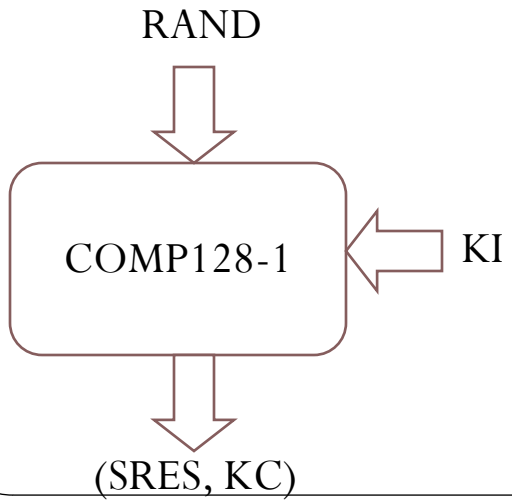
Lecture 1: (part 2)

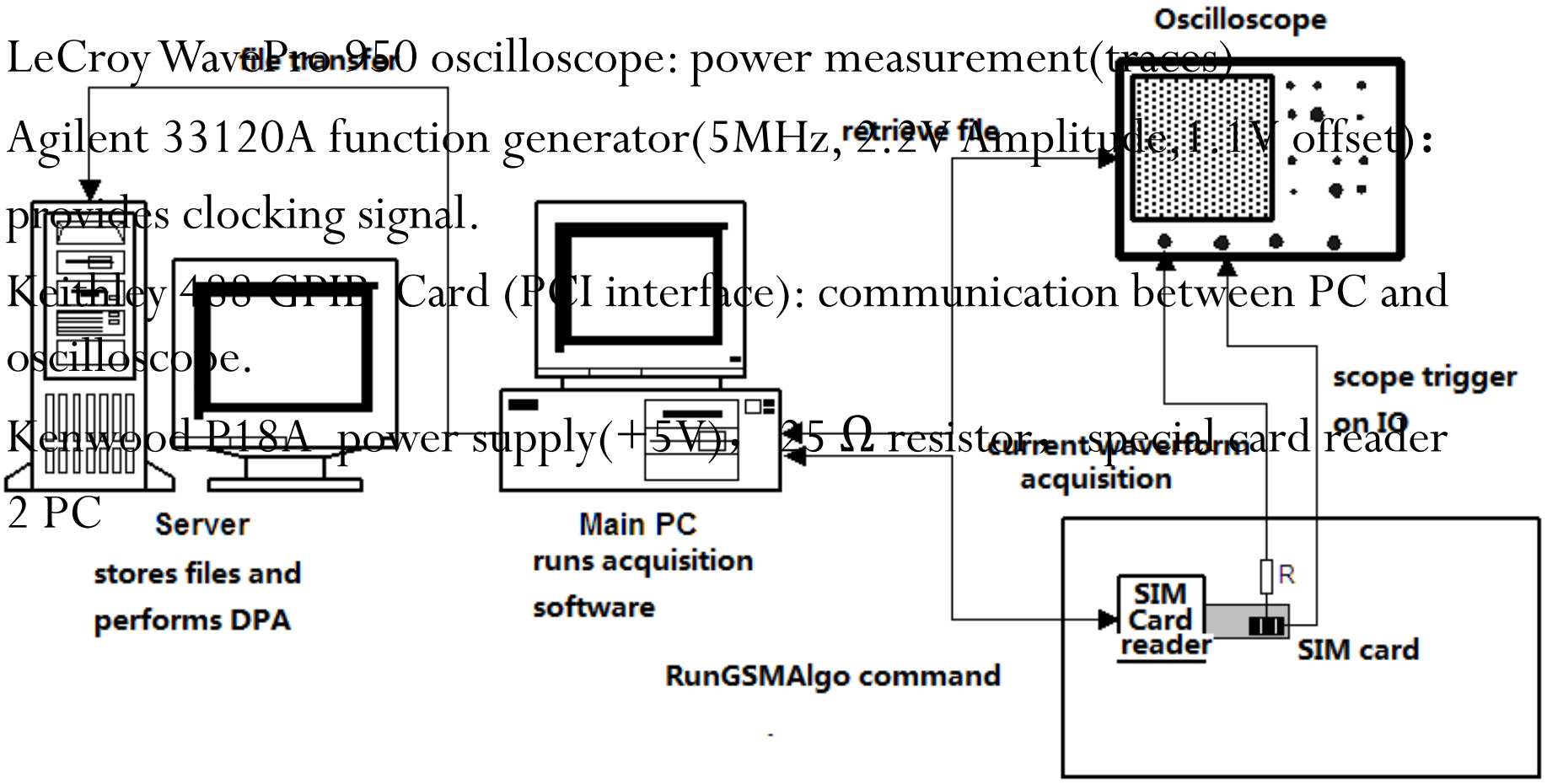
Attack 2： Power Analysis Attacks

- Collision attacks fail because they are easy to detect.
- Power anlaysis： Send truly random R to SIM, not causing sim lock.
- How it works： SIM relies on external power and clocking signal.
- It needs also a special measurement setup, signal and data preprocessing and cryptanalysis.



Measurement Setup for Power Analysis

- LeCroy WavePro 950 oscilloscope: power measurement(traces)
- Agilent 33120A function generator(5MHz, 2.2V Amplitude, 1.1V offset): provides clocking signal.
- Keithley 488 GPIB Card (PCI interface): communication between PC and oscilloscope.
- Kenwood P18A power supply(+5V), 25 Ω resistor, special card reader
- 2 PC



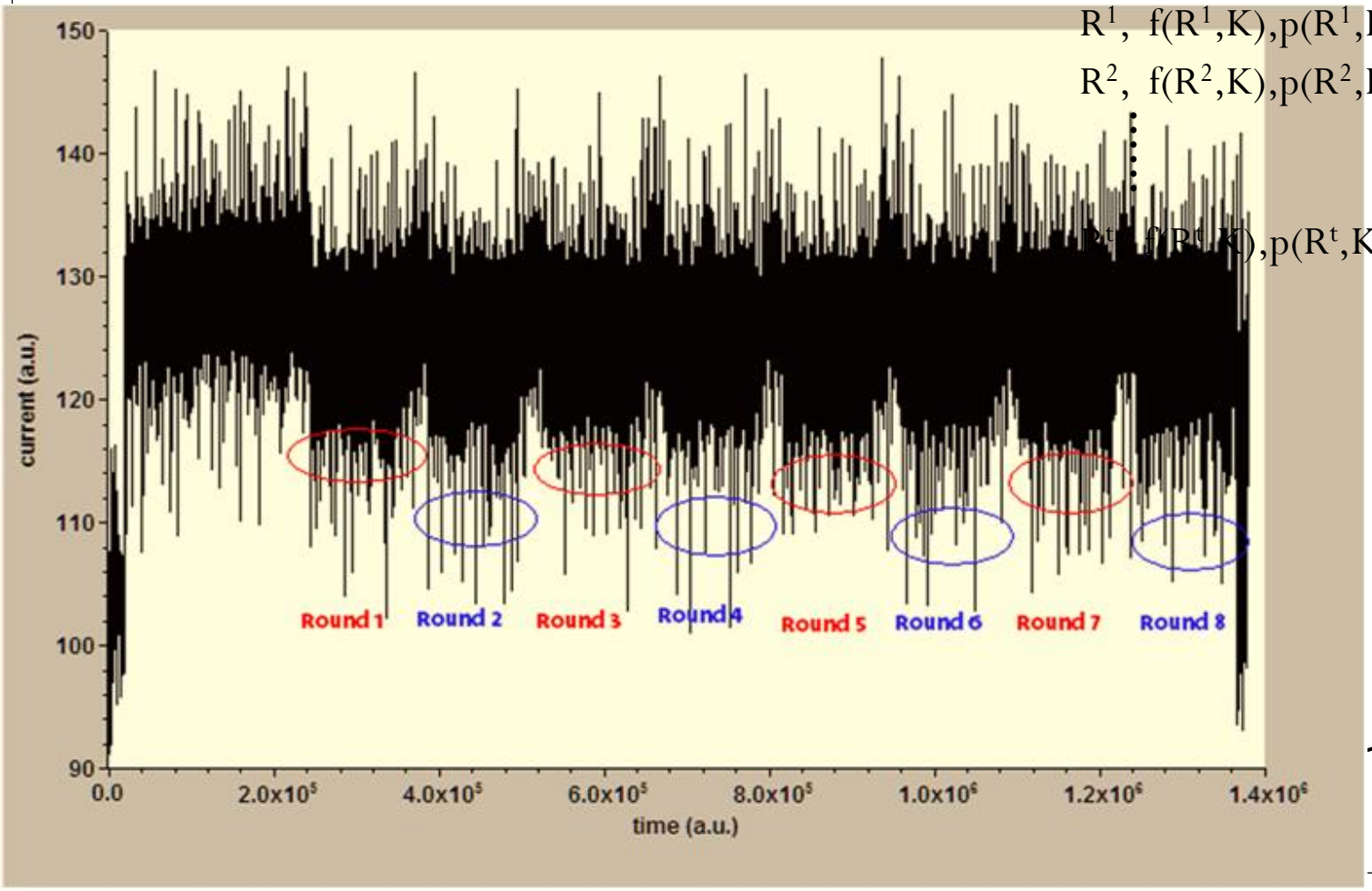
Power Trace Measurement

- 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

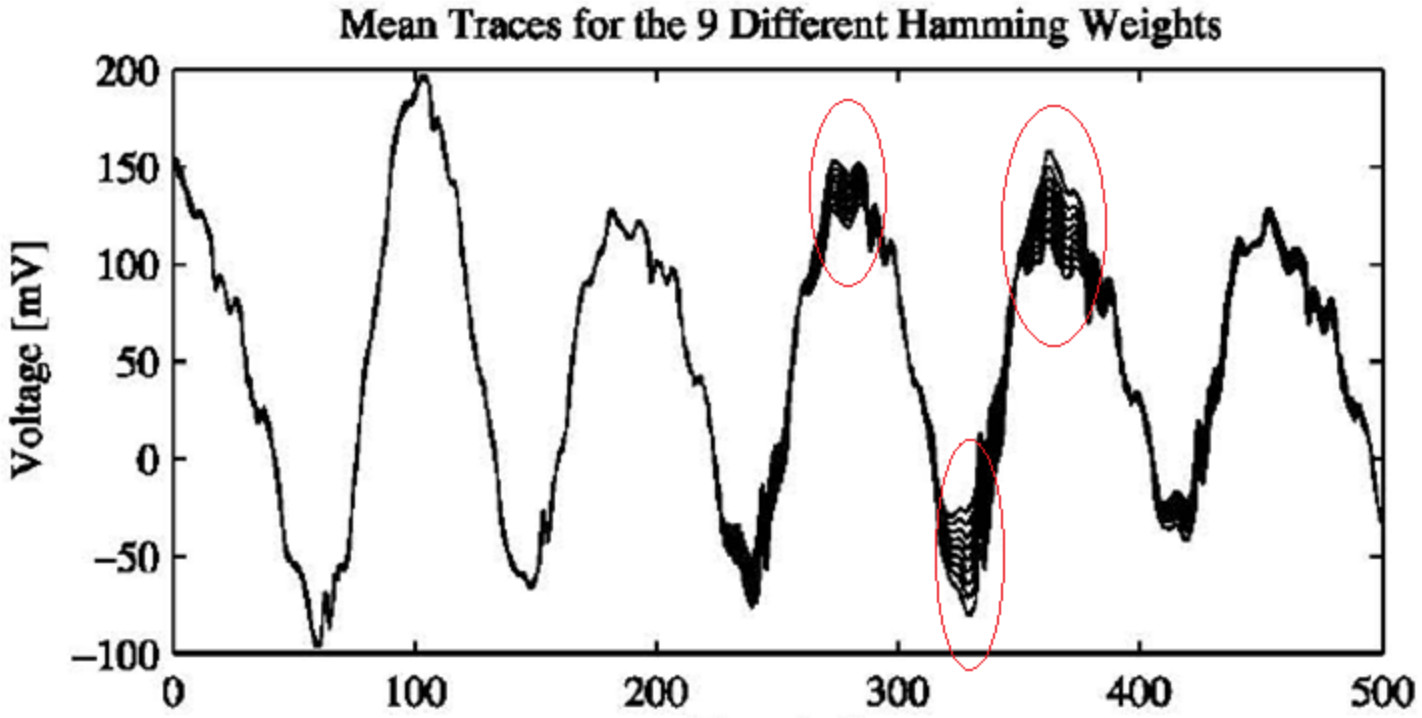
How secrets are leaked from traces (leakage model)?

- Hamming weight model: The power consumption for storing a value (e.g. r=10100111) is proportional (or conversely) to the Hamming weight of that value.
- Why?: In CMOS circuits, data bus is precharged with constant voltages (e.g. GND or VCC).

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

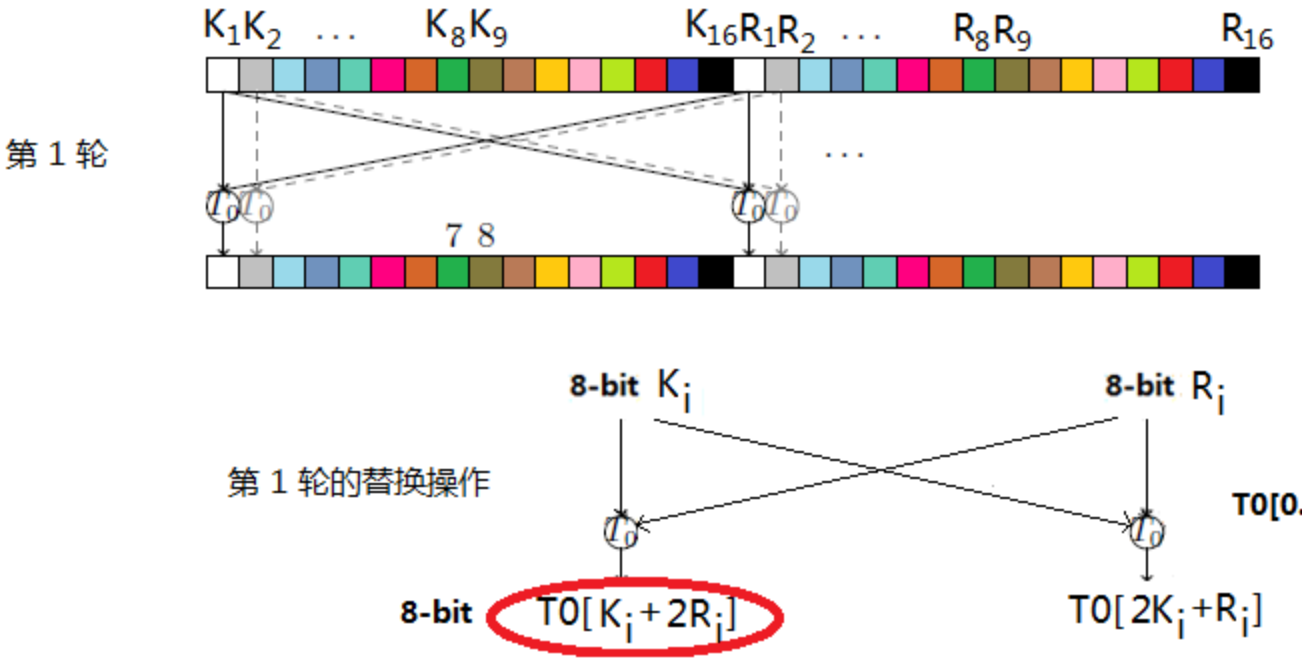
Power traces with intermediate results of different hamming weights.



Note: the above power traces have been preprocessed (e.g. noise reduction)

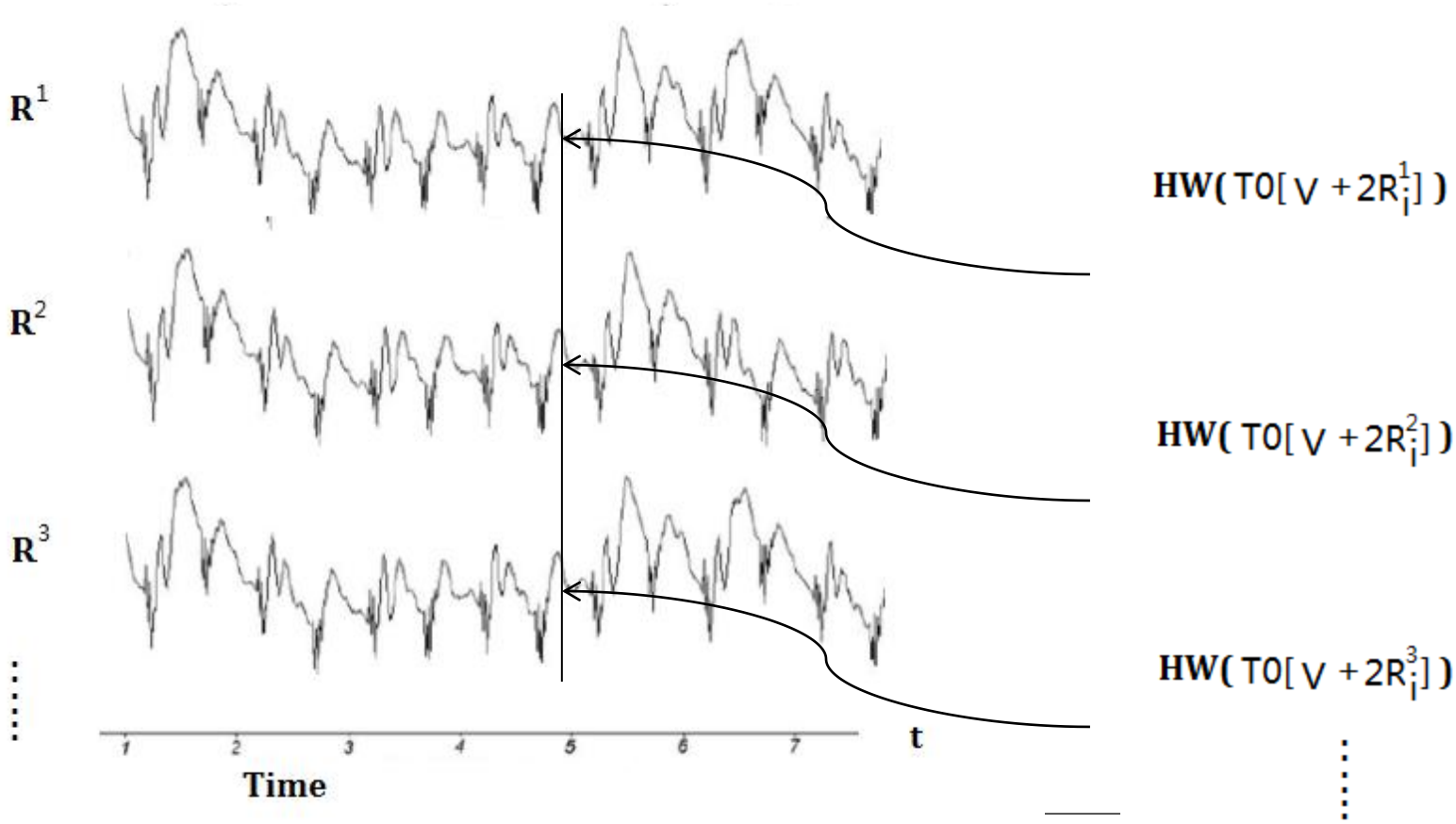
Which intermediate result as the target?

- Strategy: Attack one color at a time($0 \le i \le 15$), but not fixing the other 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.
-



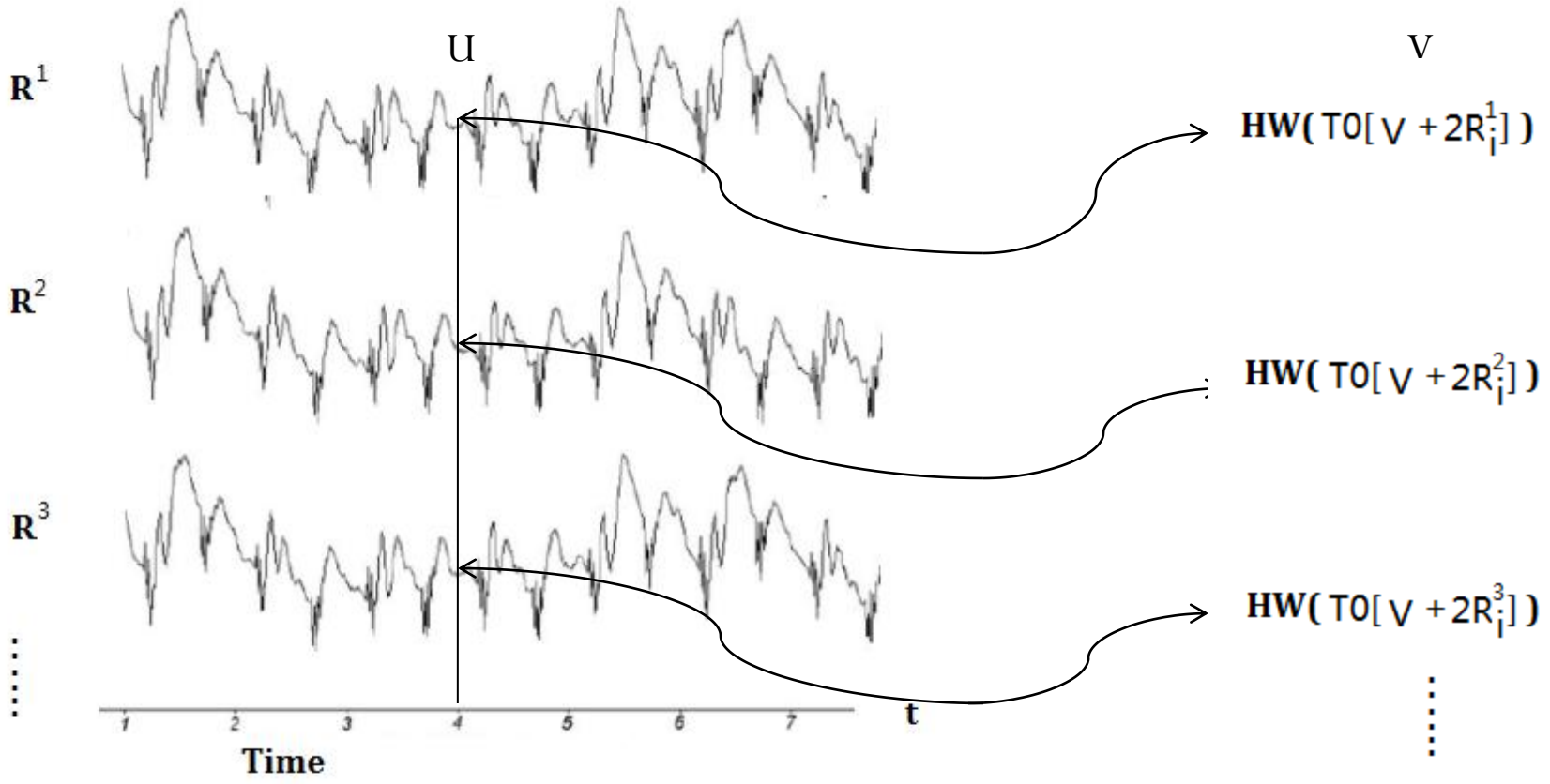
Traces are misaligned

Must be aligned before conducting the attack.



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*:

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

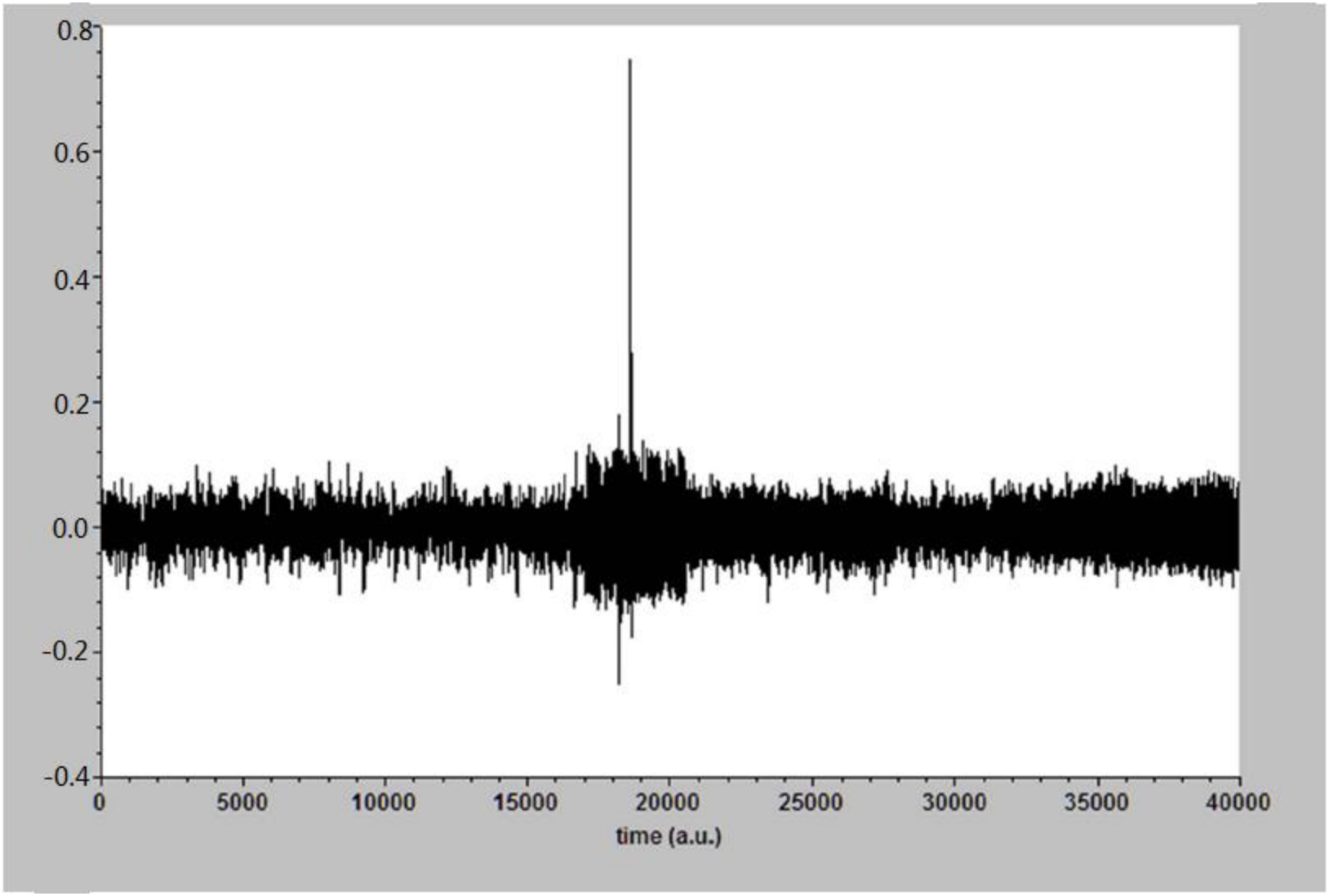
where E is expectation, $\mu_U \overset{def}{=} \mathrm{E}[U]$, and standard deviation $\sigma_U \overset{def}{=} \sqrt{\mathrm{E}[(U-\mu_U)^2]}$.

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

The coefficient plot for a correct hypothesis (K_i=v)



Power analysis vs. collision attacks

- Targets： 4 SIM cards from two mobile operator and 4 different manufacters
- Efficiency in terms of： the number of inputs needed.

	制造商	运营商	保护措施	功耗分析	碰撞攻击
SIM#1	I	A	无	400	20,000
SIM#2	II	B	I-C	200	≥20,000
SIM#3	III	B	I-C + C-F	4000	失败(被锁卡)
SIM#4	IV	B	I-C + C-F	10000	失败(被锁卡)

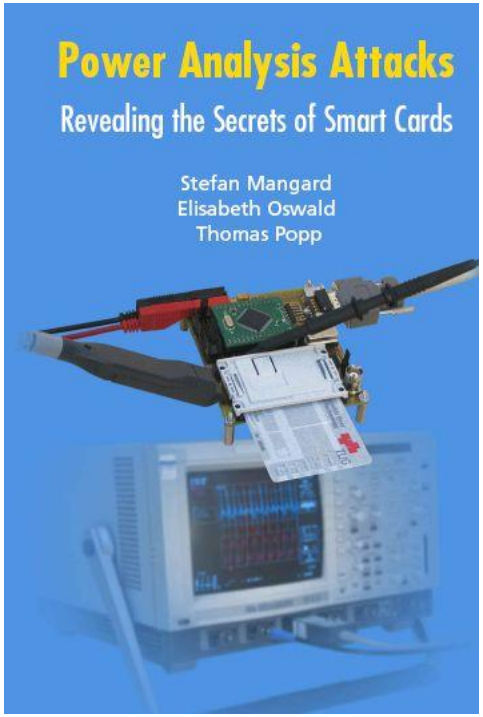
- Collision attacks： low-cost, fast implementation, and easily detected (prevented).

  not applicable to new SIM cards
- Power analysis： powerful, but needs special measure setup.

1. Measurement setup(~60k usd).
2. Knowledge in cryptanalysis, statistics and signal processing.

More advanced topics about power analysis

- The DPA Book. www.dpabook.org
- Recent updates: The CHES, Crypto, Eurocrypt conferences organized by IACR (International Association for Cryptologic Research).



the measurement setup at IIIS

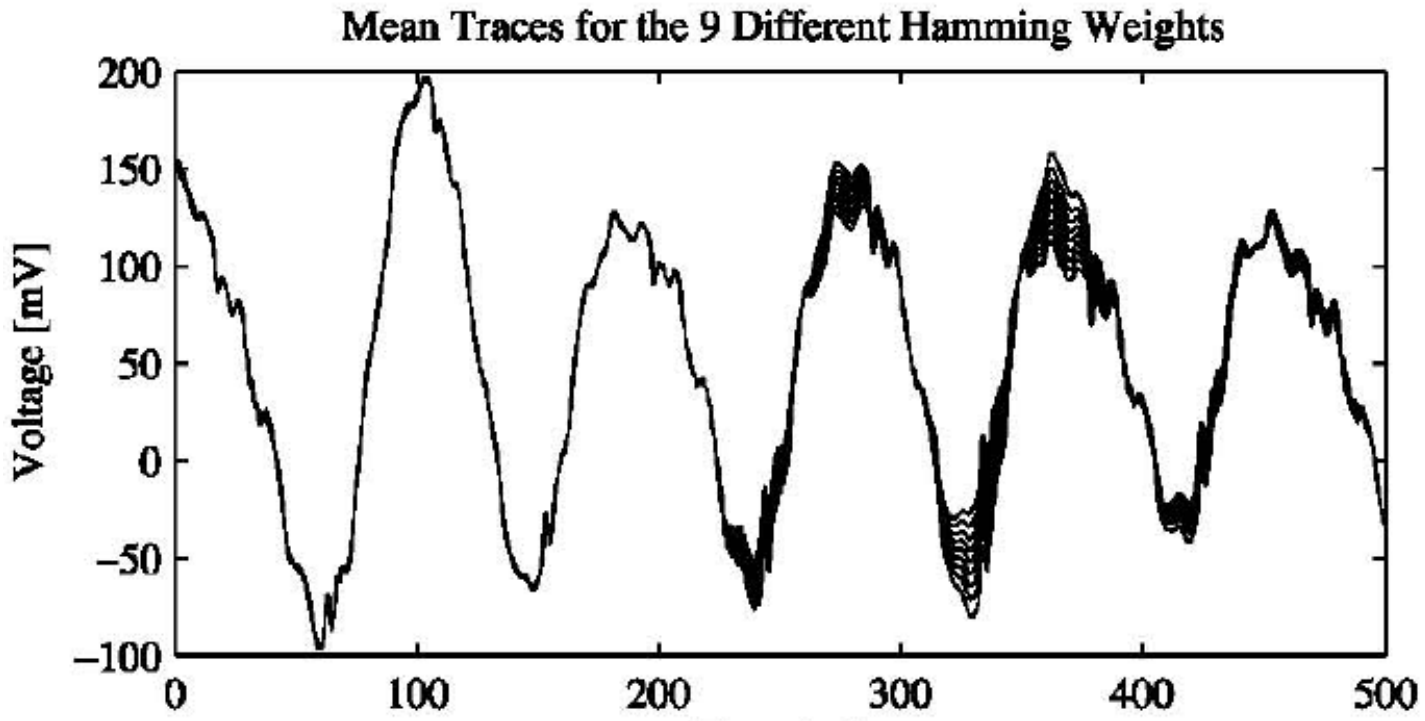
Open to interested undergraduate students.

Please contact me if you're interested in doing such experiments!

Thanks!

汉明重量模型(Hamming weight model):

- 如果没有噪声,从功耗曲线中直接读出中间变量的汉明重量:
  简单功耗分析 (Simple Power Analysis)



- 有噪声情况下,可采用统计方法获得汉明重量的信息(采样数量取决于信噪比)：差分功耗分析(Differential Power Analysis)