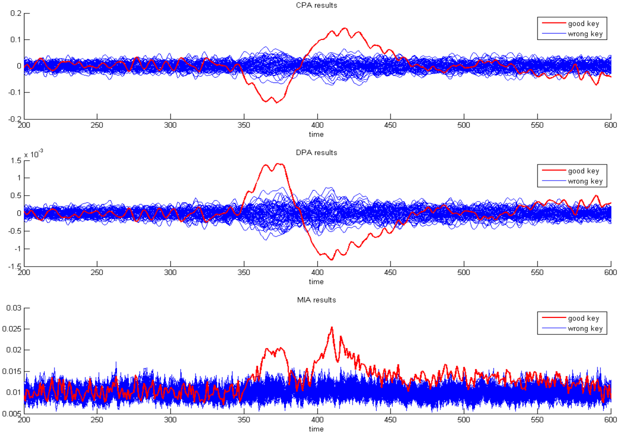
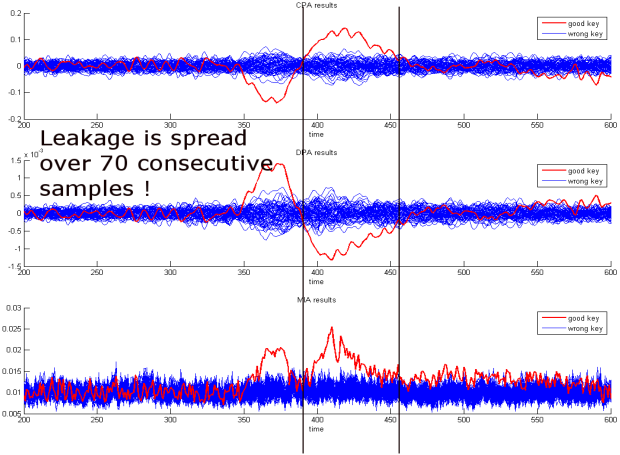
Magnitude Squared Coherence based SCA

S. Tiran, A. Dehbaoui, P.Maurine

CryptArchi 2012

June 20, 2012


CPA results
good key
wrong key
0.2
0.1
0
-0.1
-0.2
200
250
300
350
400
450
500
550
600
time
DPA results
x 10^-3
1.5
1
0.5
0
-0.5
-1
-1.5
MIA results
0.03
0.025
0.02
0.015
0.01
0.005


CPA results
good key
wrong key
0.2
0.1
0
-0.1
-0.2
200
250
300
350
400
450
500
550
600
time
Leakage is spread
over 70 consecutive
samples !
DPA results
x 10^-3
1.5
1
0.5
0
-0.5
-1
-1.5
MIA results
0.03
0.025
0.02
0.015
0.01
0.005

- Is working with one sample at a time optimal?

$\Rightarrow$ Maybe not?

- Are there tools to work with several consecutive samples?

$\Rightarrow$ Magnitude Squared Coherence

What is MSC?

Magnitude Squared Coherence :

1. is a signal processing tool that returns real values between 0 and 1 to indicate how well two time domain signals *x(t)* and *y(t)* match one with the other.
2. works in the frequency domain.

Magnitude Squared Coherence

$$MSC_{x,y}(f) = \frac{|P_{xy}(f)|^2}{P_{xx}(f) * P_{yy}(f)} \quad (1)$$

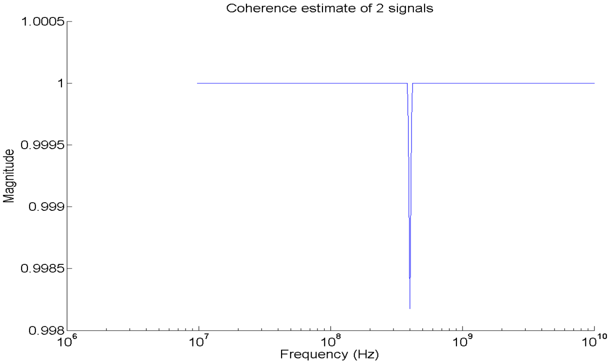
With :

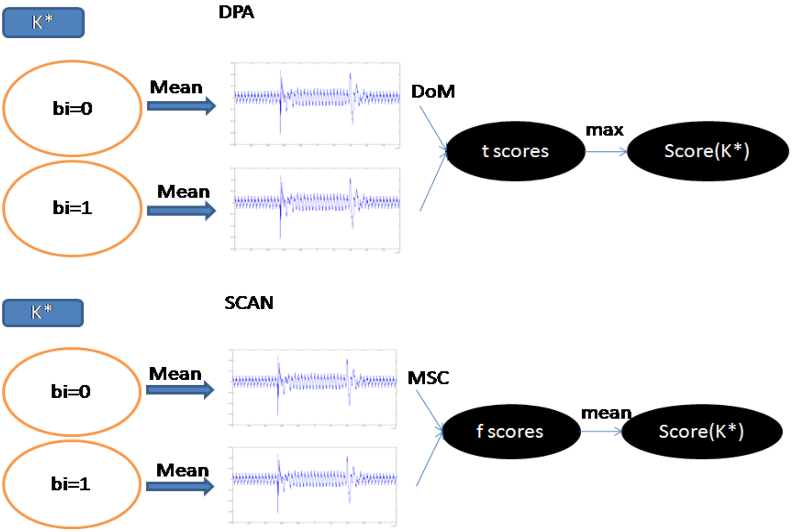
- P_{xy} the cross-spectral density between x and y
- P_{xx} and P_{yy} the autospectral density of x and y

Illustration of the use of MSC

Result of the coherence between two signals sampled at 20GHz.

$$s_1(t) = 1.sin(2\pi.200e^6.t)$$
$$s_2(t) = 1.sin(2\pi.200e^6.t) + 0.0001.sin(2\pi.400e^6.t)$$




K*
DPA
bi=0
Mean
DoM
bi=1
Mean
t scores
max
Score(K*)
K*
SCAN
bi=0
Mean
MSC
bi=1
Mean
f scores
mean
Score(K*)

HD model

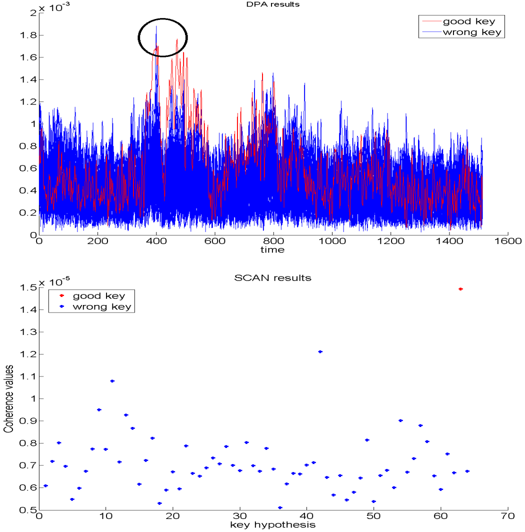
Attacks of EM curves of a DES implementation on a FPGA

	Success Rate	10%	20%	40%	60%	80%	100%
time domain	CPA	775	1075	1525	2150	4475	5000
	DPA	850	1175	1750	2800	4250	4975
	MIA	1650	1850	2450	2900	3300	4150
	MIA mb	950	1150	1250	1600	1750	2100
frequency domain	CPFA	1110	1205	1410	1630	2025	3150
	SCAN	260	320	430	660	910	1725

Table 1 : Number of processed traces vs Success Rate (HD model)

- frequency domain analyses > time domain analyses
- SCAN requires less than 2k traces

Results of sbox 3 at 1000 curves, HD model



Working with several samples at a time filters ghost peaks.

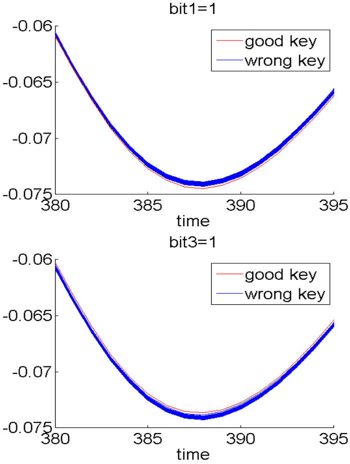
HW model

	Success Rate	10%	20%	40%	60%	80%	100%
time domain	CPA	fail	fail	fail	fail	fail	fail
	DPA	fail	fail	fail	fail	fail	fail
	MIA	fail	fail	fail	fail	fail	fail
	MIA mb	3550	3700	3900	4350	4550	4900
frequency domain	CPFA	fail	fail	fail	fail	fail	fail
	SCAN	1510	1800	2270	2690	3220	4600

Table 2 : Number of processed traces vs Success Rate (HW model)

⇒SCAN and MIA mb are the only one to recover the key with only 5000 curves

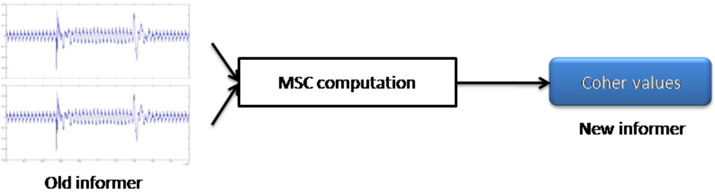
Results of sbox 3 at 5000 curves, HW model



- Did we use optimally MSC?

$\Rightarrow$ Surely not.

New approach



$\Rightarrow \frac{n-1}{2}$ times as much informers as in a classical attack.

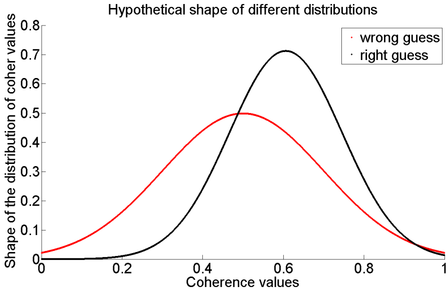
1. 500 messages $\rightarrow$ 124750 informers
2. 1000 messages $\rightarrow$ 499500 informers

Working with pair of messages :

$$b_i(m_p) \rightarrow \Delta b_i = |b_i(m_p) - b_i(m_q)|$$

New goal $\rightarrow$ analyse coher distributions to retrieve the key

Mean and Variance analyses



$$\Delta b_i = 0 \rightarrow b_i(m_1) = b_i(m_2)$$

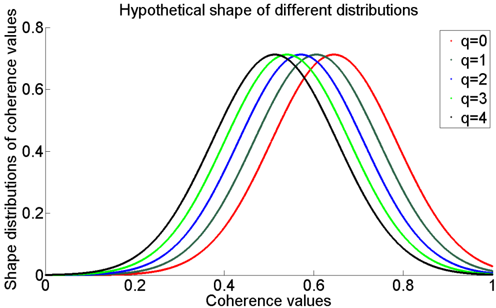
Mean Analysis Formula

$$\max_{k*\in K}\left\{\sum_i |E(C_{k*}|\Delta b_i = 1) - E(C_{k*}|\Delta b_i = 0)|\right\} \quad (2)$$

Variance Analysis Formula

$$\min_{k*\in K}\left\{\sum_i |V(C_{k*}|\Delta b_i = 0)|\right\} \quad (3)$$

Correlation analysis



Let us assum that the expectations $E(C_{k*} | \sum_i \Delta b_i = q)$ are decreasing with the increasing value of q.

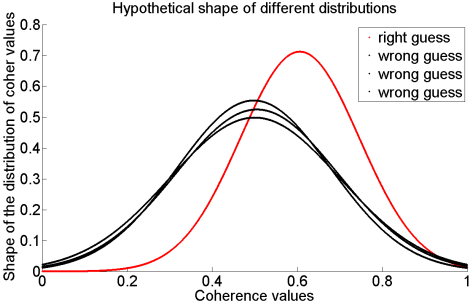
Pearson Correlation :

- returns a value between -1 and 1
- estimates the linear dependence between two variables

Correlation Analysis Formula

$$\max_{k* \in K} \{Correlation(Coher, q)\} \quad (4)$$

KS test based analysis

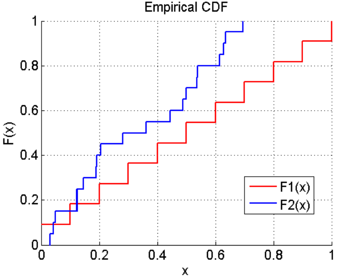


Assuming :

1. that the distribution associated to the secret key is unique and different from that of wrong key guesses
2. and that the distributions of all wrong guesses are similar in shape

Kolmogorov-Smirnov test

The KS test is a non parametric test to compare the distributions of two samples.



CDF formula

$$F_{1,n}(x) = \frac{1}{n}\sum_{i=1}^{n} I\{x_i \leq x\} \qquad (5)$$

KS test formula

$$\sqrt{\frac{nm}{n+m}}\sup_x |F_{1,n}(x) - F_{2,m}(x)| \qquad (6)$$

KS test based analysis

$$\max_{k*\in K}\left\{\sum_i \sum_{k\neq k*} KStest(C_{k*}|\Delta b_i = 0, C_k|\Delta b_i = 0)\right\} \qquad (7)$$

It aims at identifying the key guess associated to the CDF differing the most from all the others.

HD model

	Success Rate	10%	20%	40%	60%	80%	100%	
time domain	CPA	775	1075	1525	2150	4475	5000	*7
	DPA	850	1175	1750	2800	4250	4975	*7
	MIA	1650	1850	2450	2900	3300	4150	*6
	MIA mb	950	1150	1250	1600	1750	2100	*3
frequency domain	CPFA	1110	1205	1410	1630	2025	3150	*5
	SCAN	260	320	430	660	910	1725	*2.5
	mean+MSC	230	260	310	440	495	650	*1
	var+MSC	440	450	535	670	780	1135	*2
	corr+MSC	320	410	480	532	660	730	*1
	KS+MSC	350	370	440	455	540	690	*1

Table 3 : Number of processed traces vs Success Rate (HD model)

HW model

	Success Rate	10%	20%	40%	60%	80%	100%
time domain	CPA	fail	fail	fail	fail	fail	fail
	DPA	fail	fail	fail	fail	fail	fail
	MIA	fail	fail	fail	fail	fail	fail
	MIA mb	3550	3700	3900	4350	4550	4900
frequency domain	CPFA	fail	fail	fail	fail	fail	fail
	SCAN	1510	1800	2270	2690	3220	4600
	mean+MSC	2430	2510	2685	3460	3980	4855
	var+MSC	4250	4400	fail	fail	fail	fail
	corr+MSC	2375	2515	2705	3495	3990	4810
	KS+MSC	2120	2580	3310	3710	4070	4495

Table 4 : Number of processed traces vs Success Rate (HW model)

CPU times

Number of traces :	500	1000
CPA	13s	26s
DPA	15s	30s
MIA	4m	8m
MIA mb	13m	25m
CPFA	13s	27s
SCAN	15s	31s
MSC based analyses	1h5m	4h20m

Table 5 : CPU times of the attacks with a step of 10 curves

- single sample attacks are not optimal
- in some cases frequency analyses are better, and particularly MSC based analyses
- working with pair of curves $\rightarrow$ in some cases requires less curves
- working with pair of curves is time consuming