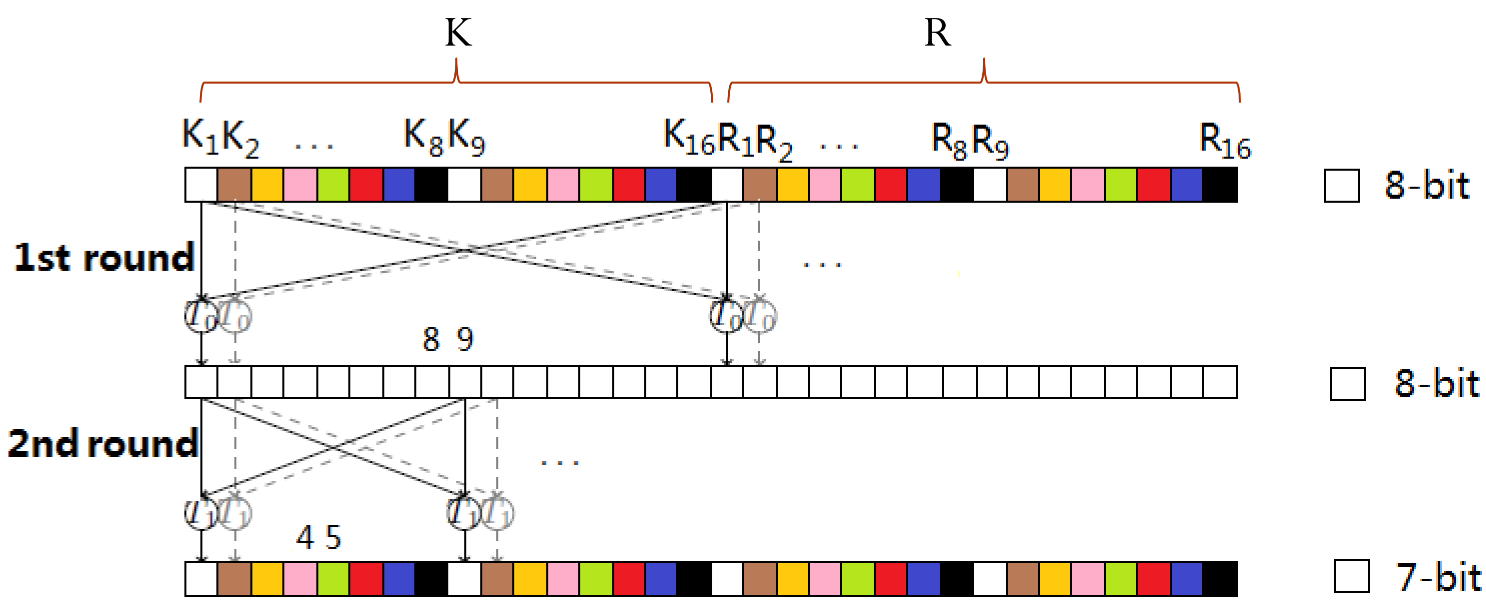


flaw： insufficient diffusion



Exploiting the Flaw: Collision attack

- Strategy: Divide and Conquer.
- Attack one color(1 key byte) at a time， fix the rest colors (s.t. collision on the output of 2^{nd} round can propagate to the final output).
- Each color at 2^{nd} round has 28 (4x7) bits, by birthday paradox, it takes 2^{14} inputs to obtain 1 collision, so covering whole key needs 2^{14} x 8=131,000 inputs.



Collision attacks are implemented: SIM cloning kits available

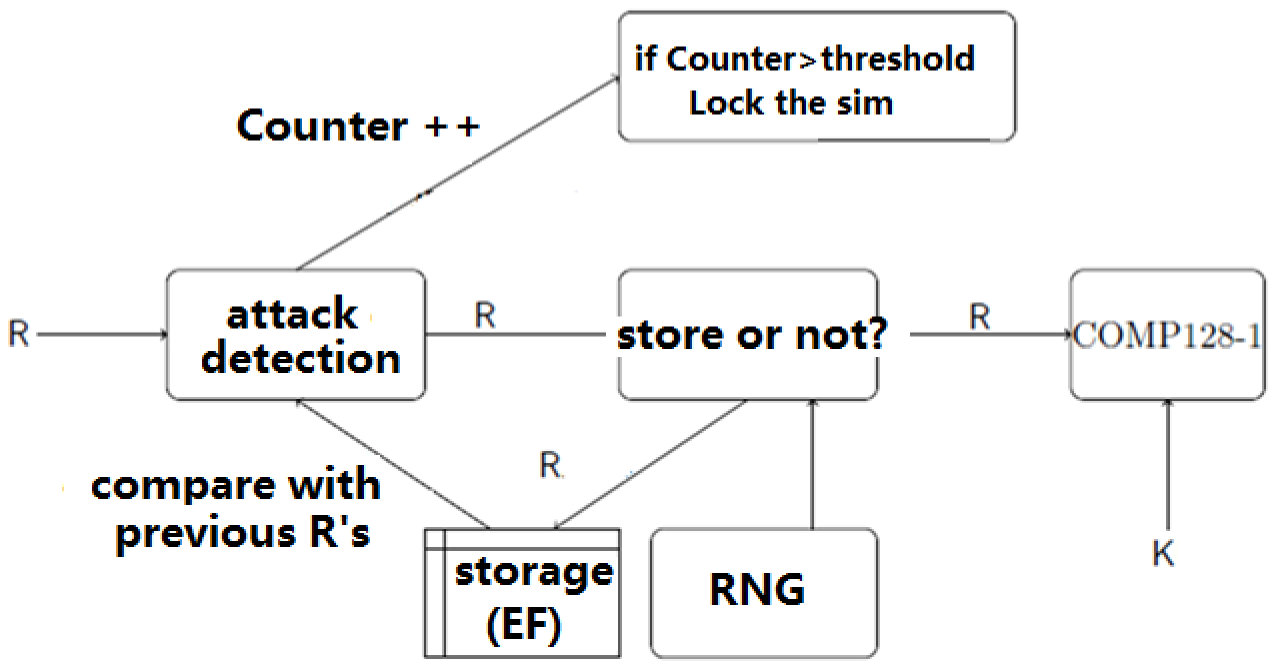
- Low cost (~$10).
- Cloning kit: SIM card reader, software (driver, cracking, SIM writing), blank SIM card
- Effective with COMP 128-1.

Ad-hoc Countermeasures

- Move to newer versions COMP128-2, COMP128-3 (still kept secret!)
- Patch COMP128-1:

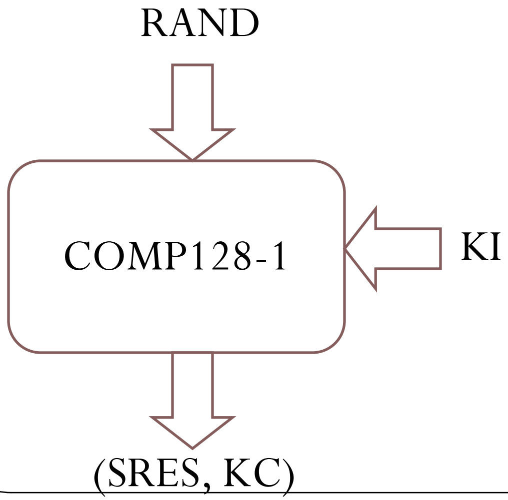
Known attacks easy to detect： attacker sends many correlated inputs.

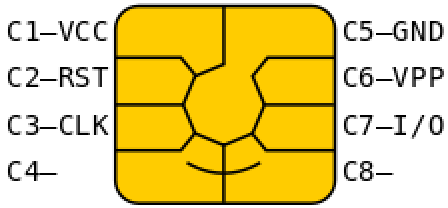
Detecting heuristics (used by some operators)： Store a few previous inputs, compare with the current one. Lock the card if too many attempts are detected.



Attack 2 (our results)： Power Analysis Attacks

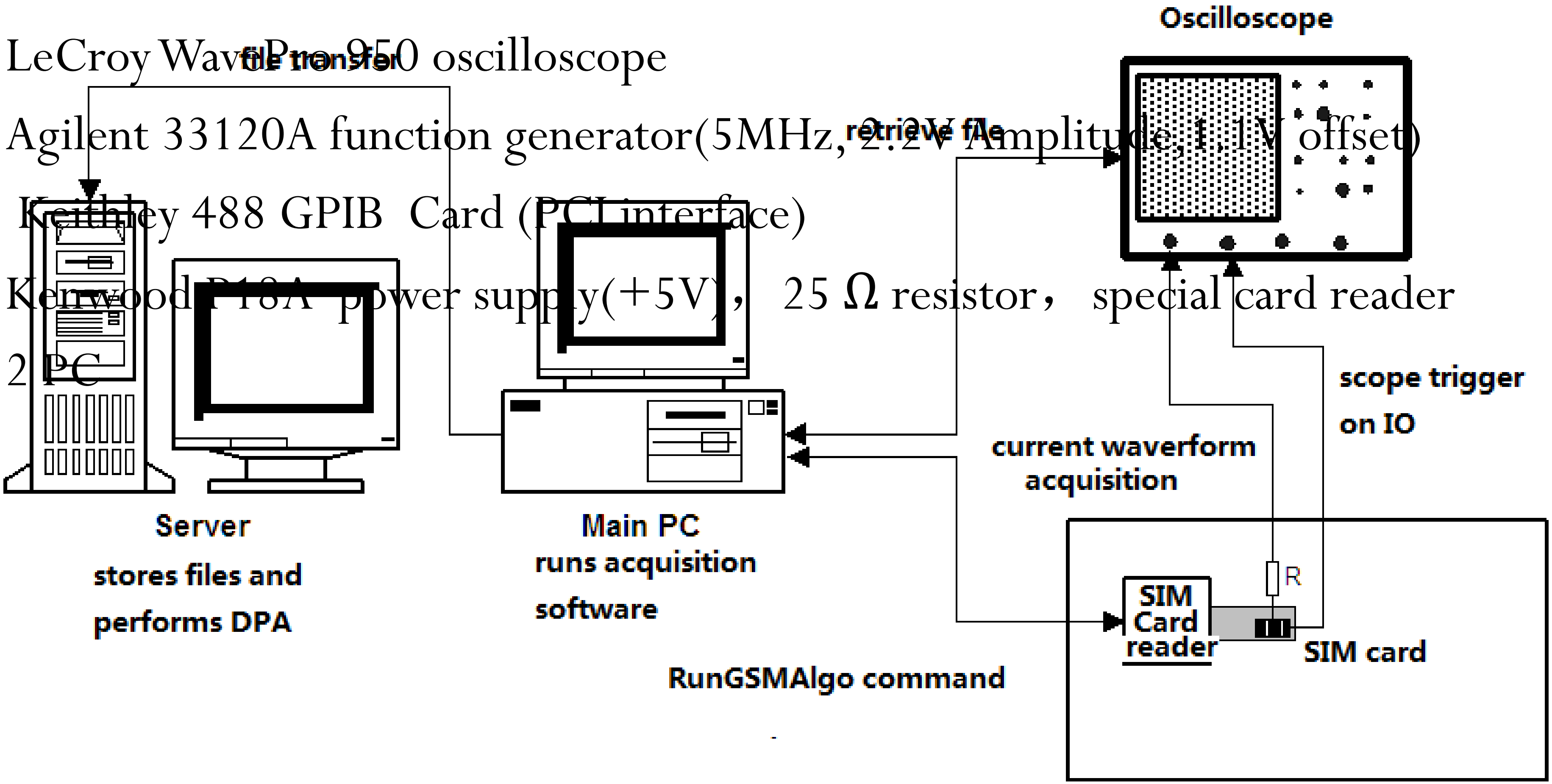
- Collision attacks fail because they are easy to detect.
- Power analysis： Send truly random R to SIM, not causing sim lock.
- How it works： SIM relies on external power and clocking signal.





Measurement Setup for Power Analysis

- LeCroy WavePro 950 oscilloscope
- Agilent 33120A function generator(5MHz, 2.2V Amplitude,1.1V offset)
- Keithley 488 GPIB Card (PCI interface)
- Kenwood P18A power supply(+5V)， 25 Ω resistor， special card reader
- 2 PC



Power Trace Measurement

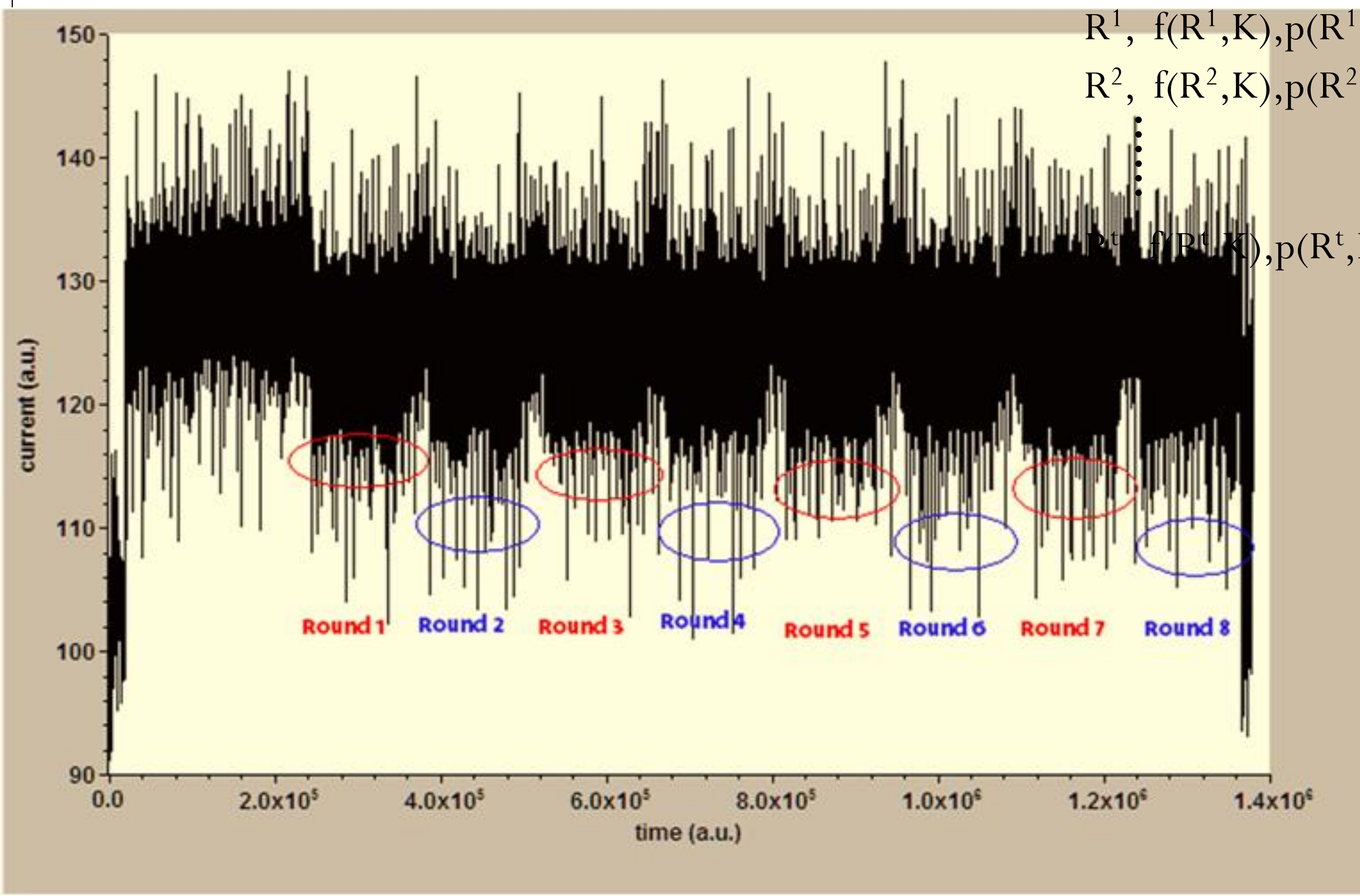
- Send random R, measure the corresponding output and power traces, and repeat.

R^1, f(R^1,K),p(R^1,K)

R^2, f(R^2,K),p(R^2,K)

⋮

R^t, f(R^t,K),p(R^t,K)



Power trace p

How secrets are leaked from traces (leakage model)?

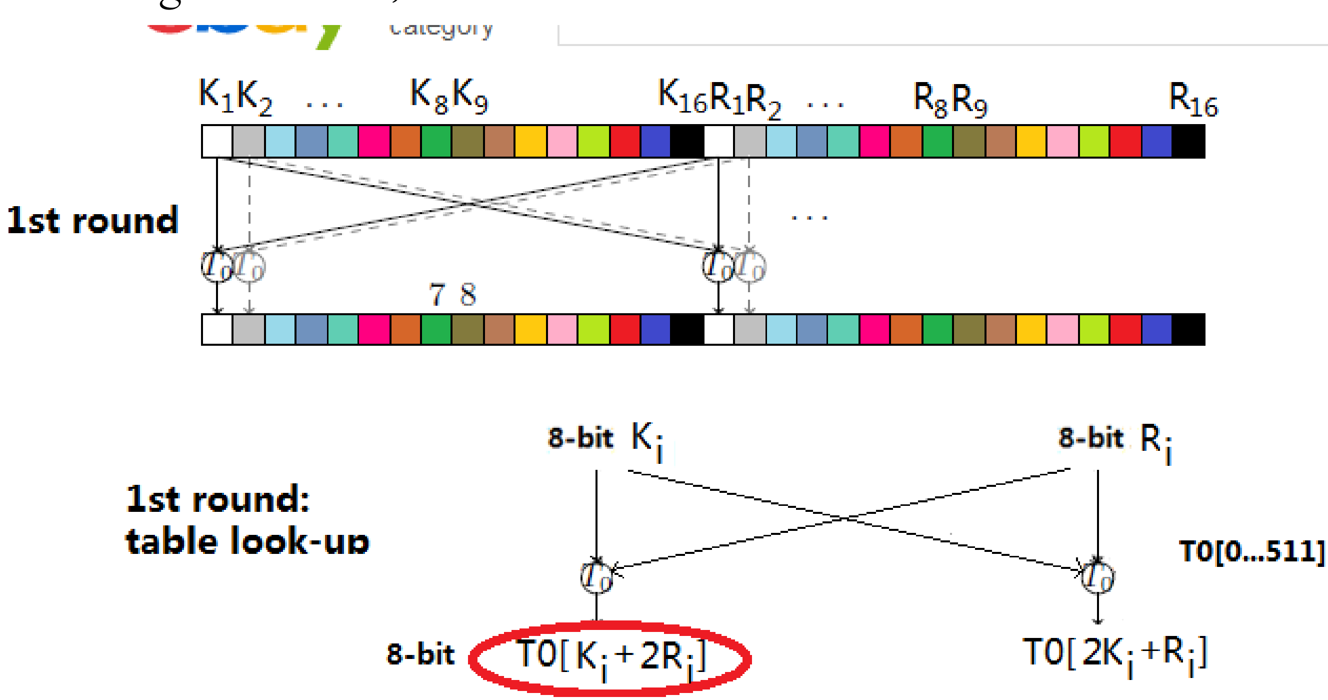
- Hamming weight model: The power consumption (for preserving value e.g. r=10100111) is proportional (or conversely) to its Hamming weight.
- Applicable to CMOS circuits (with precharged data bus)

	time t[i]	time t[i+1]	Power (i→i+1)
Byte[0]	0	1	$E_{0\to1}$
Byte[1]	0	0	$E_{0\to0}$
Byte[2]	0	1	$E_{0\to1}$
Byte[3]	0	0	$E_{0\to0}$
Byte[4]	0	0	$E_{0\to0}$
Byte[5]	0	1	$E_{0\to1}$
Byte[6]	0	1	$E_{0\to1}$
Byte[7]	0	1	$E_{0\to1}$

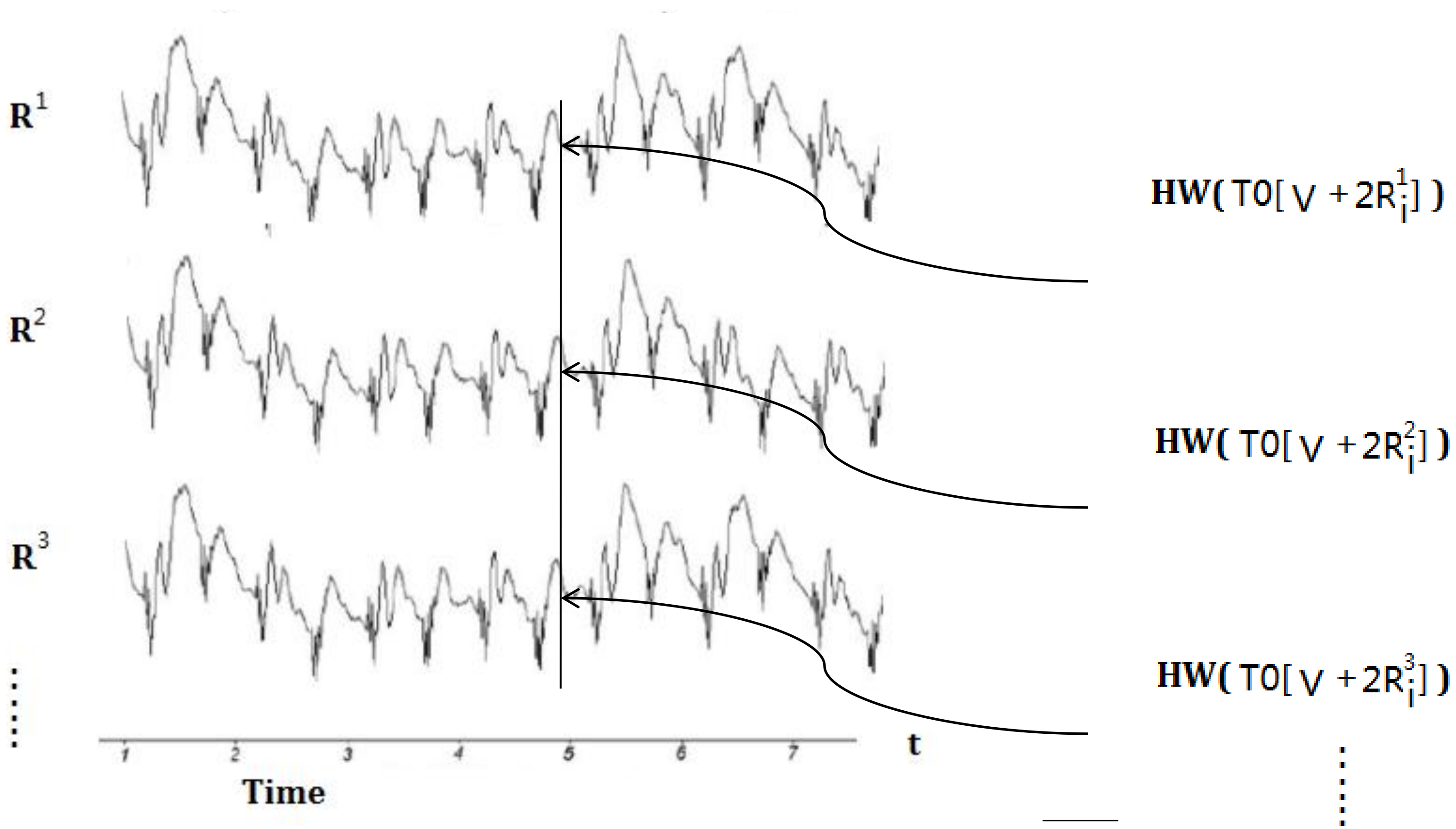
Total: $5E_{0\to1}+3E_{0\to0} \approx 5E_{0\to1}$

Which intermediate result as the target?

- Strategy: Attack one color at a time($0 \leq i \leq 15$), but not fixing the rest colors (not causing SIM card lock).
- hypothesis testing: Target at T0[Ki+2Ri)] , assume Ki= v (256 possibilities), compute the correlation coefficient between T0[v+2Ri]]'s Hamming weight and power traces.
- For correct guess Ki=v , the correlation should be maximal.

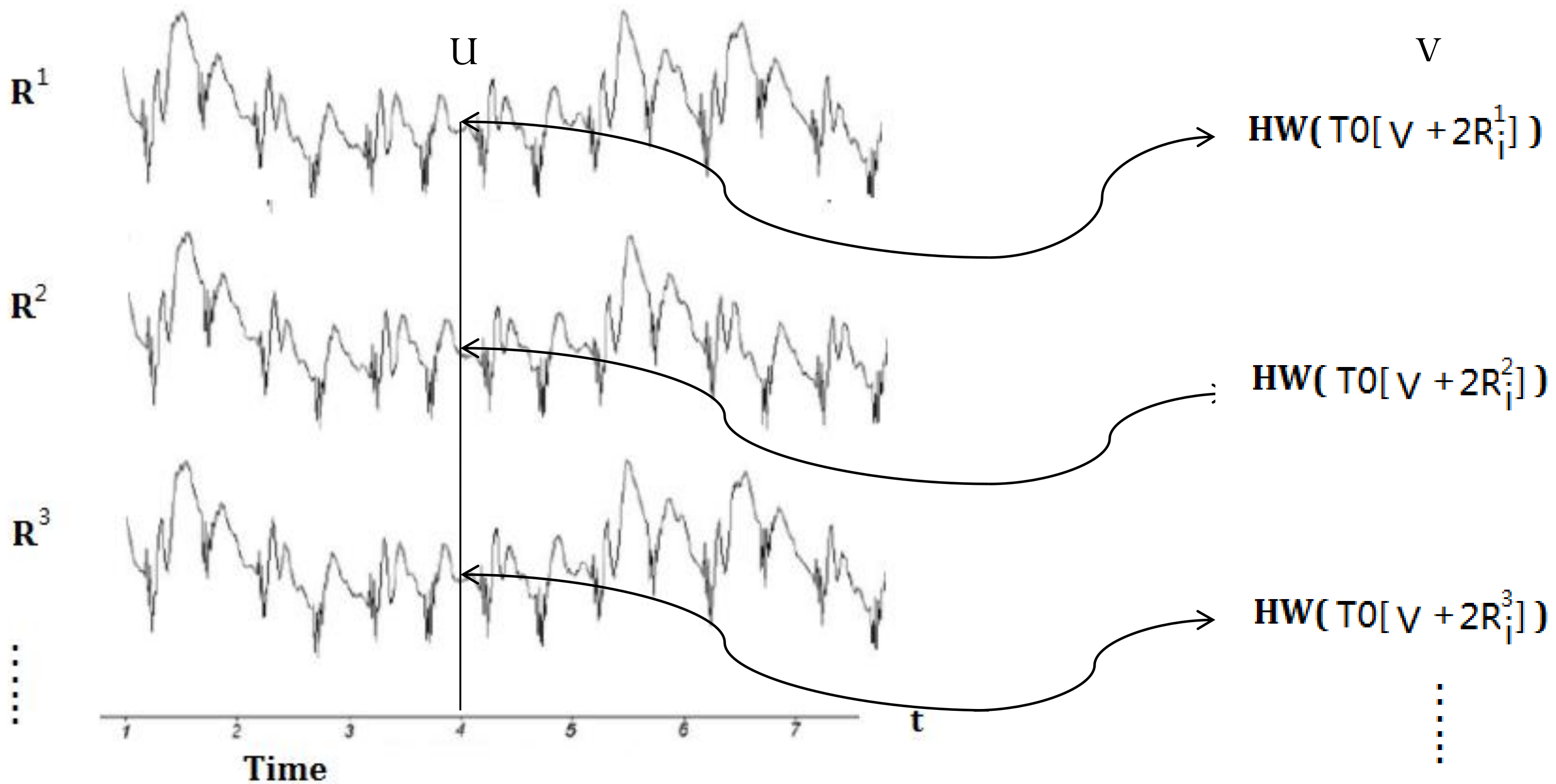


Traces might be misaligned



Assume Ki= v, Compute correlation coefficient (between power traces and HW($T_0[v+2R_i]$))

- hypothesis testing: compute the coefficient corresponding to v=0,1,…,255 one by one, the maximum should be with the correct hypothesis.



Pearson correlation coefficient

Correlation coefficient between U and V, denoted by $\rho_{U,V}$, *is*:

$$\rho_{U,V} \overset{def}{=} \frac{\mathrm{E}[(X-\mu_U)(Y-\mu_V)]}{\sigma_U \sigma_V}$$

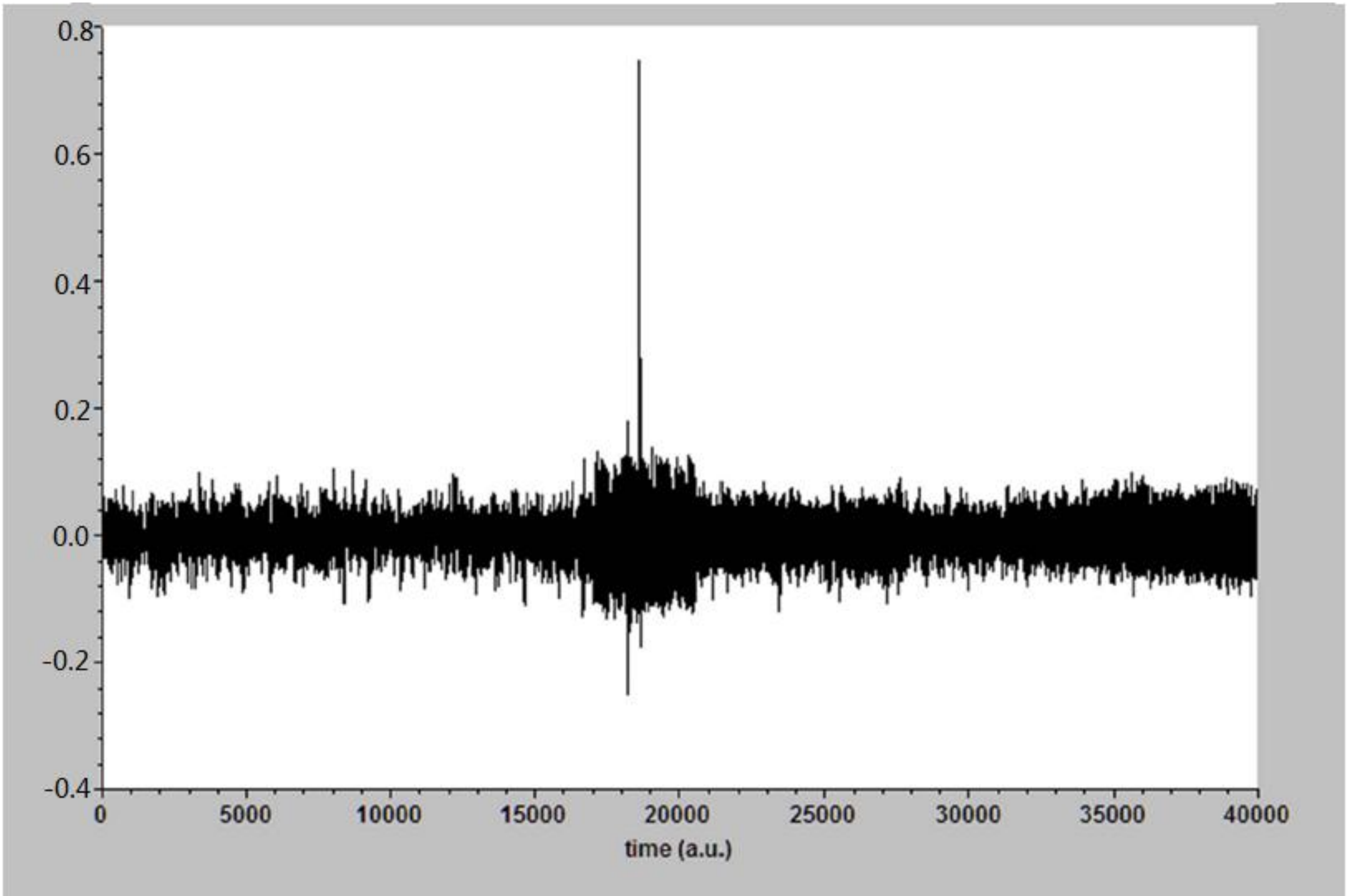
where E is expectation, $\mu_U \overset{def}{=} \mathrm{E}[U]$, and standard deviation $\sigma_U \overset{def}{=} \sqrt{\mathrm{E}[(U-\mu_U)^2]}$.

By sampling from（U,V）to $(u_1,v_1),\ (u_2,v_2),\ \cdots,(u_n,v_n)$, the estimator of $\rho_{X,Y}$, denoted by $r_{x,y}$, is given by:

$$r_{x,y} = \frac{\sum_{i=1}^{n}(u_i-\bar{u})(v_i-\bar{v})}{\sqrt{\sum_{i=1}^{n}(u_i-\bar{u})^2}\sqrt{\sum_{i=1}^{n}(v_i-\bar{v})^2}},$$

where $\bar{u} = \dfrac{u_1+u_2+\cdots+u_n}{n}$ and $\bar{v} = \dfrac{v_1+v_2+\cdots+v_n}{n}$ detotes mean value.

coefficient for a correct hypothesis (K_i=v)



Power analysis vs. collision attacks

- Targets: 4 SIM cards from two mobile operators and 4 different manufacters
- Efforts in terms of: the number of inputs (traces) needed.

	manufacturer	operator	patch (countermeasure)	DPA	collision attacks
SIM#1	I	A	Not available	400	20,000
SIM#2	II	B	I-C	200	≥20,000
SIM#3	III	B	I-C + C-F	4000	fail (card locked)
SIM#4	IV	B	I-C + C-F	10000	fail (card locked)

- Collision attacks: cheap set-up, only applicable to unpatched targets
- Power analysis: powerful, provided with special measurement setup

Lessons Learned

- Awareness of physical security for small embedded devices.
- The contrast:
  - Low cost devices ≈ limited budget for CC/EMVCo security testing.
  - Low-cost × huge volume = big impact / loss
- Some SIM cards are used for more sensitive applications such as mobile payments.
- Practical security requires BOTH:
  - A mathematically secure (and publicly referred) algorithm.
  - Sufficient countermeasures in place against physical attacks.

Thanks!