A method for resynchronizing a random clock on smart cards ...

Didier Moyart - Régis Bevan

Oberthur Card Systems

A short history of DPA attacks

- First published SPA DPA attack by Paul Kocher in 1998
- Silicon manufacturers introduce hardware countermeasures for all algorithms
- We focus on random clock

Oberthur Card Systems

Plan

Introduce a way to reconstruct power curves

- How does a DPA attack work
- Manufacturer’s random clock
- A new method to reconstruct the signal

Oberthur Card Systems

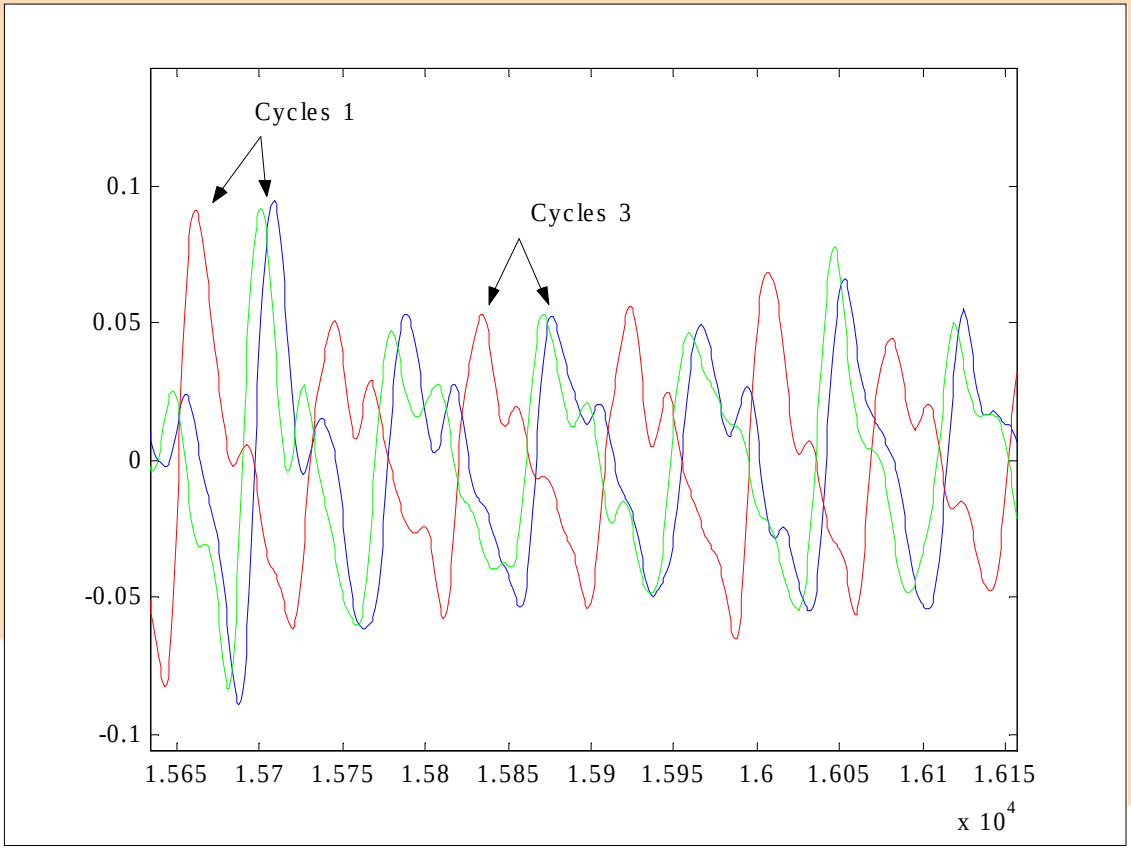
How a DPA attack works

- Principle : comparison of current consumption traces at the same instruction in the algorithm
- Traces are superposed
- The necessary information is not diluted along the time scale : Easy to realise an attack

Oberthur Card Systems

Manufacturer's random clock(1)

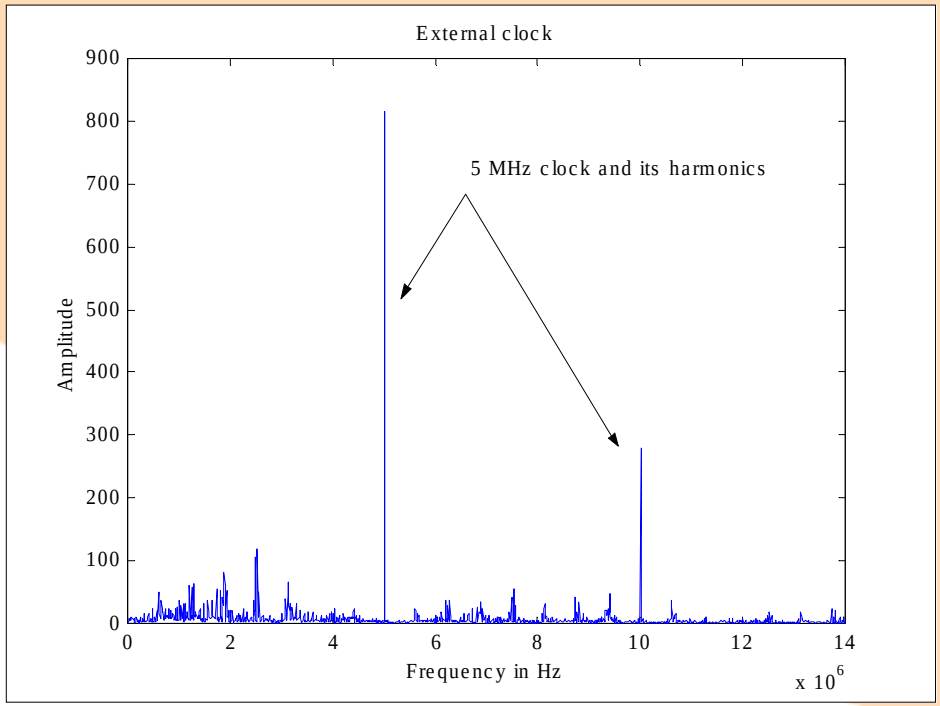
Time domain representation

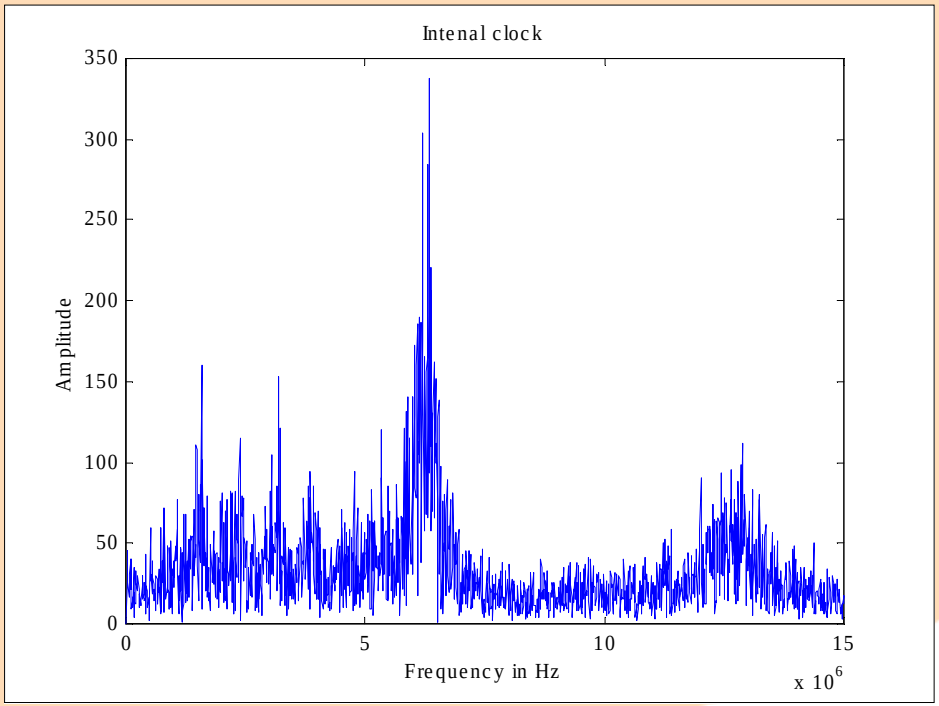


Oberthur Card Systems

Manufacturer's random clock(2)

FFT of "normal" and random clock





Oberthur Card Systems

A new method to reconstruct the signal (1)

The protocol is the following :

1) Digital filtering of the traces
2) Find the number of cycles of the traces
3) Rebuild the curves where the same number of minima has been found with two points per cycle
4) Conduct a DPA attack

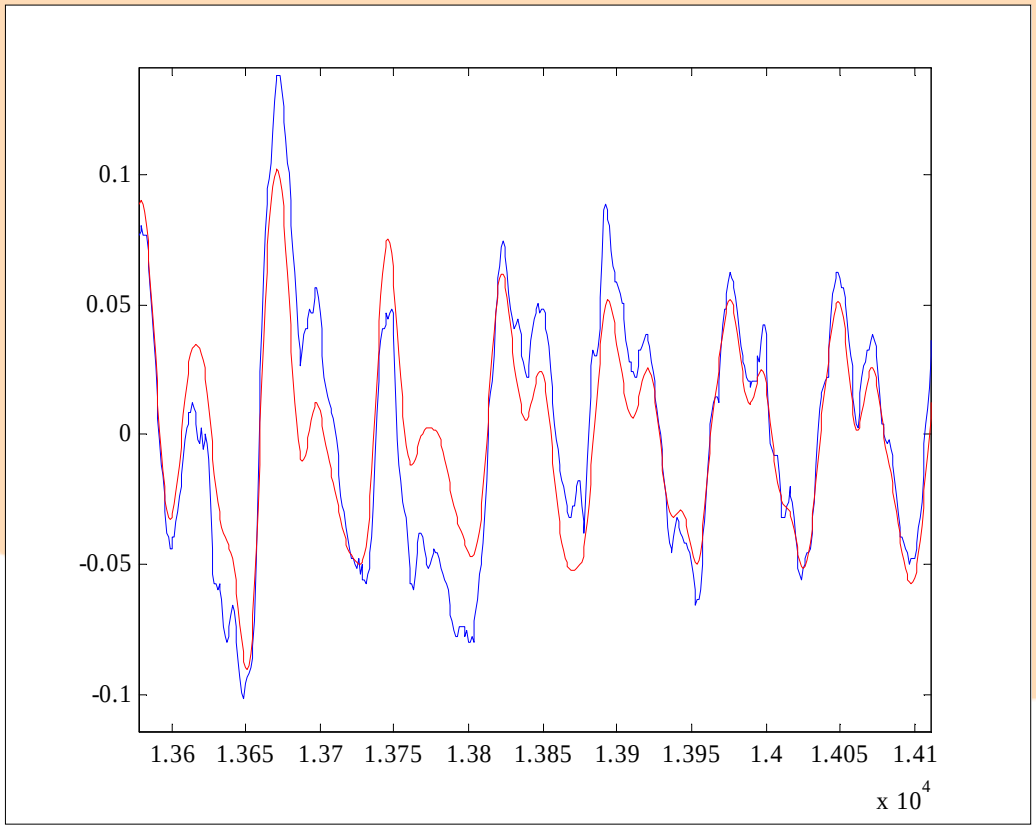
Oberthur Card Systems

A new method to reconstruct the signal (2)

1) Digital filtering

In blue : original signal

In red : filtered signal



Oberthur Card Systems

A new method to reconstruct the signal (3)

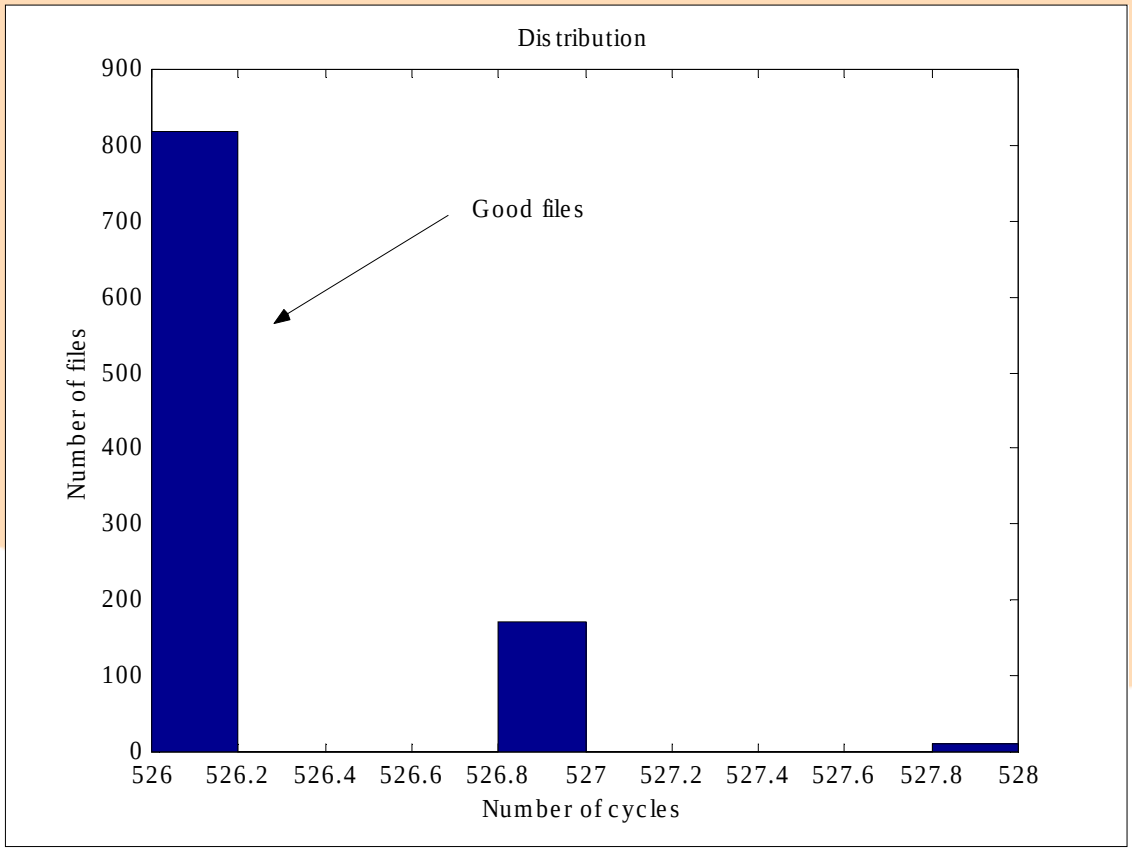
2) Find the number of cycles in the traces

- Repeat for all traces
  - Repeat for all instructions
    - Find a minima
    - Look for the following minima in a given range

Oberthur Card Systems

A new method to reconstruct the signal (4)

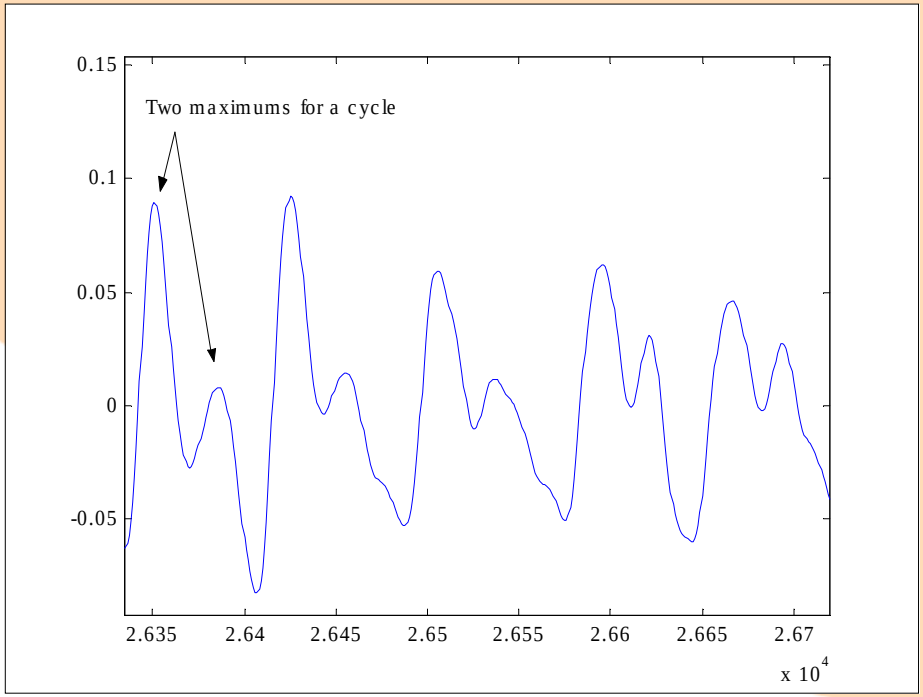
3) Distribution of the number of cycles

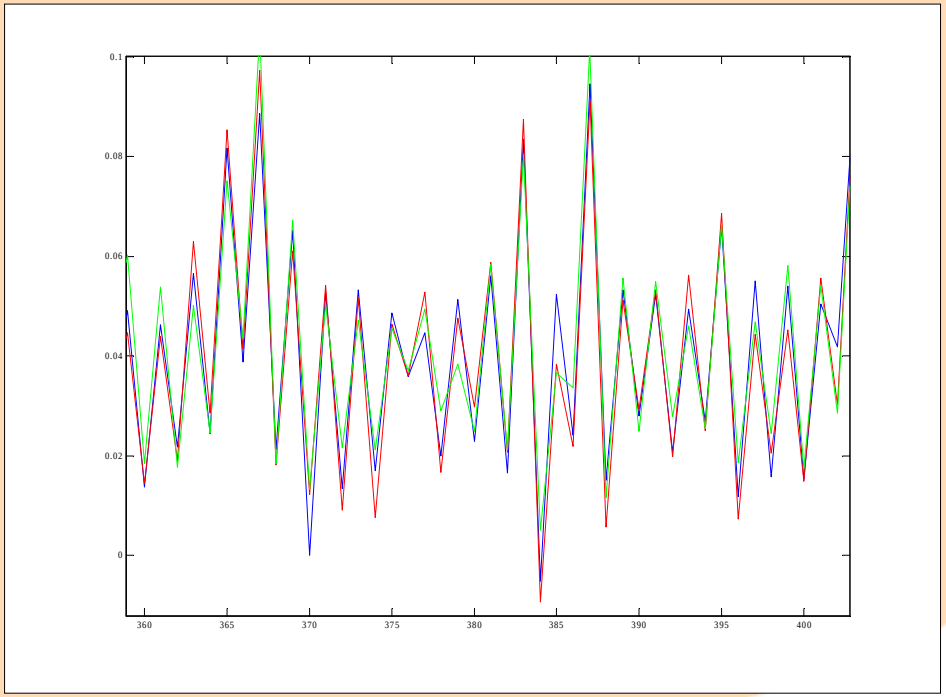


Oberthur Card Systems

A new method to reconstruct the signal (5)

4) Each curve is reconstructed with two points per cycle





Oberthur Card Systems

Results

•Results show the number of messages required to obtain 3 out of 4 selection functions giving the correct sub-key;

	S1	S2	S3	S4
External clock	120	260	120	100
Random clock	1010	> 5000	> 5000	> 5000
Resynchronised clock	90	310	290	490

Oberthur Card Systems

Conclusion (1)

- A method to reconstruct signals from a random clock for the component under test.
- It improves current DPA attacks without processing by a factor 10
- In-depth study to improve these results is ongoing

Oberthur Card Systems

Conclusion (2)

- Random clock countermeasures is good but not sufficient
- Software countermeasures also have to be implemented

Oberthur Card Systems