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
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
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
Manufacturer’s random clock(1)

Time domain representation
Manufacturer’s random clock(2)

FFT of “normal” and random clock

- **External clock**: 5 MHz clock and its harmonics
- **Internal clock**:
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
1) Digital filtering

In blue: original signal
In red: filtered signal
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
A new method to reconstruct the signal (4)

3) Distribution of the number of cycles

![Bar graph showing the distribution of the number of cycles. The x-axis represents the number of cycles, ranging from 526 to 528, and the y-axis represents the number of files. The graph shows a peak at 526.2 cycles, indicating a higher concentration of good files at this cycle count.]
A new method to reconstruct the signal (5)

4) Each curve is reconstructed with two points per cycle
Results

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

<table>
<thead>
<tr>
<th></th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
</tr>
</thead>
<tbody>
<tr>
<td>External clock</td>
<td>120</td>
<td>260</td>
<td>120</td>
<td>100</td>
</tr>
<tr>
<td>Random clock</td>
<td>1010</td>
<td>&gt; 5000</td>
<td>&gt; 5000</td>
<td>&gt; 5000</td>
</tr>
<tr>
<td>Resynchronised clock</td>
<td>90</td>
<td>310</td>
<td>290</td>
<td>490</td>
</tr>
</tbody>
</table>
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
Conclusion (2)

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