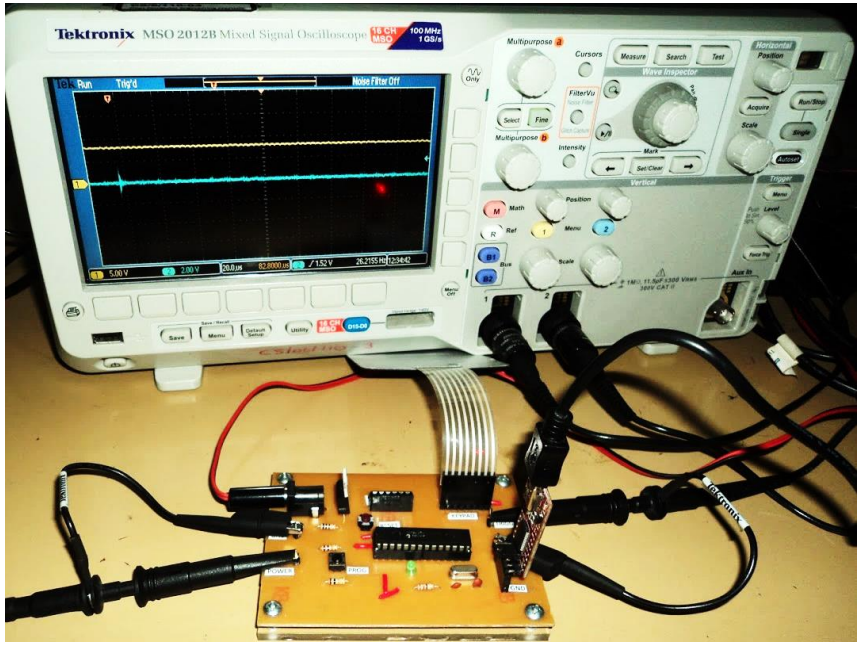
Power Analysis Attacks

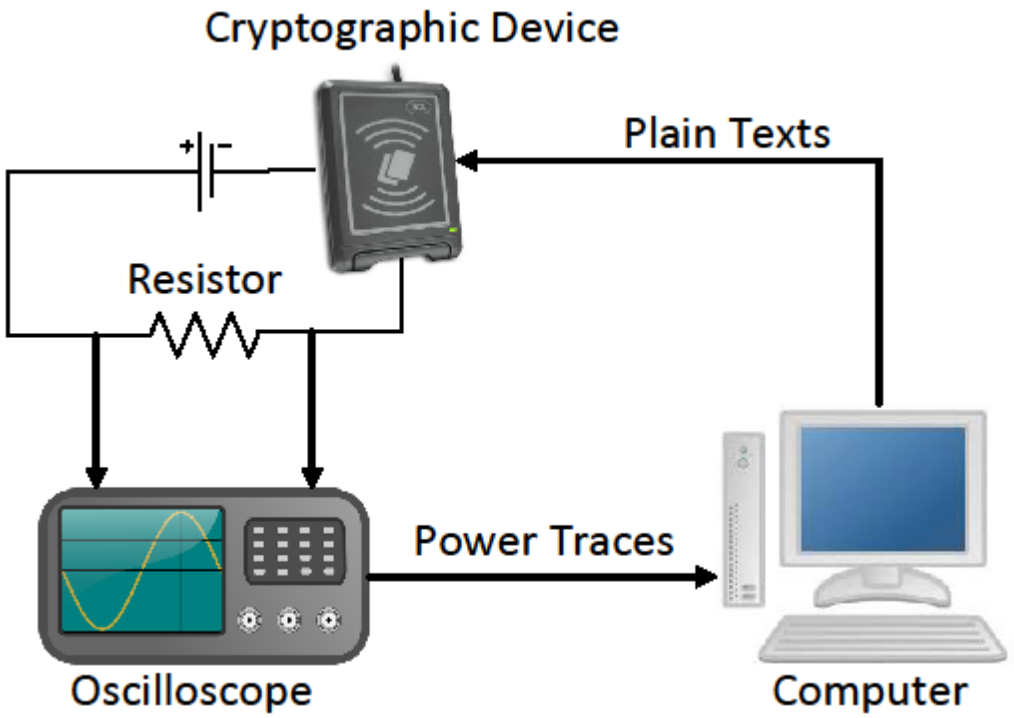


Tutorial on Cryptographic and Security Aspects for
Information and Communication Systems
At ICIAfS 2016

Dec. 18, 2016

Hasindu Gamaarachchi
Department of Computer Engineering,
University of Peradeniya
hasindu2008@gmail.com

Power analysis

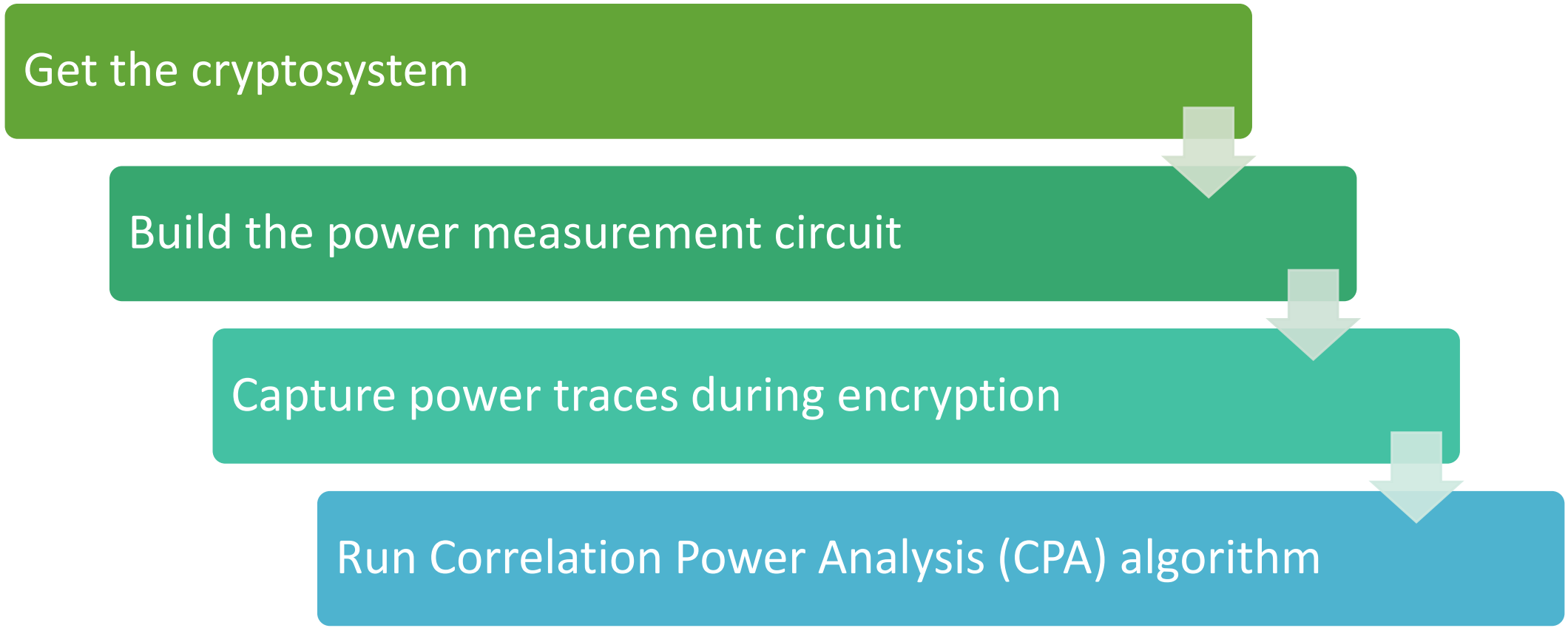


- Use power consumption data as the side channel
- First collect power traces
- Then do mathematical analysis
  - Simple power analysis
  - Differential power analysis
  - Correlation power analysis
  - Mutual information analysis

Target devices for the attack

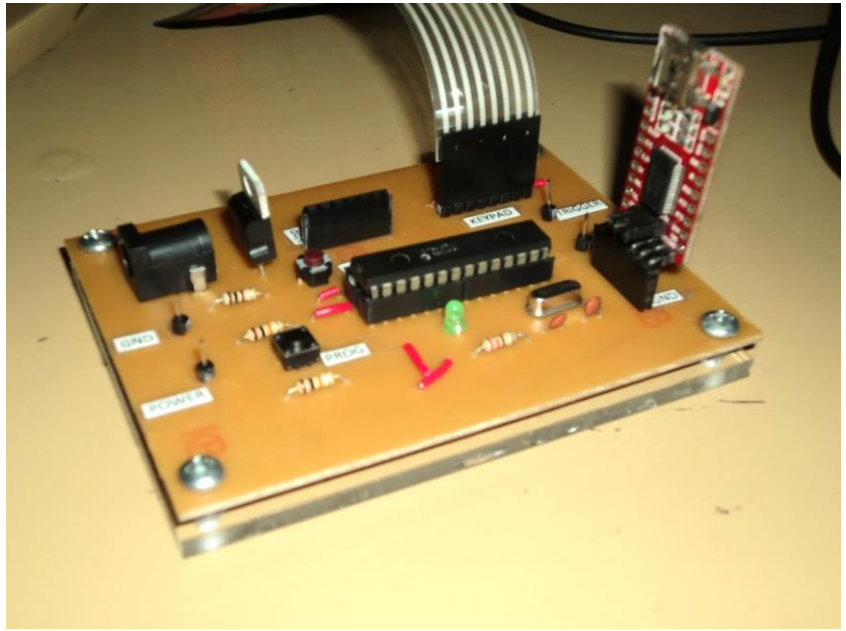
- Security of embedded devices such as smartcards was completely shattered when power analysis attack was introduced
- But today various countermeasures have been applied

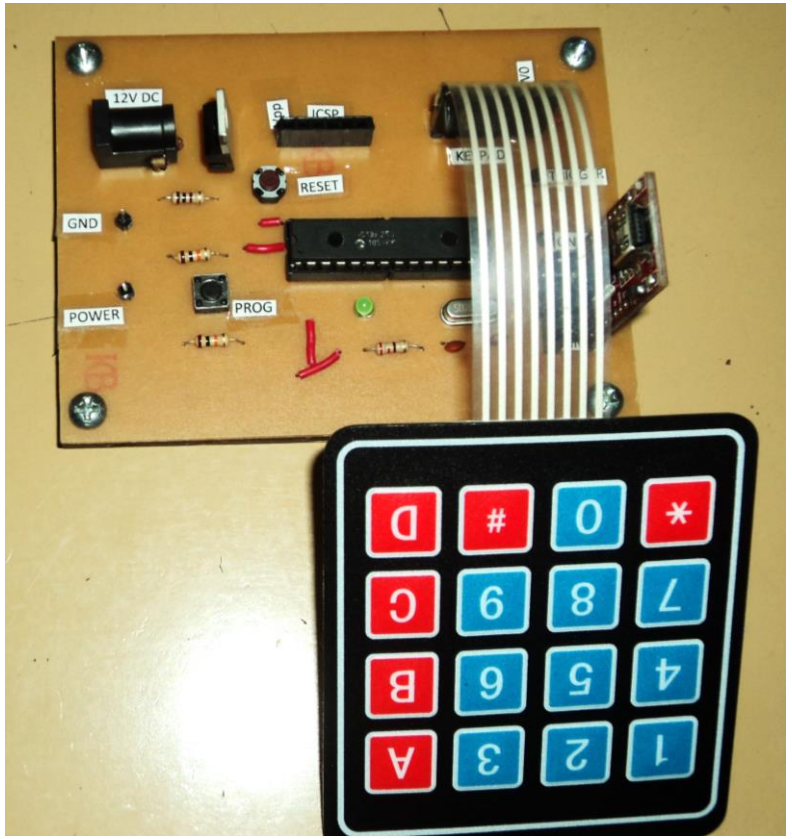
Basic Steps of Power Analysis Attack



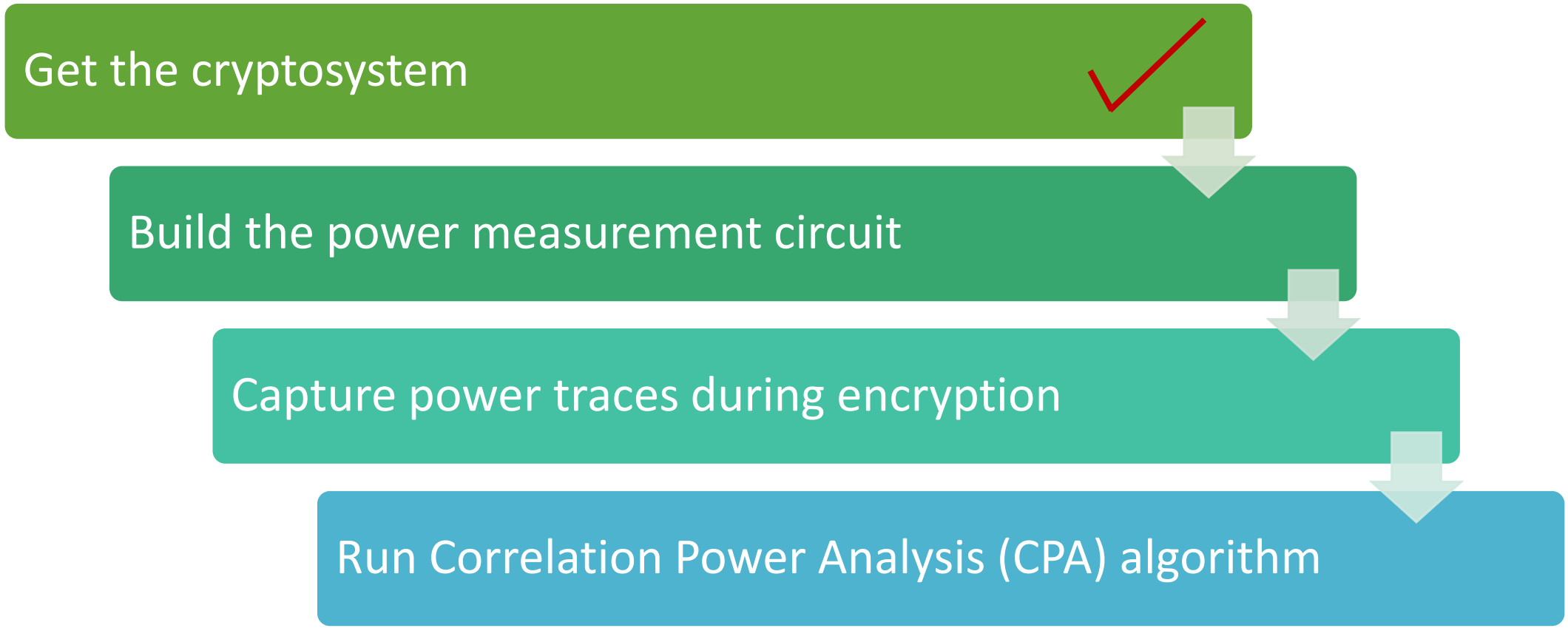
Our cryptographic device

- A PIC microcontroller based circuit that mimics the operation of a smartcard
- Programmed to run AES

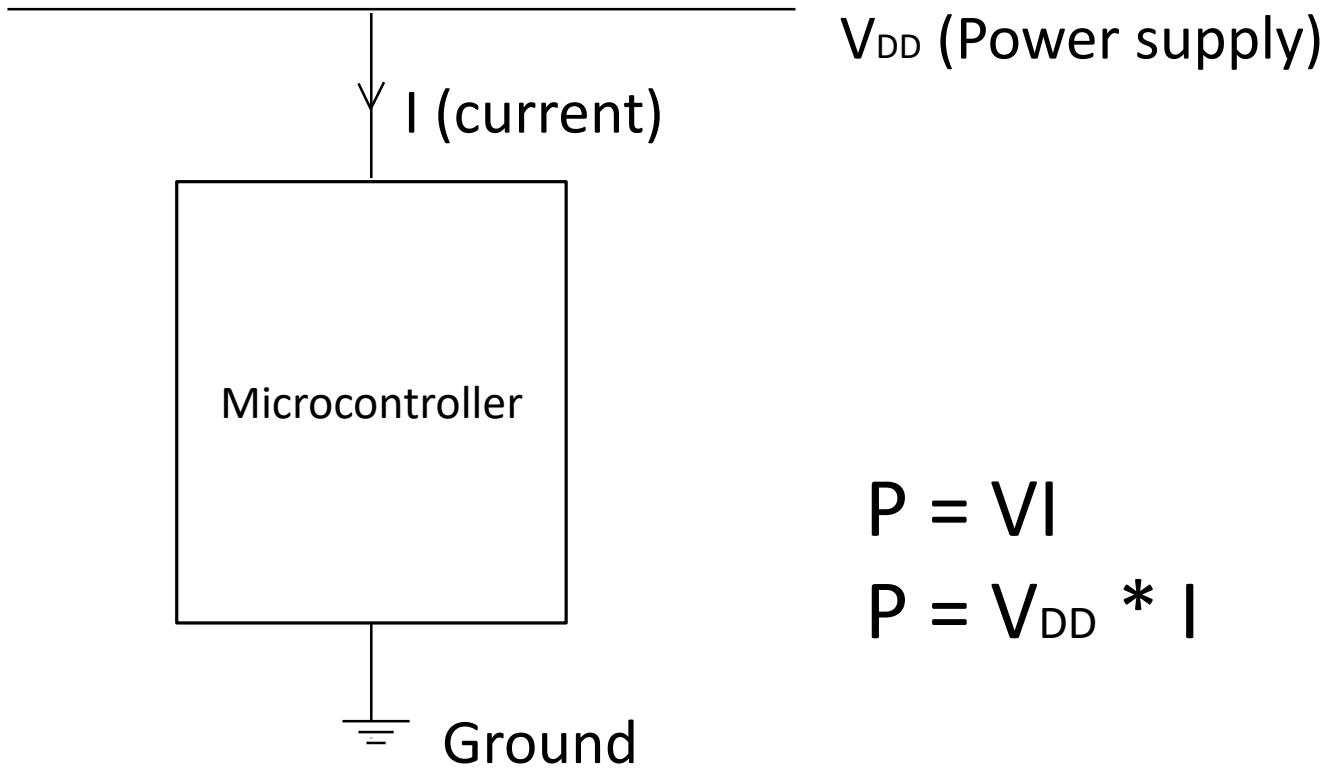




Basic Steps of Power Analysis Attack



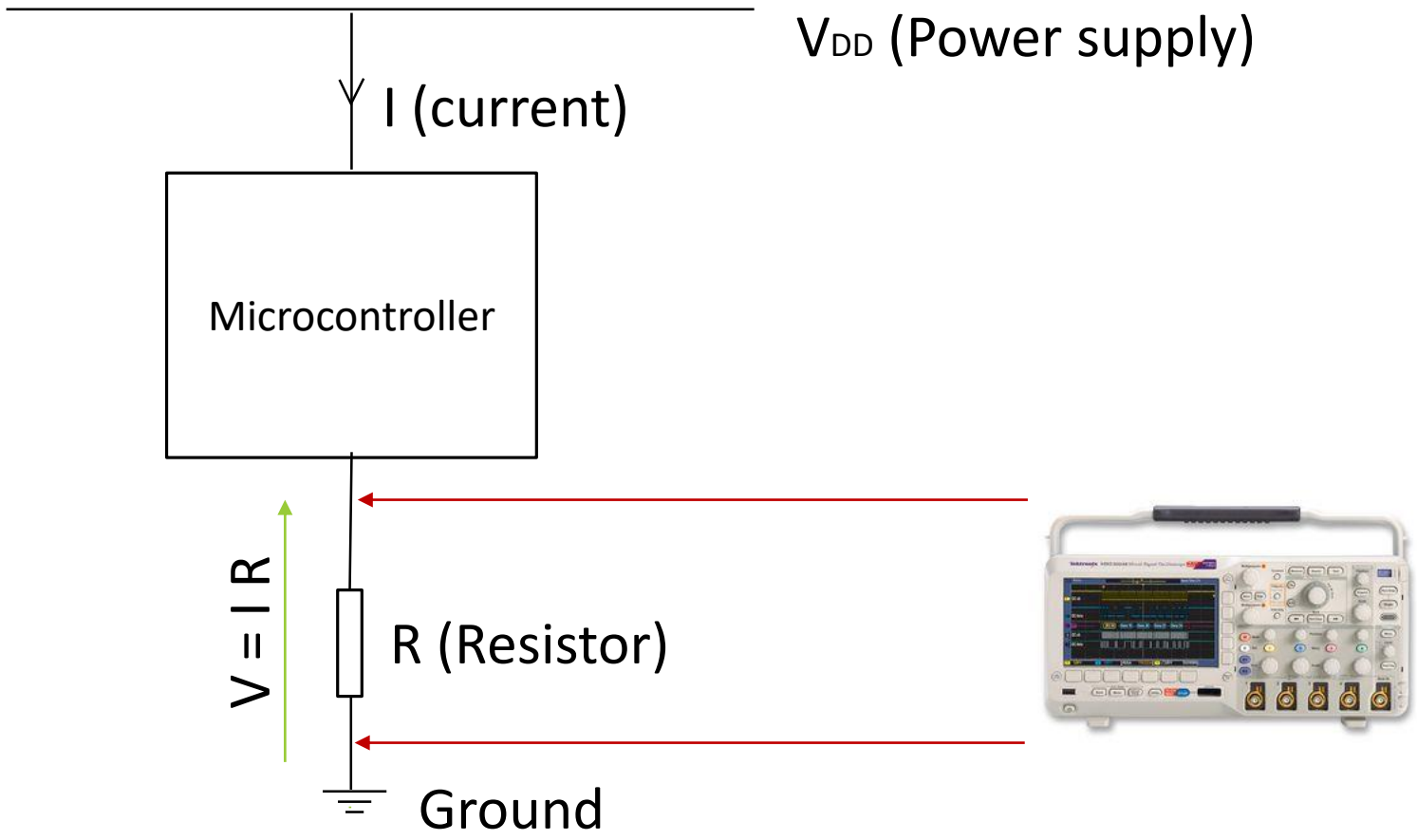
Power Measurement



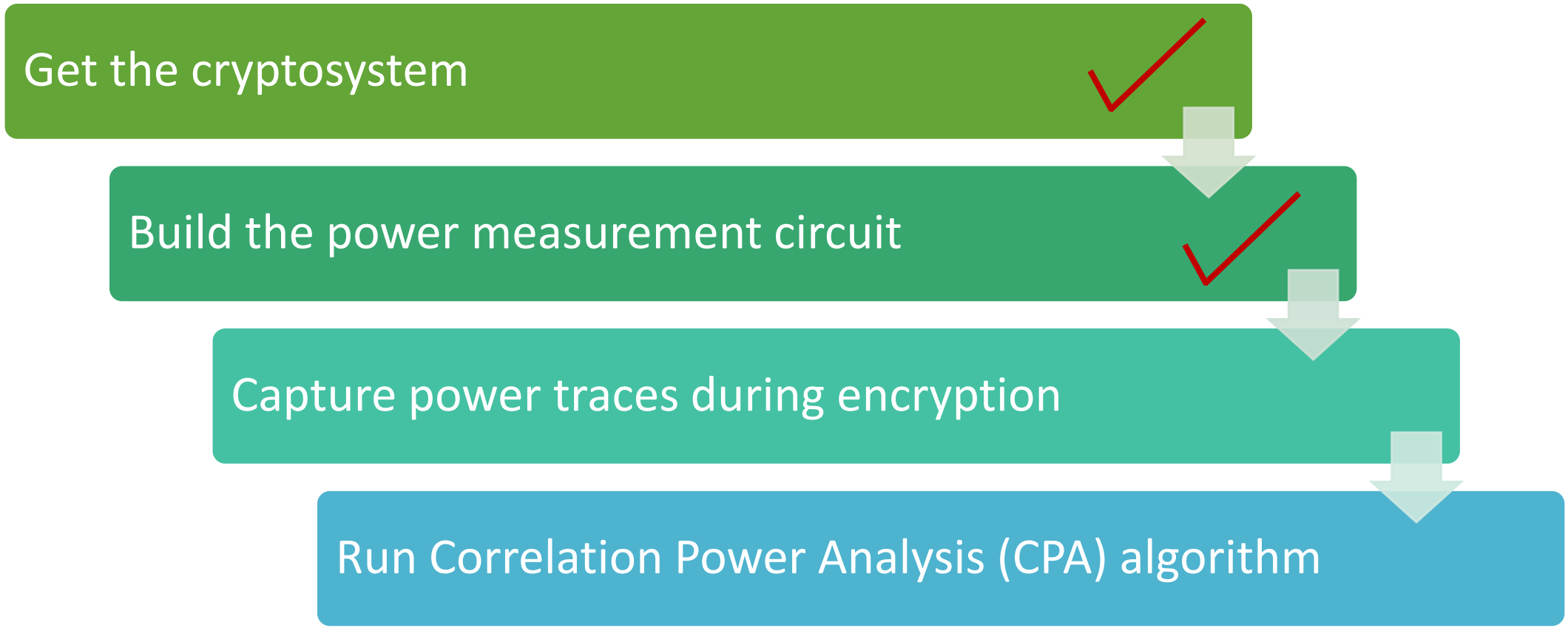
$P = VI$

$P = V_{DD} * I$

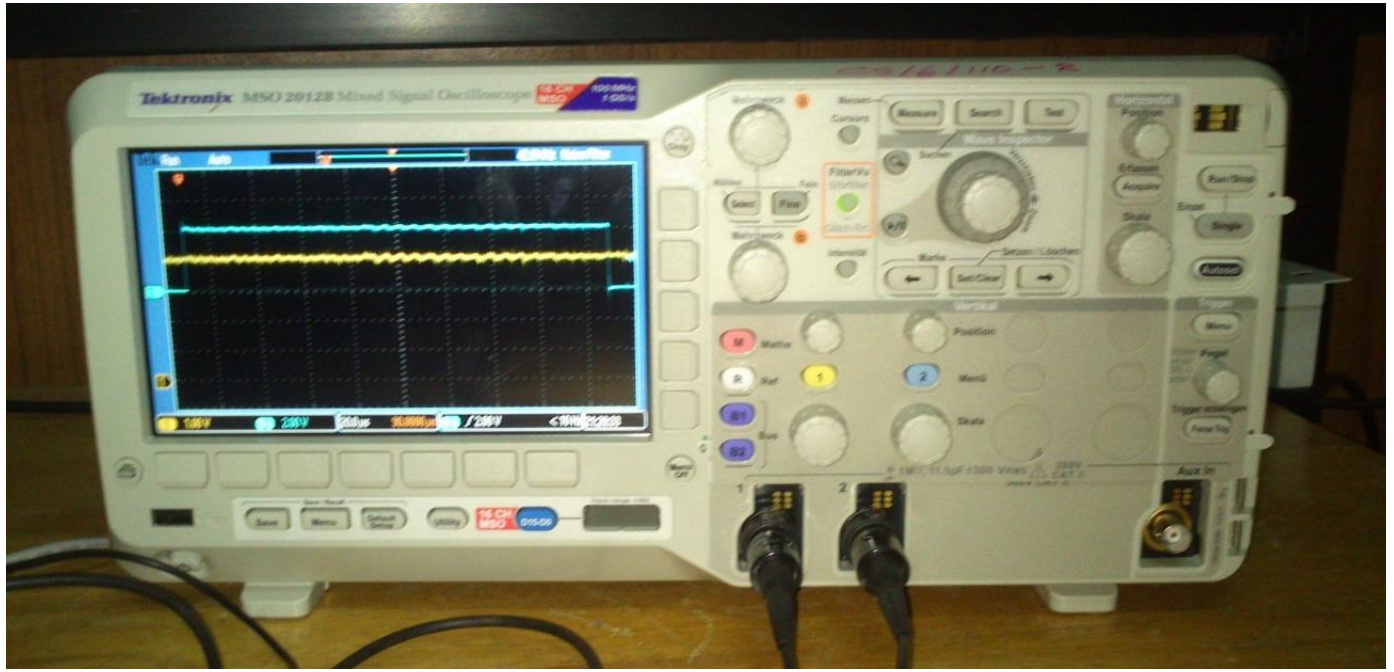
Power Measurement



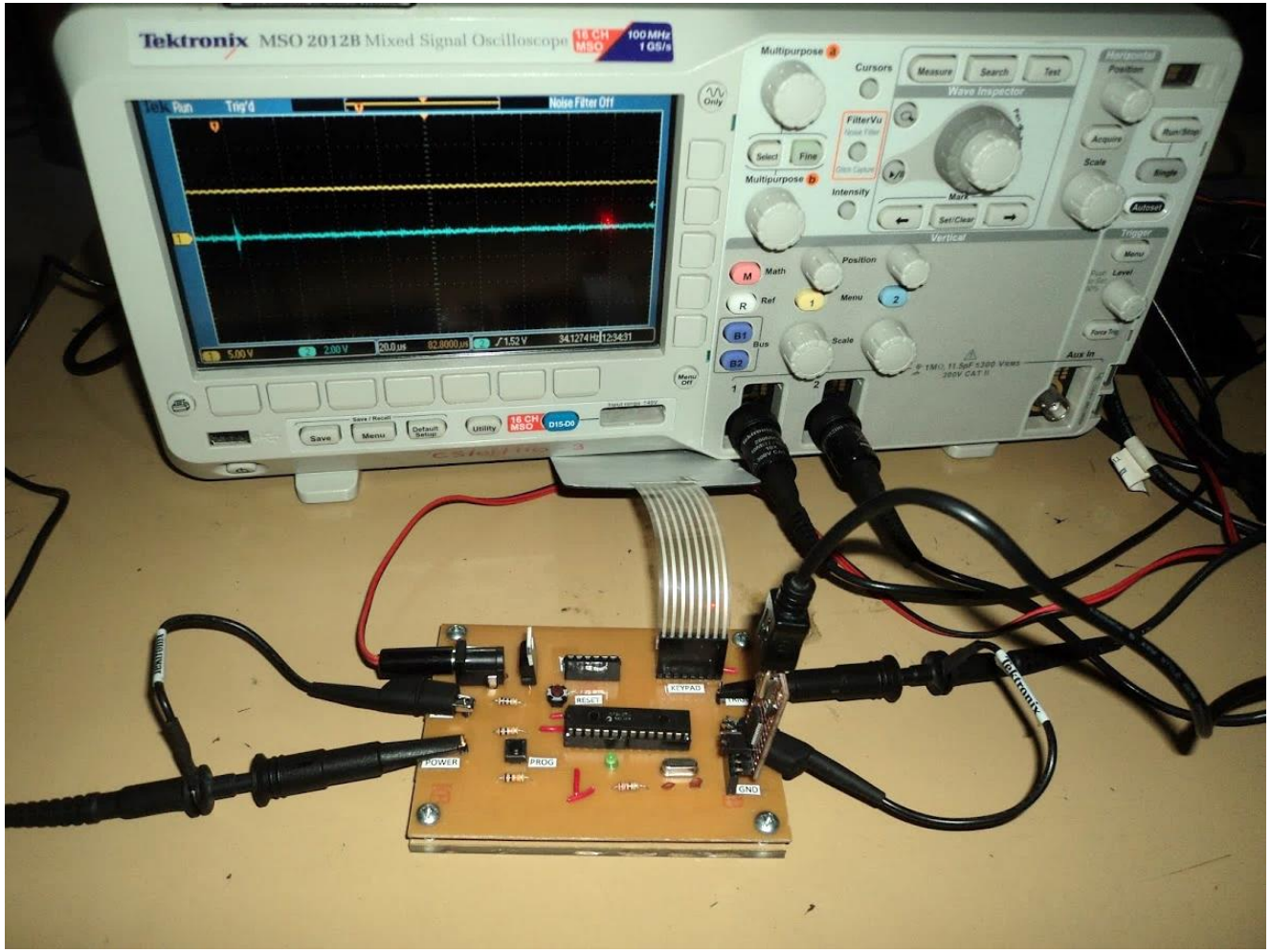
Basic Steps of Power Analysis Attack



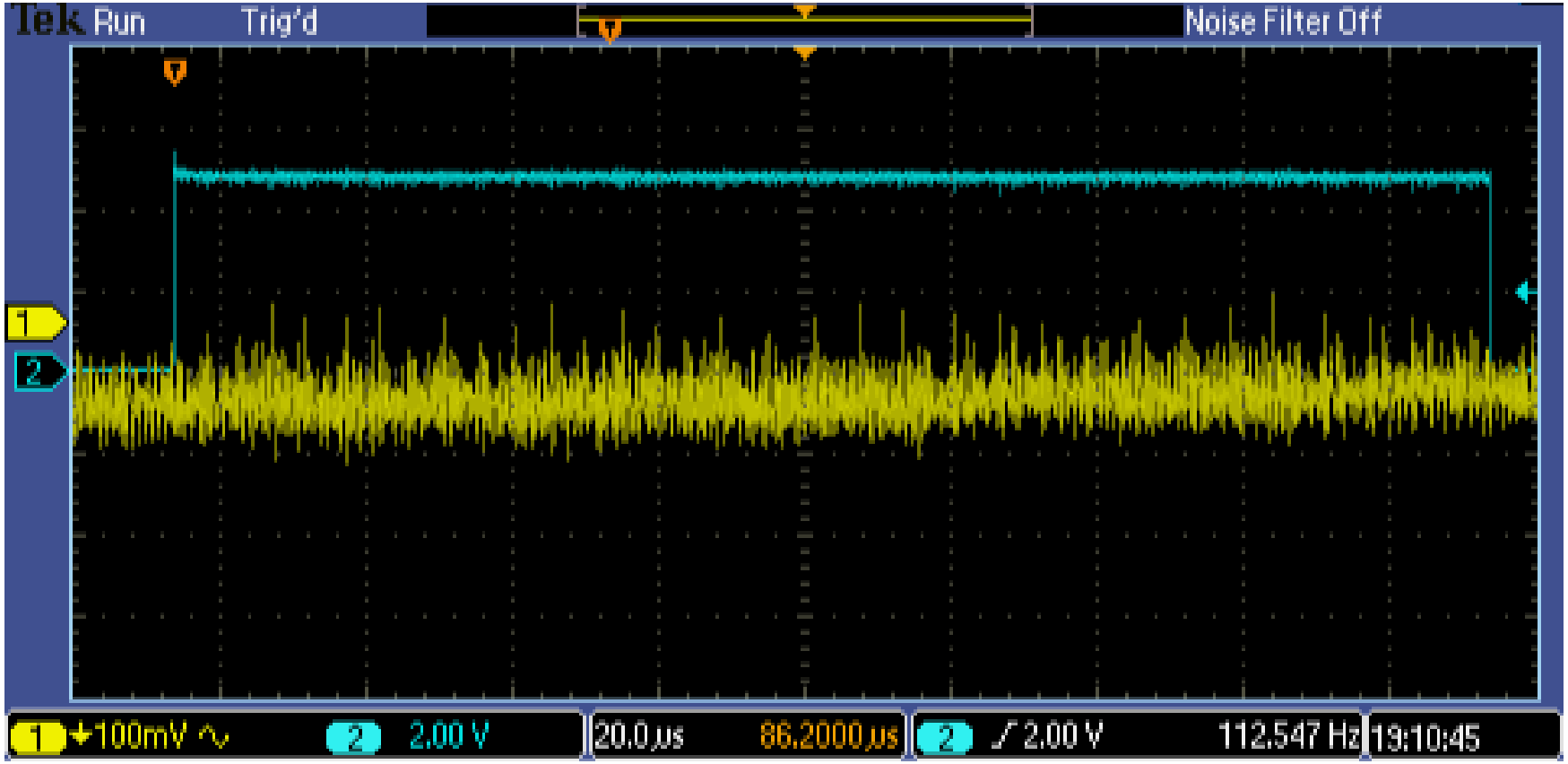
Oscilloscope (Tektronix MSO2012B)



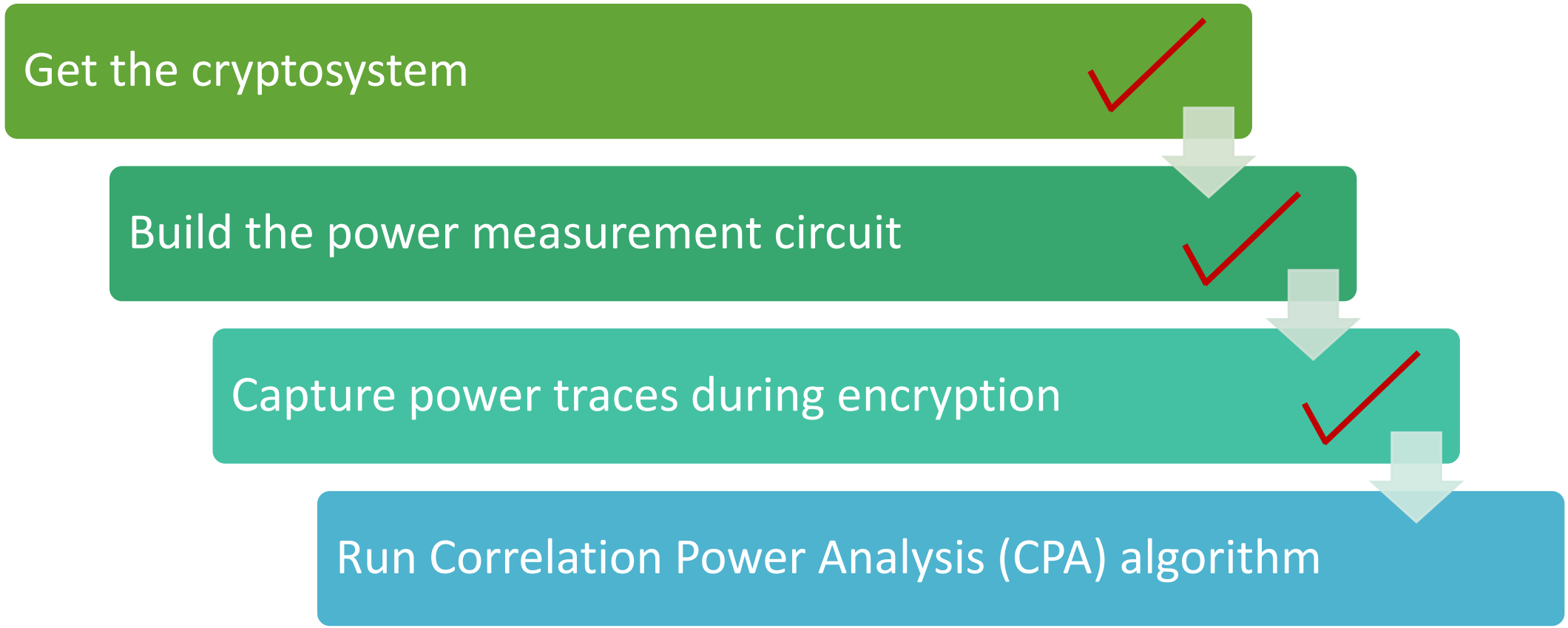
Connecting the oscilloscope



A power trace



Basic Steps of Power Analysis Attack



CPA Algorithm on CUDA

*D:\Hasindu\Documents\university\Semester 7\CO411-Individual Project 1\wave analysis for aes\key dependence\kernel.cu - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

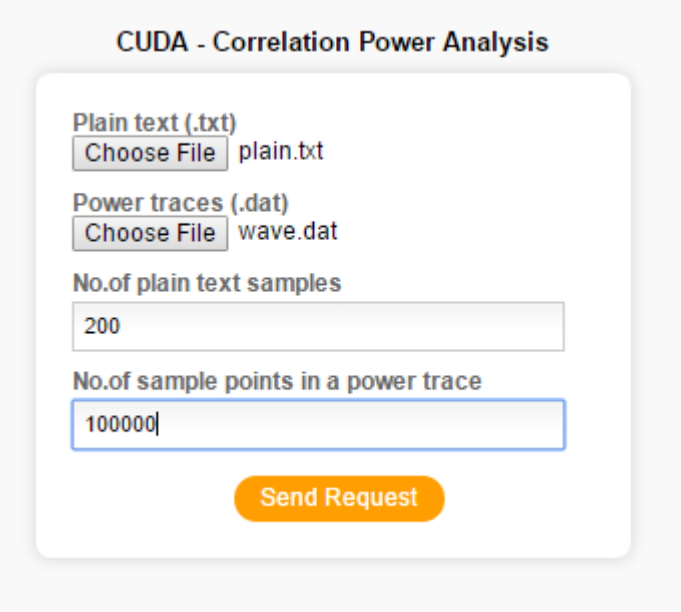
kernel.cu

```
187             fscanf(file,"%f",&dat);
188             if(j<WAVELENGTH*(loops+1) && j>=WAVELENGTH*loops){
189                 wavedata[i*WAVELENGTH+k]=(double)dat;
190                 k++;
191             }
192         }
193     }
194     fclose(file);
195
196     checkCudaError(cudaMemcpy(dev_wavedata,wavedata,SAMPLES*WAVELENGTH*sizeof(double),cudaMemcpyHostToDevice)
197
198     dim3 block3d(16,16,4);
199     dim3 grid3d(KEYBYTES/16,KEYS/16,WAVELENGTH/4);
200     //find wave stats
201     wavestatkernel<<<grid3d,block3d>>>(dev_wavedata,dev_wavestat,dev_wavestat2,dev_hammingArray);
202     checkCudaError(cudaGetLastError());
203
204     //deploy double
205     maxCorelationkernel<<<grid,block>>>(dev_corelation,dev_wavestat,dev_wavestat2,dev_hammingstat);
206     checkCudaError(cudaGetLastError());
207
208
```

C source file | length : 9739 lines : 364 | Ln : 194 Col : 22 Sel : 0 | 0 | Dos\Windows | UTF-8 w/o BOM | INS

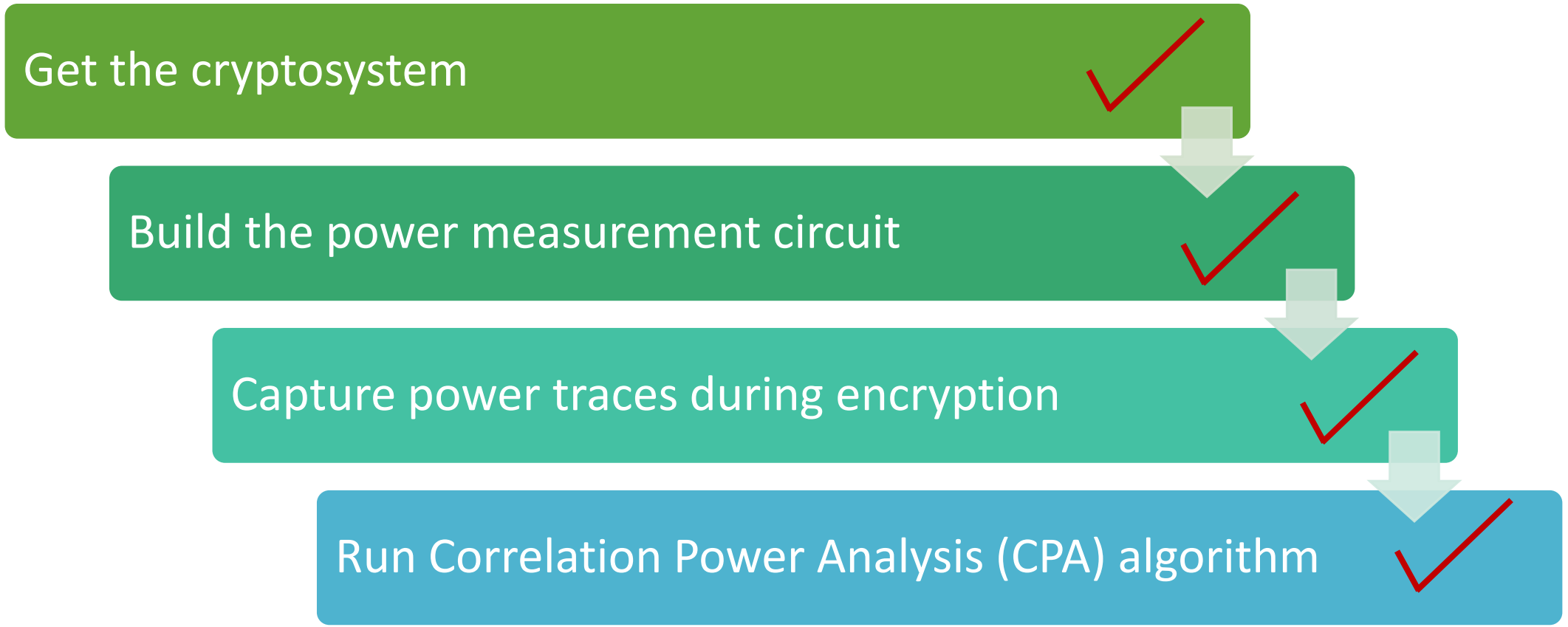
NVIDIA

Analysis and the results



		Key byte number															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Best match	Key value	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10
	Corelation	0.521137	0.448907	0.520267	0.551591	0.508015	0.704521	0.445823	0.423540	0.444697	0.445908	0.661739	0.426426	0.444317	0.430450	0.437648	0.628977
2nd match	Key value	6C	F4	B2	AF	5C	52	17	1A	4E	07	58	6F	3C	9C	0E	96
	Corelation	0.400599	0.380852	0.393687	0.373278	0.387632	0.366003	0.365258	0.365488	0.384889	0.377206	0.361254	0.422964	0.368108	0.360678	0.396348	0.376267
3rd match	Key value	2A	7D	FE	C1	39	B8	DD	88	29	8E	36	61	D2	E8	E8	F7
	Corelation	0.362978	0.373437	0.371296	0.366130	0.378995	0.362108	0.365145	0.360891	0.384421	0.363818	0.353900	0.387495	0.360780	0.357981	0.391313	0.372641
4th match	Key value	94	73	E7	4C	DC	F3	36	F2	DE	51	E2	36	0B	01	AB	B5
	Corelation	0.362593	0.370685	0.368100	0.363095	0.371864	0.361211	0.360876	0.360824	0.378430	0.360141	0.352414	0.368855	0.353642	0.356170	0.370210	0.369261
5th match	Key value	A2	60	F6	C8	B3	E1	D0	B4	DB	17	2B	26	C8	9F	A8	DA
	Corelation	0.360821	0.361709	0.363739	0.358498	0.370971	0.357444	0.354721	0.358538	0.366370	0.357549	0.349865	0.363613	0.347891	0.354794	0.363844	0.367125

Basic Steps of Power Analysis Attack



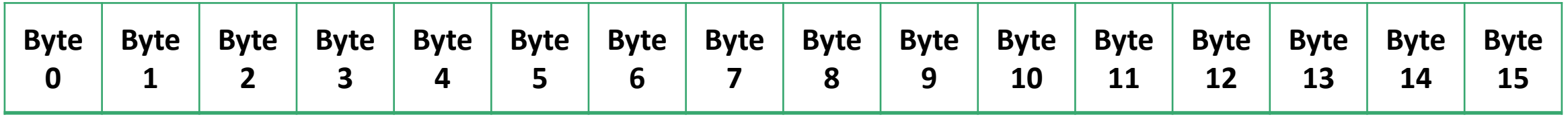
Theory behind the attack ….

Computational complexity

- Attack each byte separately

Key in AES

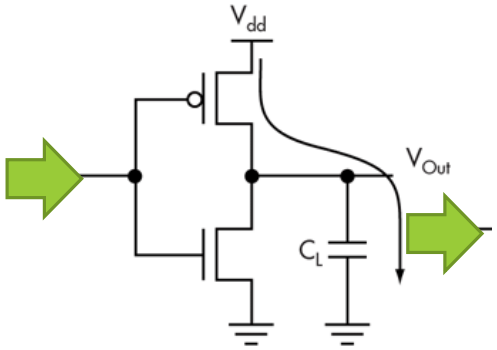
128 bits



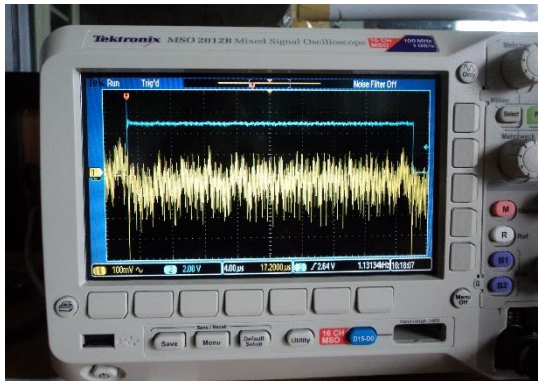
- Consists of 16 bytes (let's call byte position)
- each byte can take values from 0 to 255 (let’s call subkey)
- There are 256x16 combinations

Technical approach

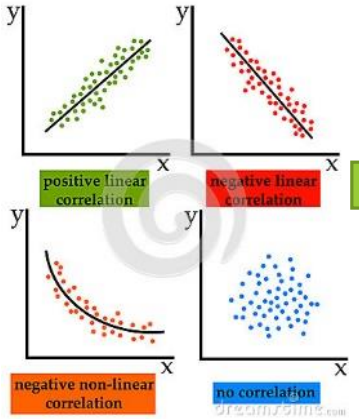
Secret key



Dynamic power consumption of CMOS circuits



Measured power traces



Pearson correlation

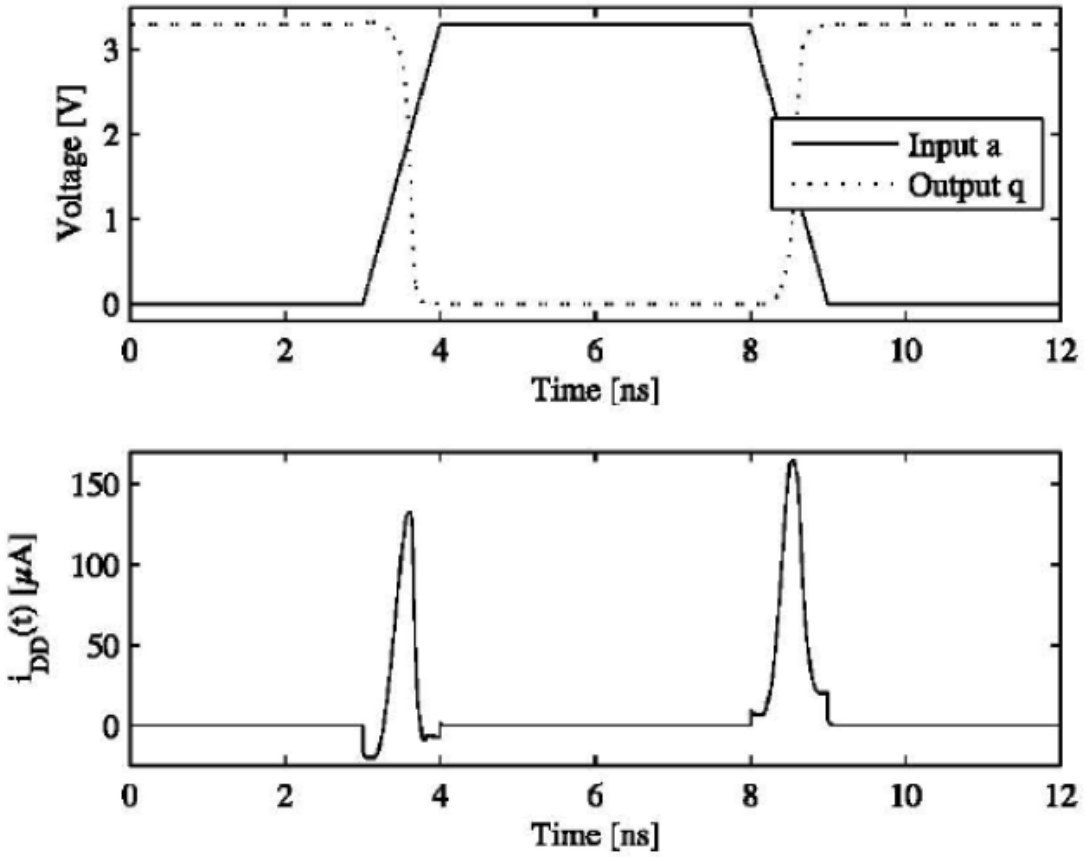
Secret key

key guesses

Power model
Eg : Hamming weight

$$\hat{\rho} = \frac{N\sum_{i=0}^{N} W_{i,j}H_i - \sum_{i=0}^{N} W_{i,j} \sum_{i=0}^{N} H_i}{\sqrt{N\sum_{i=0}^{N} W_{i,j}^2 - \left(\sum_{i=0}^{N} W_{i,j}\right)^2}\sqrt{N\sum_{i=0}^{N} H_i^2 - \left(\sum_{i=0}^{N} H_i\right)^2}}$$

Power consumption of CMOS circuits



Power consumption of a NOT gate

Power model

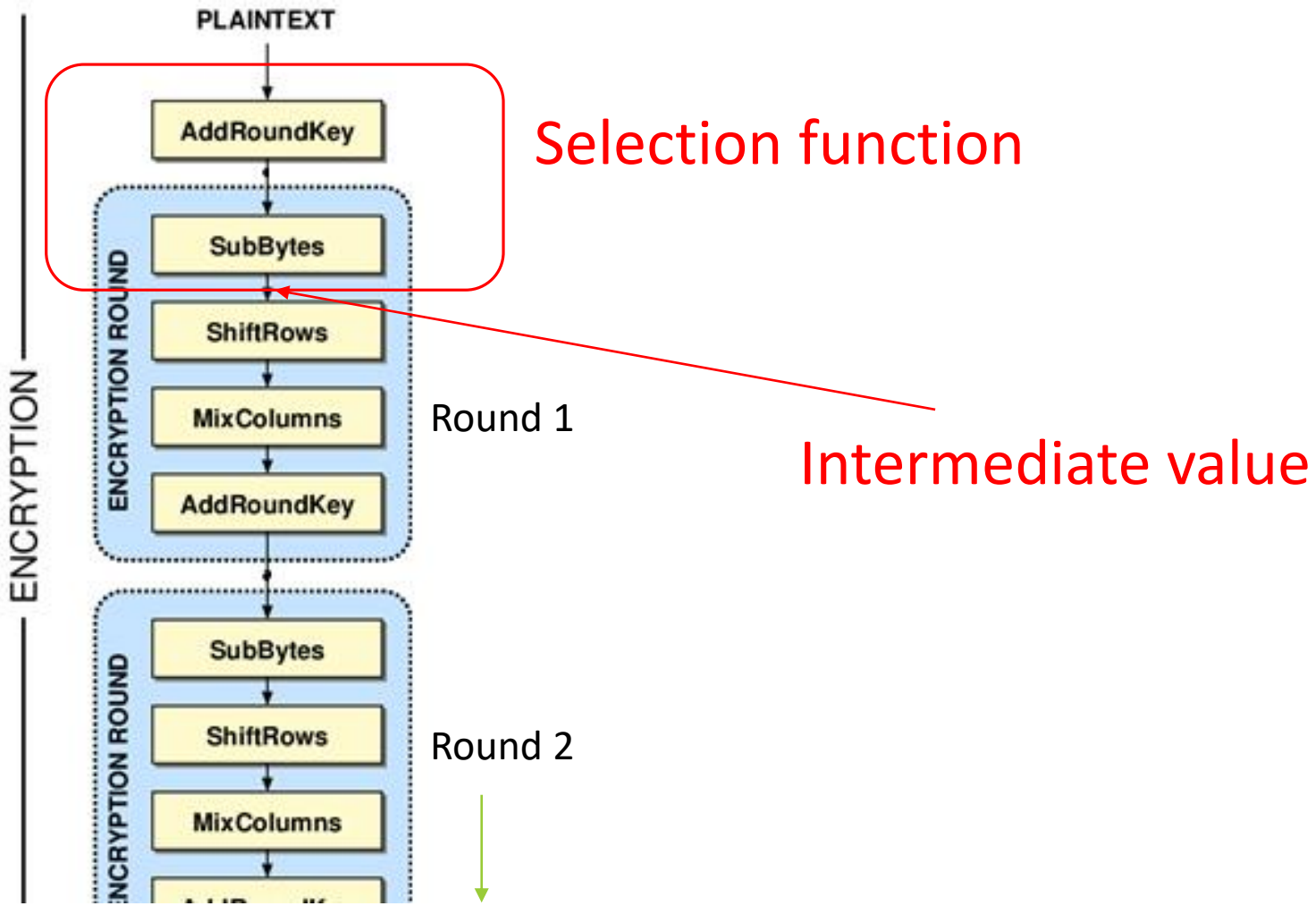
- If v0 is the initial value and v1 the next value in a register or memory bus

Hamming Distance = Sum of set bits (v0 XOR v1)

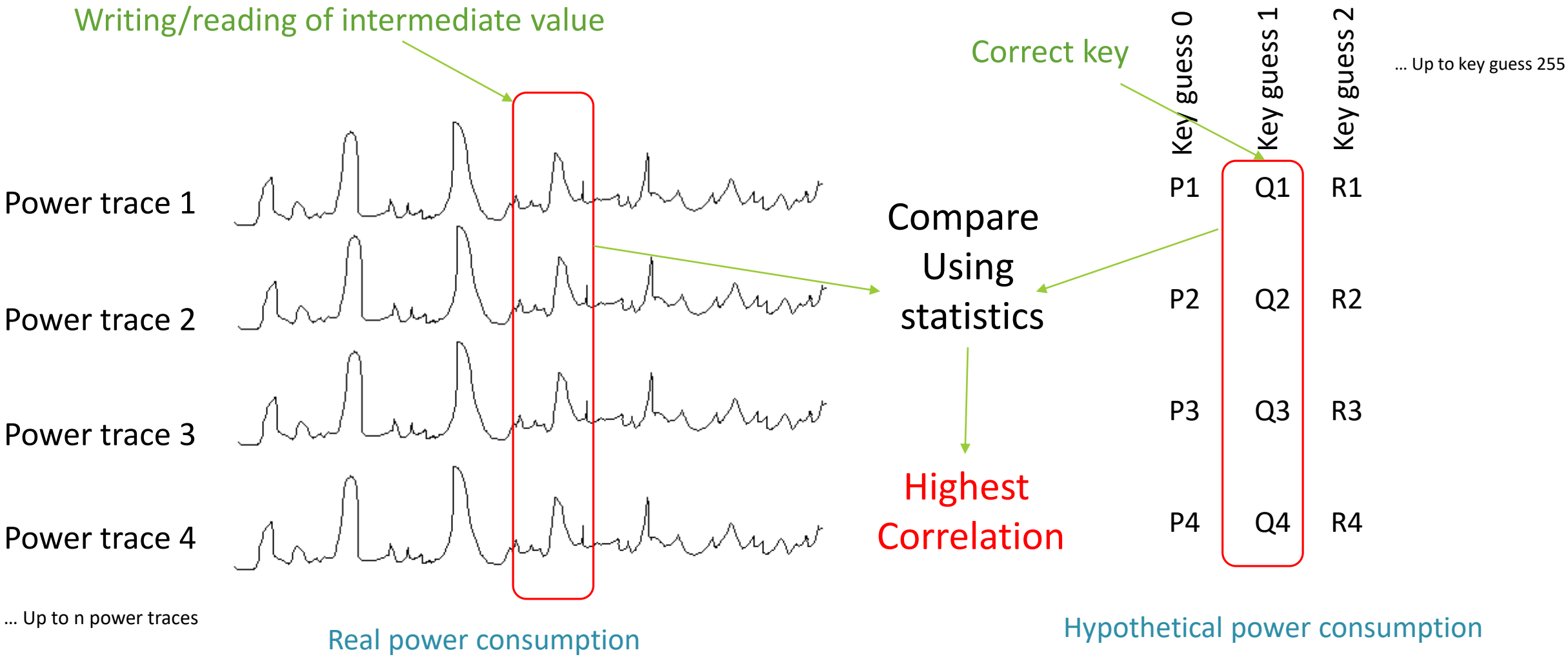
- If a pre-cleared bus, v0=0

Hamming Weight = Sum of set bits (v1)

Selection function for AES



Statistical comparison in CPA

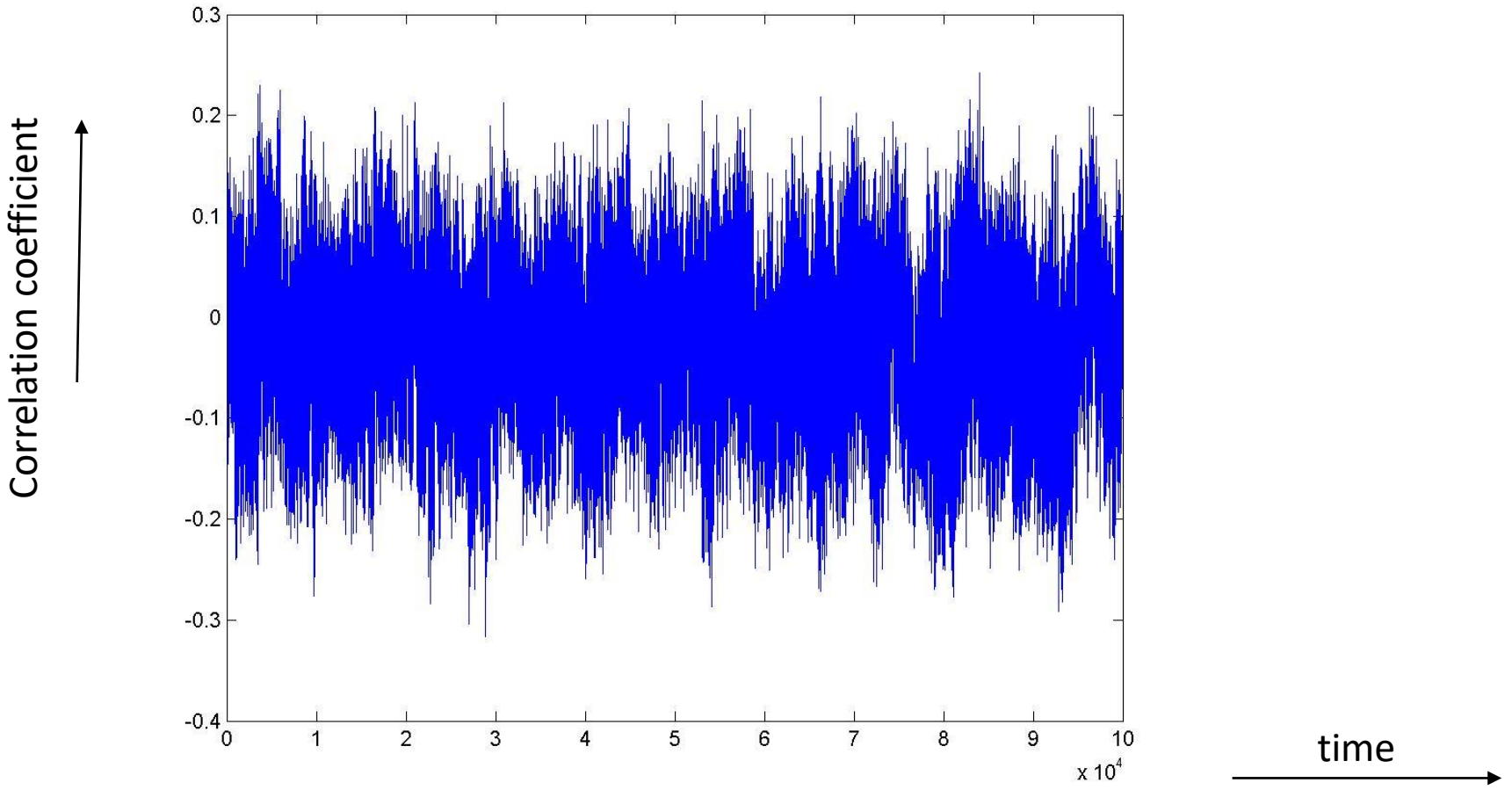


Statistical analysis

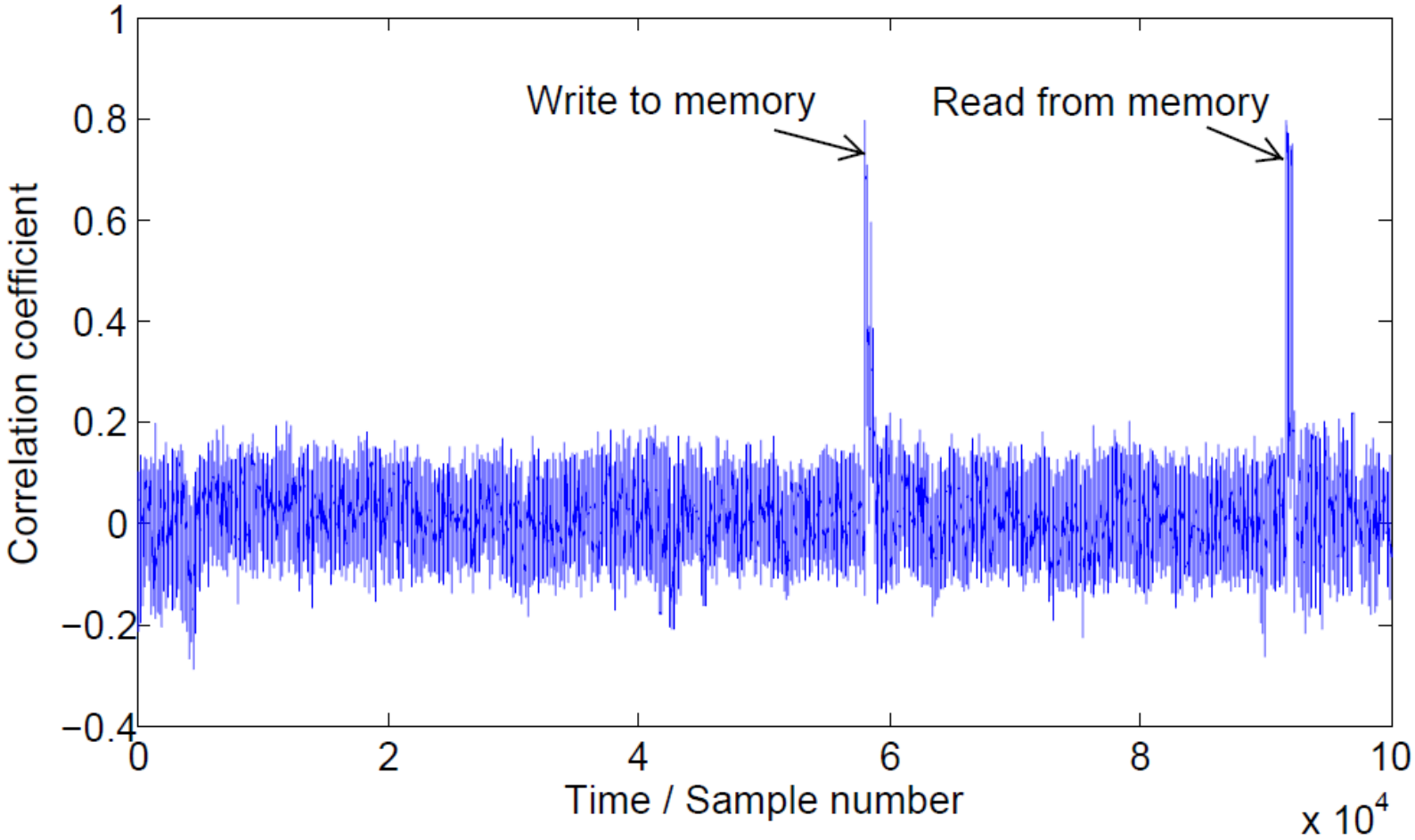
We use Pearson correlation

$$\hat{\rho} = \frac{N \sum_{i=0}^{N} W_{i,j} H_i - \sum_{i=0}^{N} W_{i,j} \sum_{i=0}^{N} H_i}{\sqrt{N \sum_{i=0}^{N} W_{i,j}^2 - \left(\sum_{i=0}^{N} W_{i,j}\right)^2} \sqrt{N \sum_{i=0}^{N} H_i^2 - \left(\sum_{i=0}^{N} H_i\right)^2}}$$

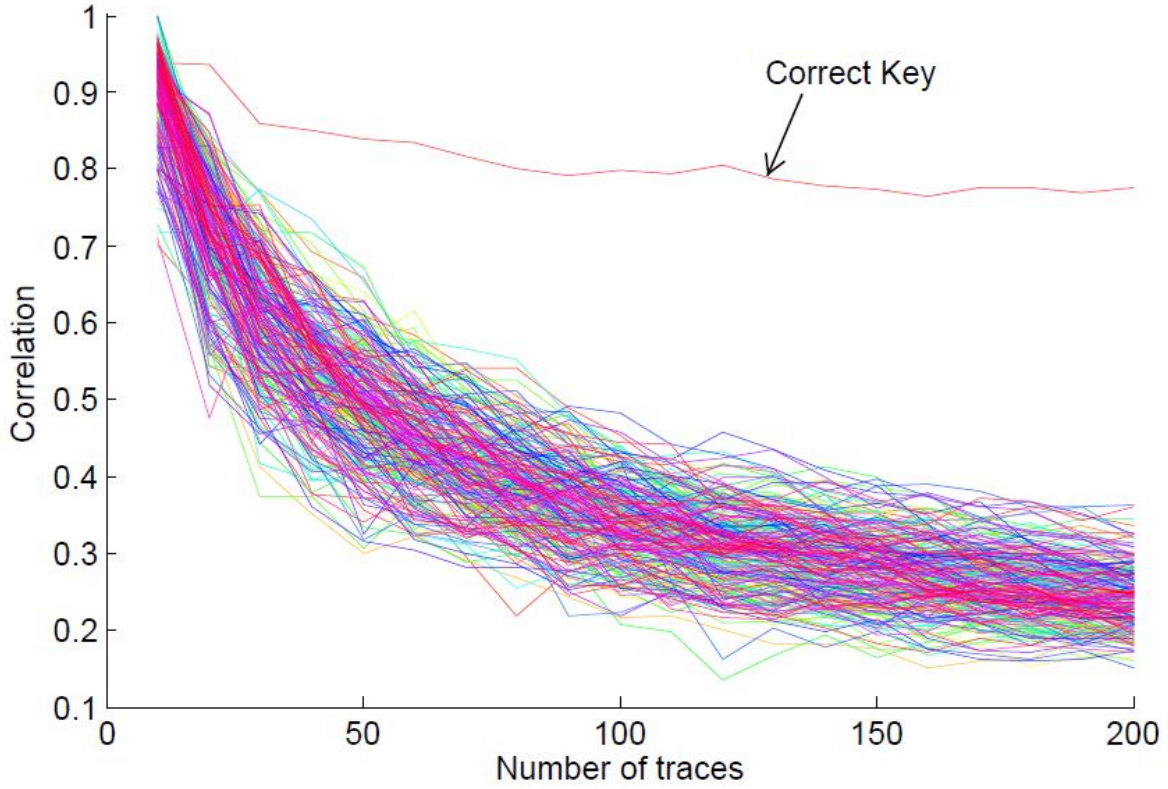
Correlation vs time for a wrong key guess



Correlation vs time for the correct key guess



Number of traces necessary



For more info

Paper :

Hasindu Gamaarachchi, Harsha Ganegoda and Roshan Ragel, "The A to Z of Building a Testbed for Power Analysis Attacks", 10th IEEE International Conference on Industrial and Information Systems 2015 (ICIIS)

Source codes :

https://github.com/hasindu2008/PowerAnalysis

More Info

Download slides from :

https://tesla.ce.pdn.ac.lk/iciafs/cpa.pdf

Online power analysis program :

https://tesla.ce.pdn.ac.lk/cuda/cpa.php

Questions?

Contact :
hasindu2008@gmail.com