Prototyping Secure Triple Track Logic (STTL) robustness against DPA & DEMA on FPGA

V. Lomné – R. Soares - T. Ordas

P. Maurine – L. Torres – M. Robert

calisson
Un projet CIMPACA

ANR
Blanc Icter

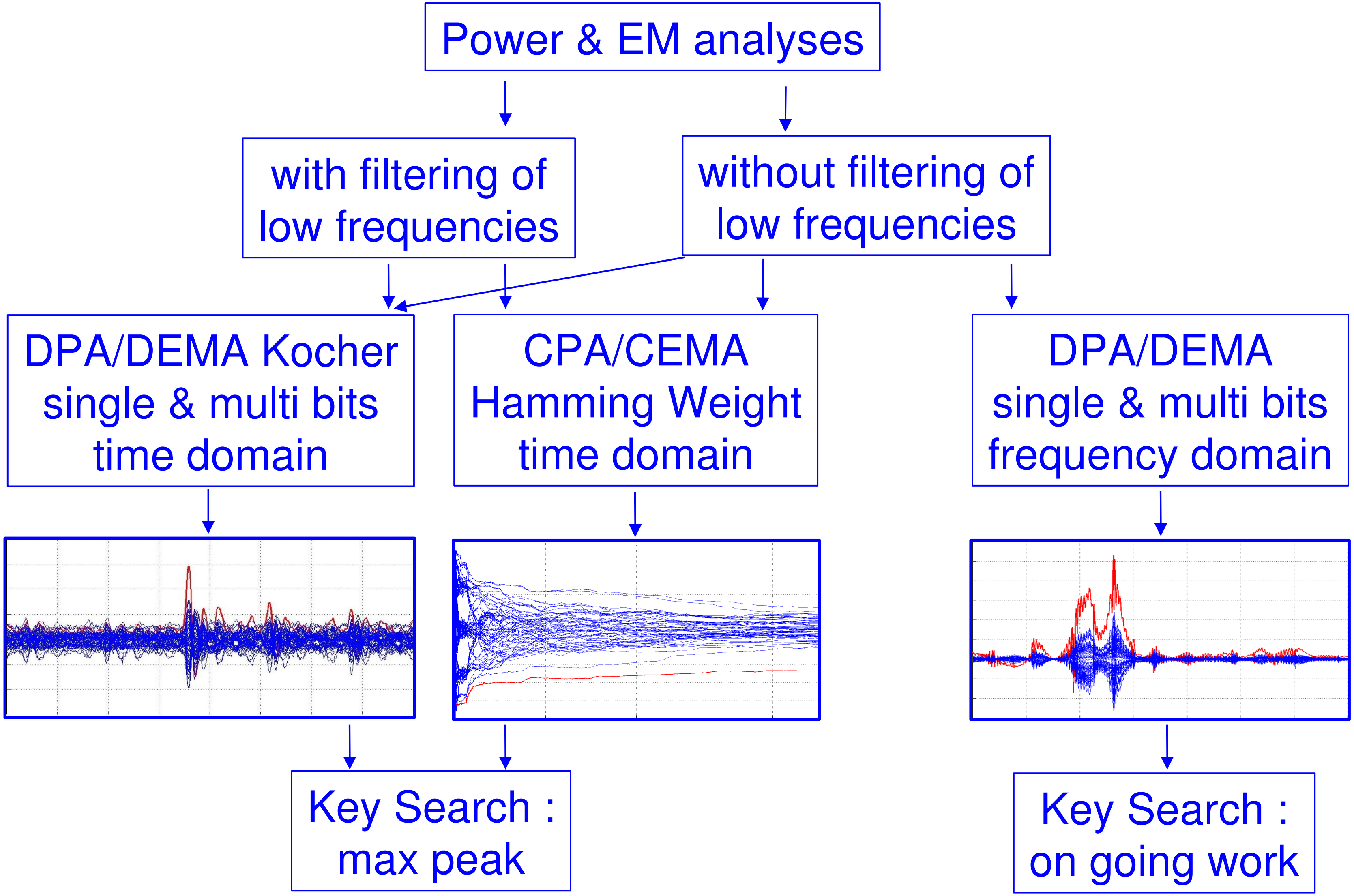
Outline

- 1. Power & EM analysis flow
- 2. Hiding at the cell level
- 3. Secure Triple Track Logic
- 4. Results
- 5. Conclusion

Outline

- 1. Power & EM analysis flow
- 2. Hiding at the cell level
- 3. Secure Triple Track Logic
- 4. Results
- 5. Conclusion

1. Power & EM analysis flow



Power & EM analyses

with filtering of low frequencies

without filtering of low frequencies

DPA/DEMA Kocher single & multi bits time domain

CPA/CEMA Hamming Weight time domain

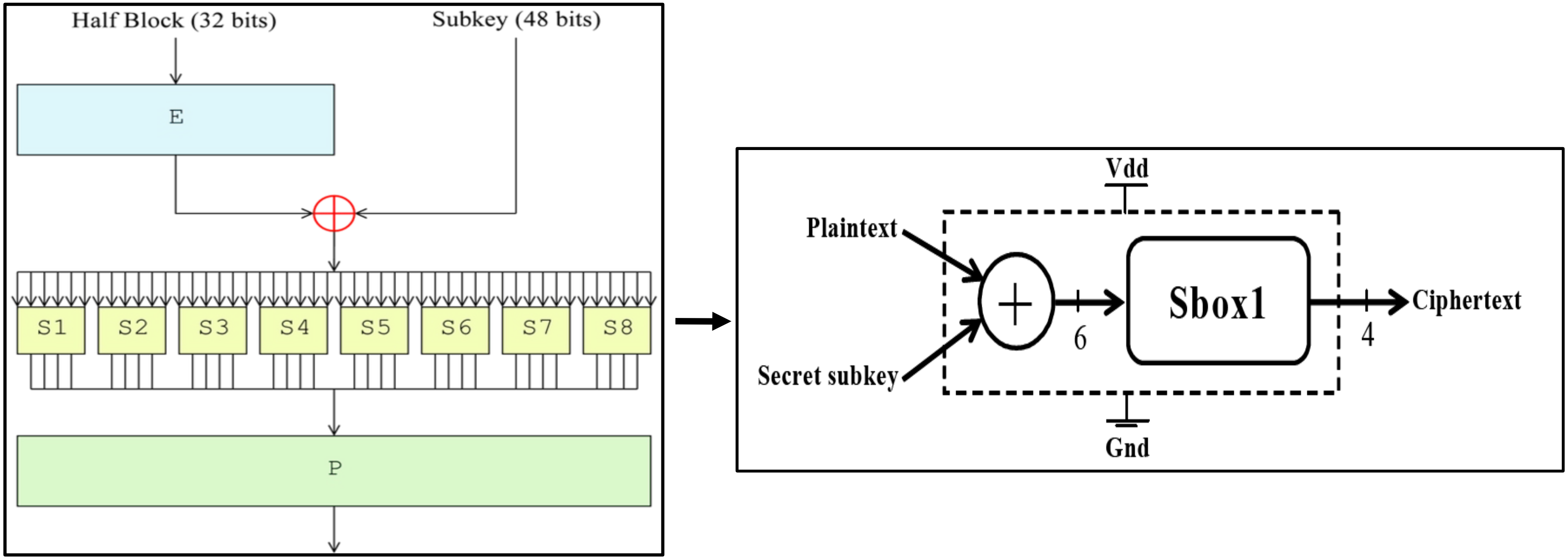
DPA/DEMA single & multi bits frequency domain

Key Search : max peak

Key Search : on going work

1. Power & EM analysis flow

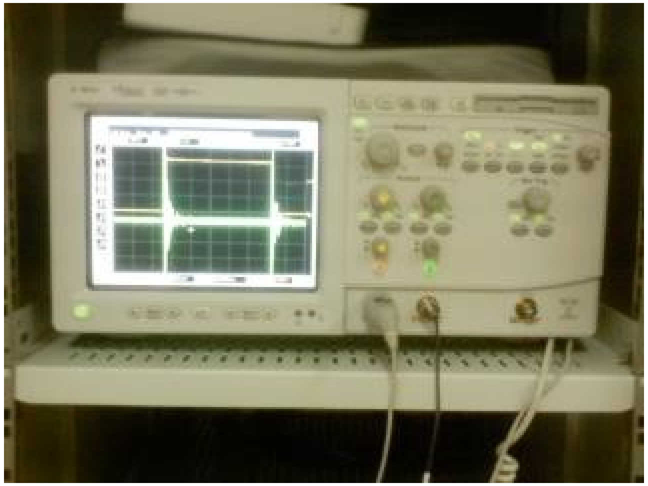
- In order to evaluate security robustness of different logic styles, we implemented a sensitive sub-module of DES cipher function :



- We applied DPA, CPA, DEMA & CEMA (single & multi-bits)
- Inputs : all transitions on 64 possible values averaged 50 times

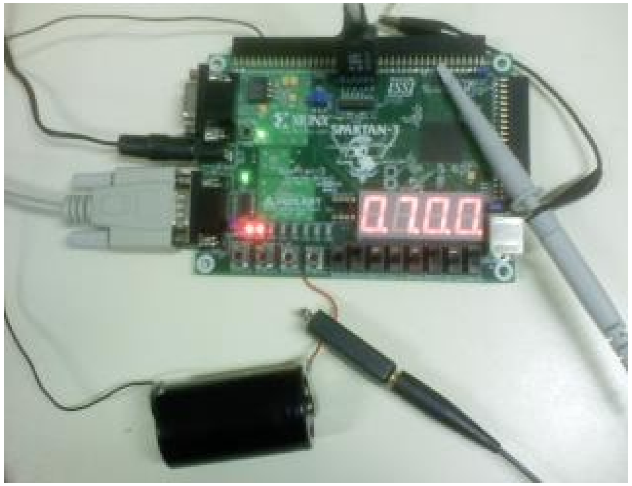
1. Power & EM analysis flow

DPA & DEMA measurement setup

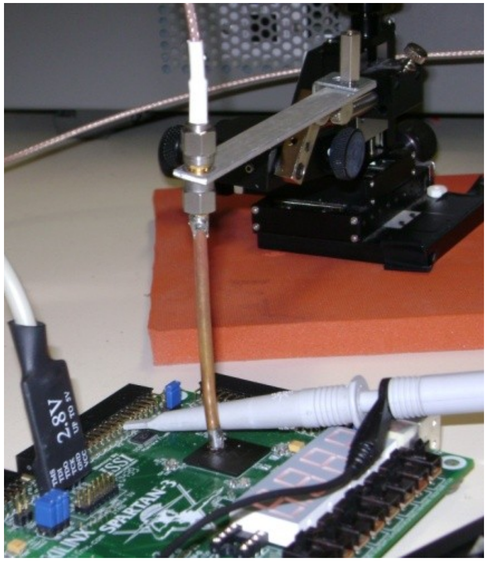


Oscilloscope Agilent Infinium S4830B 600MHz 4GSa/s

Probe Tektronix CT1 5mV/mA



1mm passive magnetic probe



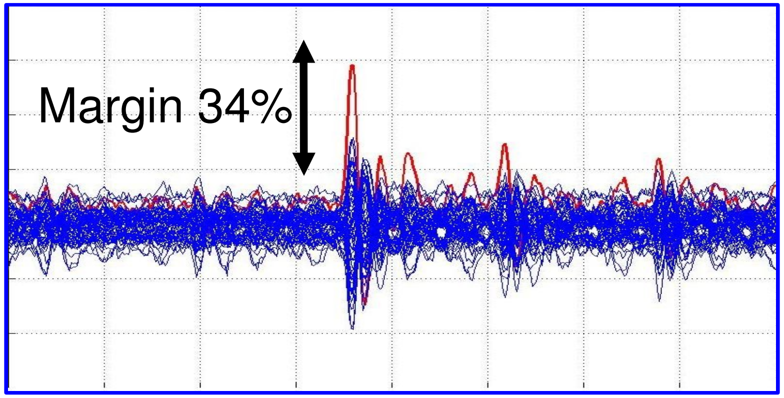
FPGA Xilinx Spartan3 supplied by 1,2V battery

1. Power & EM analysis flow

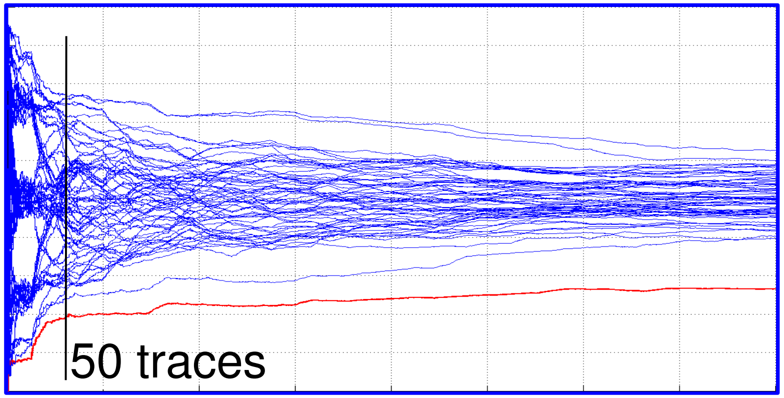
- Implementation of Single Rail logic DES sub-module

Successful DPA & DEMA pictures :

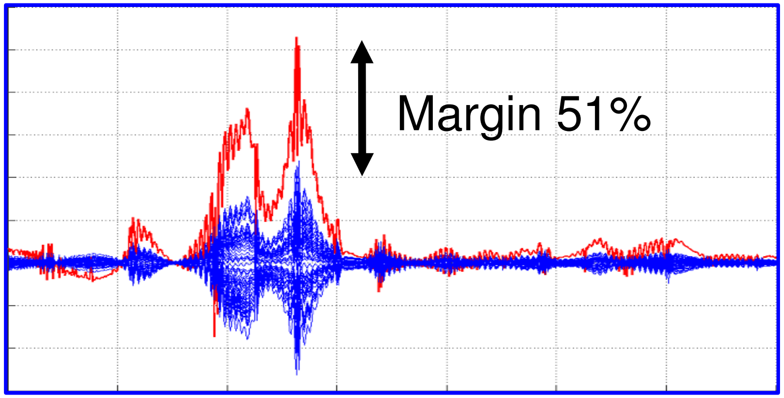
DPA on bit0



CEMA on Hamming Weight



DEMA on bit0
in frequency domain

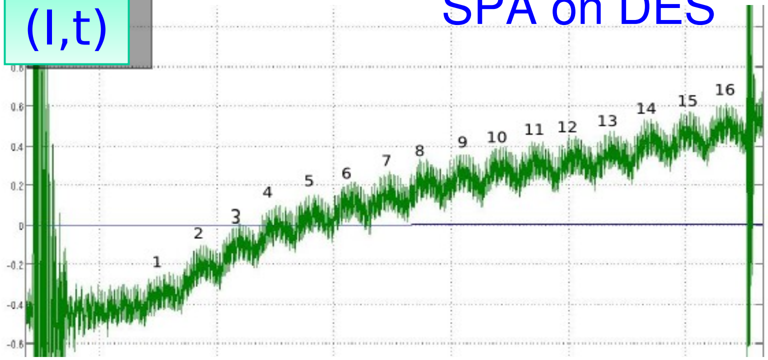


1. Power & EM analysis flow

Near Field Scan in Time Domain

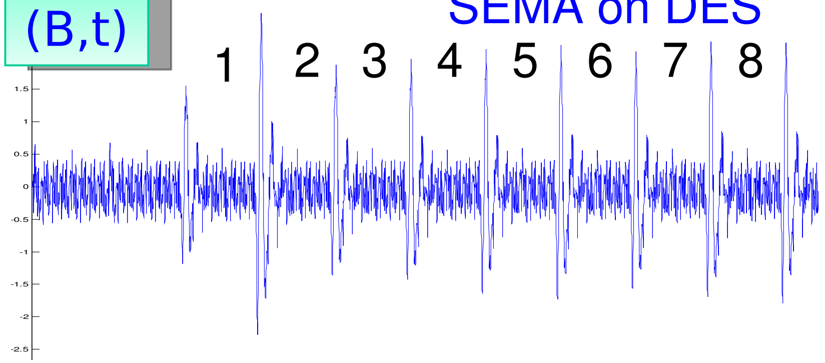
(I,t)

SPA on DES

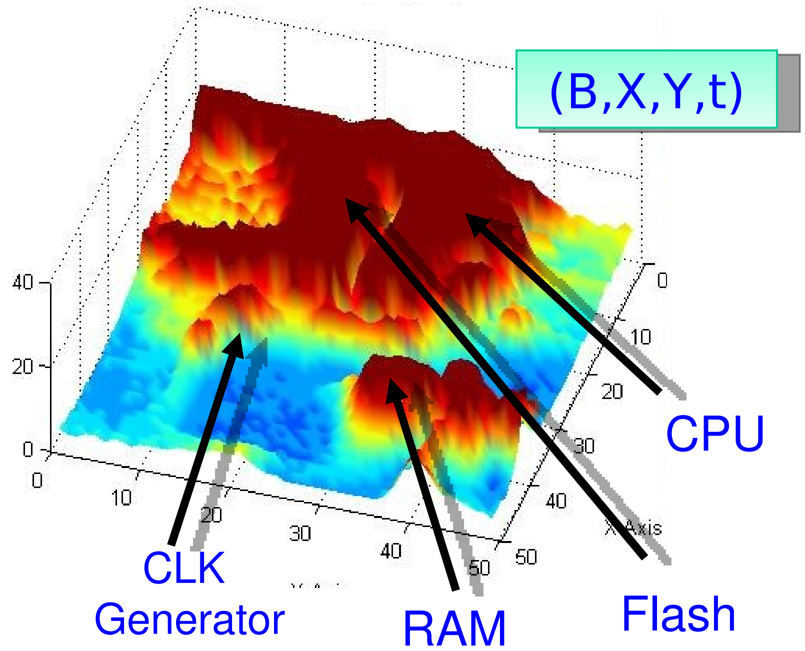


(B,t)

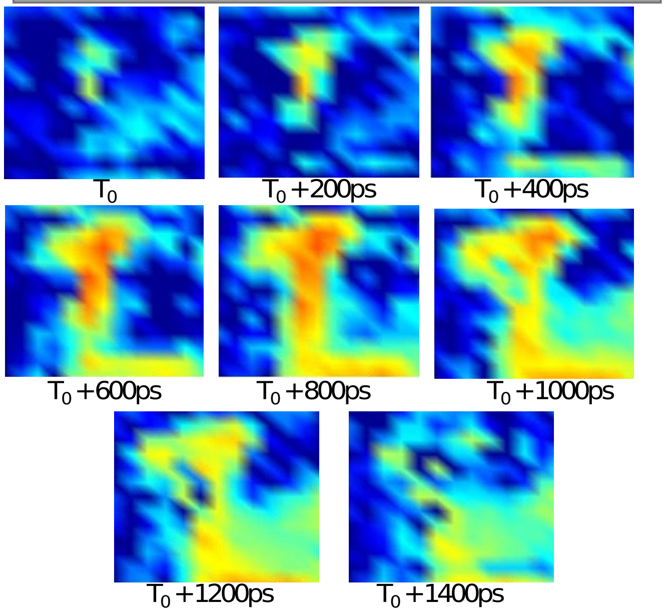
SEMA on DES



(B,X,Y,t)



(B,X,Y,t) + small die area



Outline

- 1. Power & EM analysis flow
- **2. Hiding at the cell level**
- 3. Secure Triple Track Logic
- 4. Results
- 5. Conclusion

2. Hiding at the cell level

DPA countermeasures :

- Masking
  - depends from a cryptographic algorithm
  - breakable by HODPA

- Shuffling time dimension
  - breakable by preprocessing misaligned power traces
  - breakable by leading analysis in the frequency domain

- Hiding amplitude dimension at the cell level
  - requires more area & power
  - examples : Dual Rail, WDDL, STTL

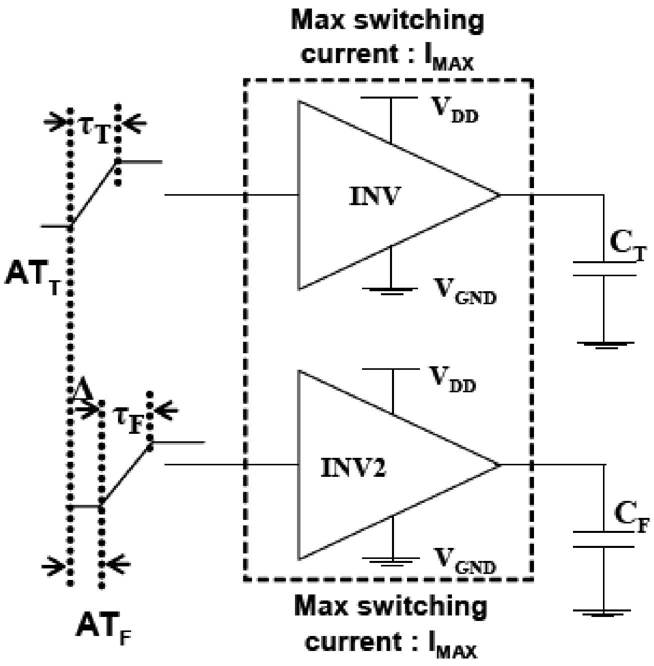
2. Hiding at the cell level

- Dual Rail logic principle : 2 wires for 1 logical signal
  - 1 wire for the logical value
  - 1 wire for the complementary of the logical value

- 2 phases : precharge & evaluation

- Dual Rail logic cells always consume the maximum amount of power

- Loss of Dual Rail benefits if the conditions below are not satisfied :
  - same load capacitance (CT=CF)
  - same transition time
  - gates switch at the same time

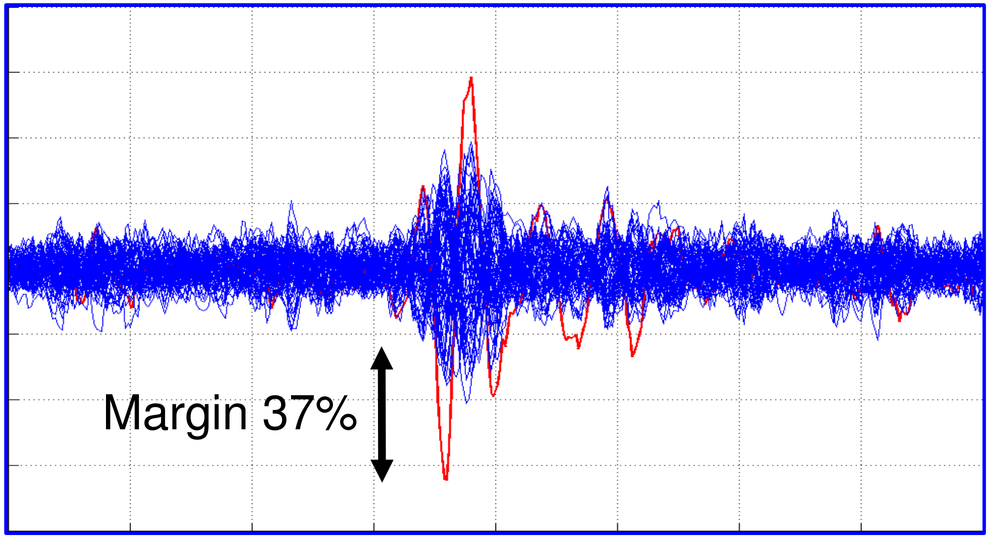


2. Hiding at the cell level

- Implementation of Dual Rail logic (DIMS) DES sub-module

DPA results show that previous conditions aren't satisfied
Successful DPA picture :

DPA on bit0



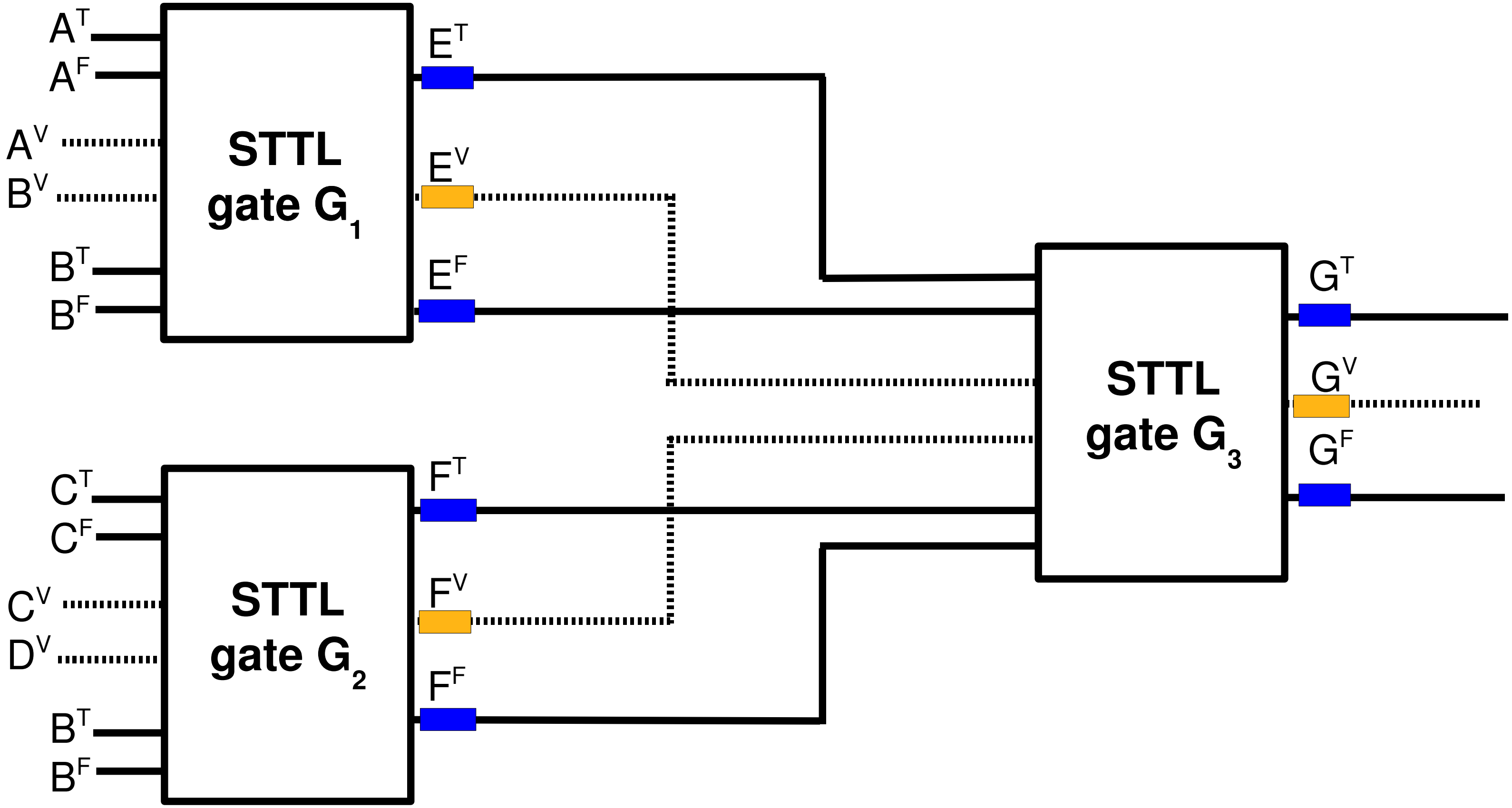
Outline

- 1. Power & EM analysis flow
- 2. Hiding at the cell level
- **3. Secure Triple Track Logic**
- 4. Results
- 5. Conclusion

3. Secure Triple Track Logic

STTL : principles

🟦 : logical signals (fast)
🟧 : validity signals (slow)



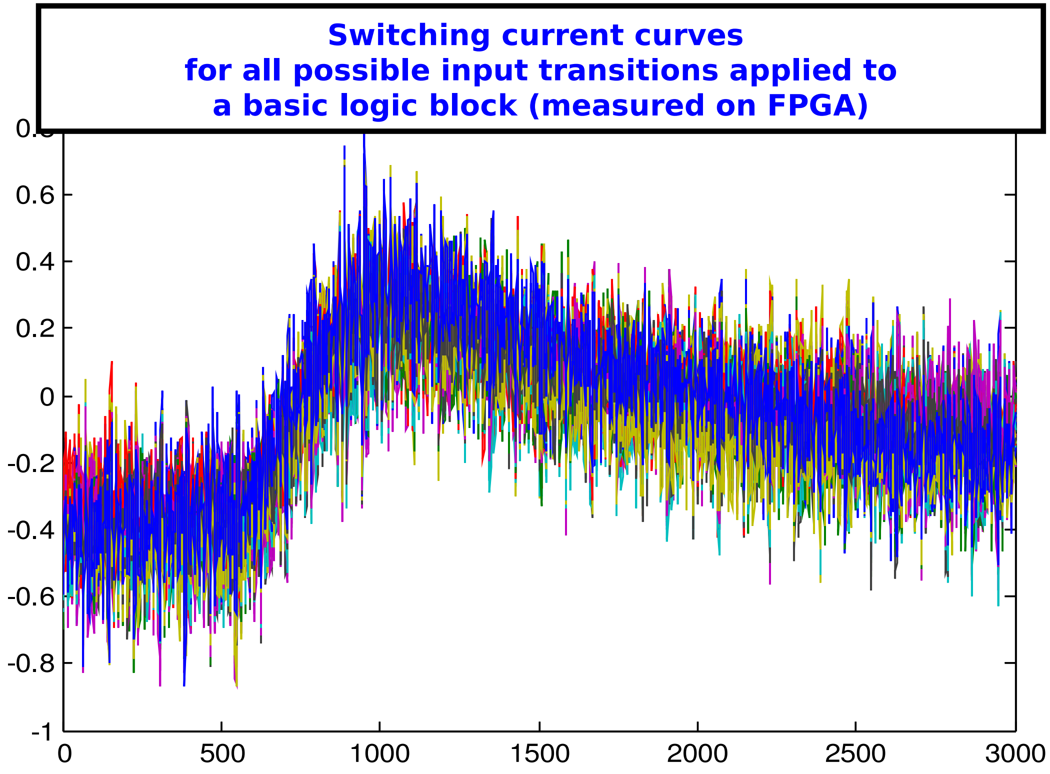
3. Secure Triple Track Logic

- STTL properties :

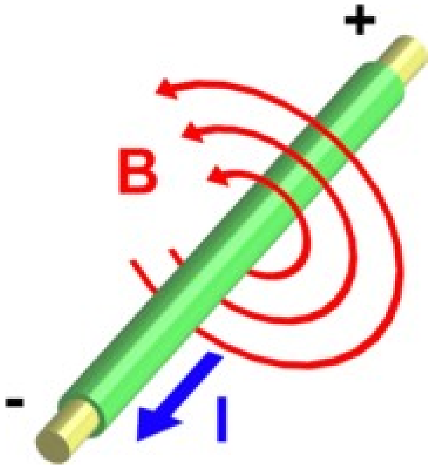
  Quasi data independent power consumption

  Quasi data independent propagation delay

  Quasi data independent electromagnetic emissions ?

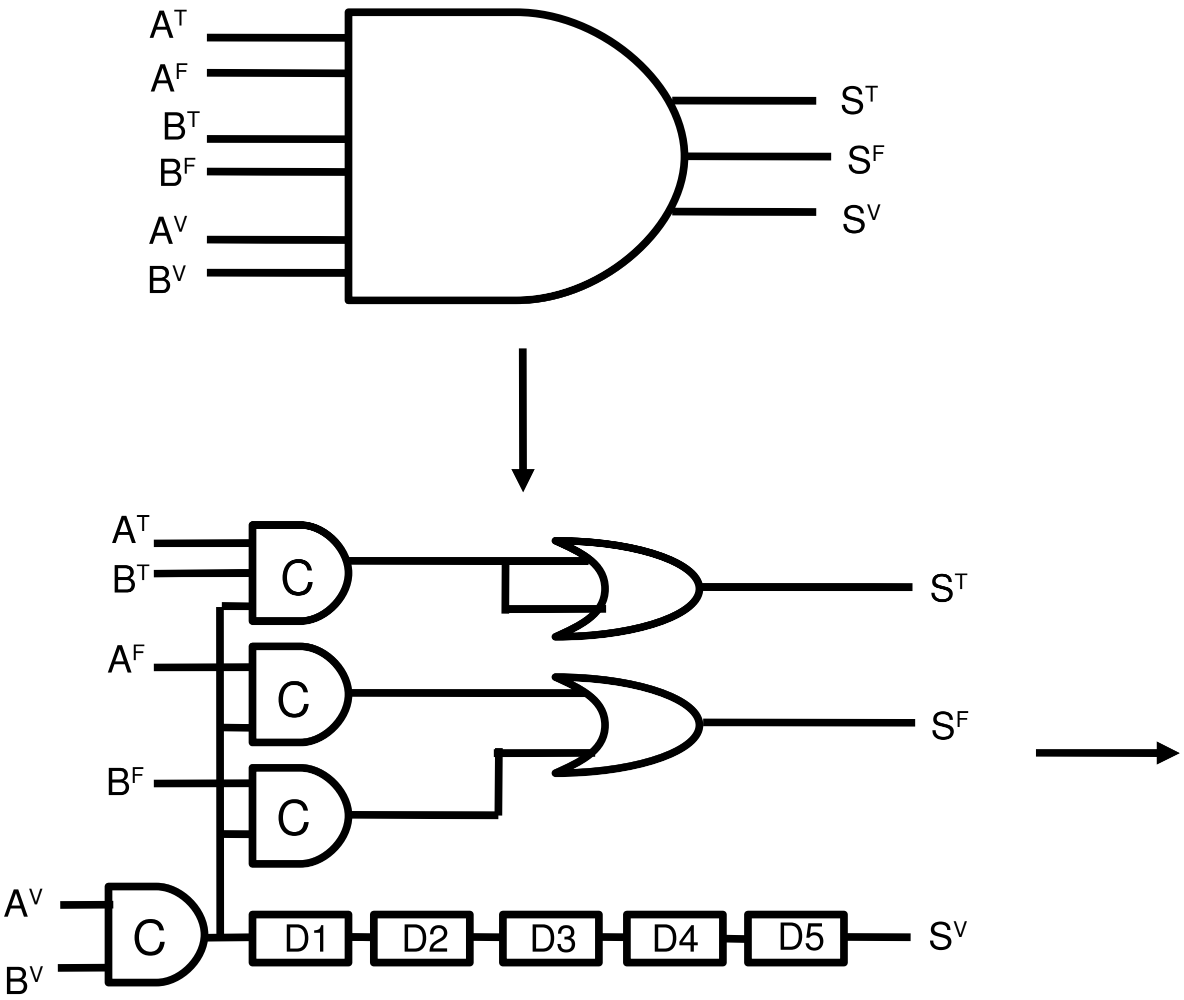


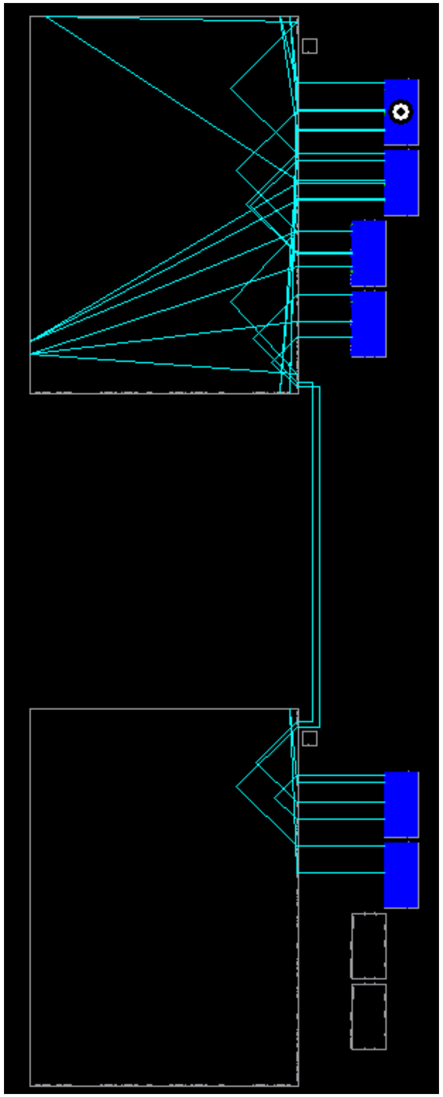
Switching current curves for all possible input transitions applied to a basic logic block (measured on FPGA)



3. Secure Triple Track Logic

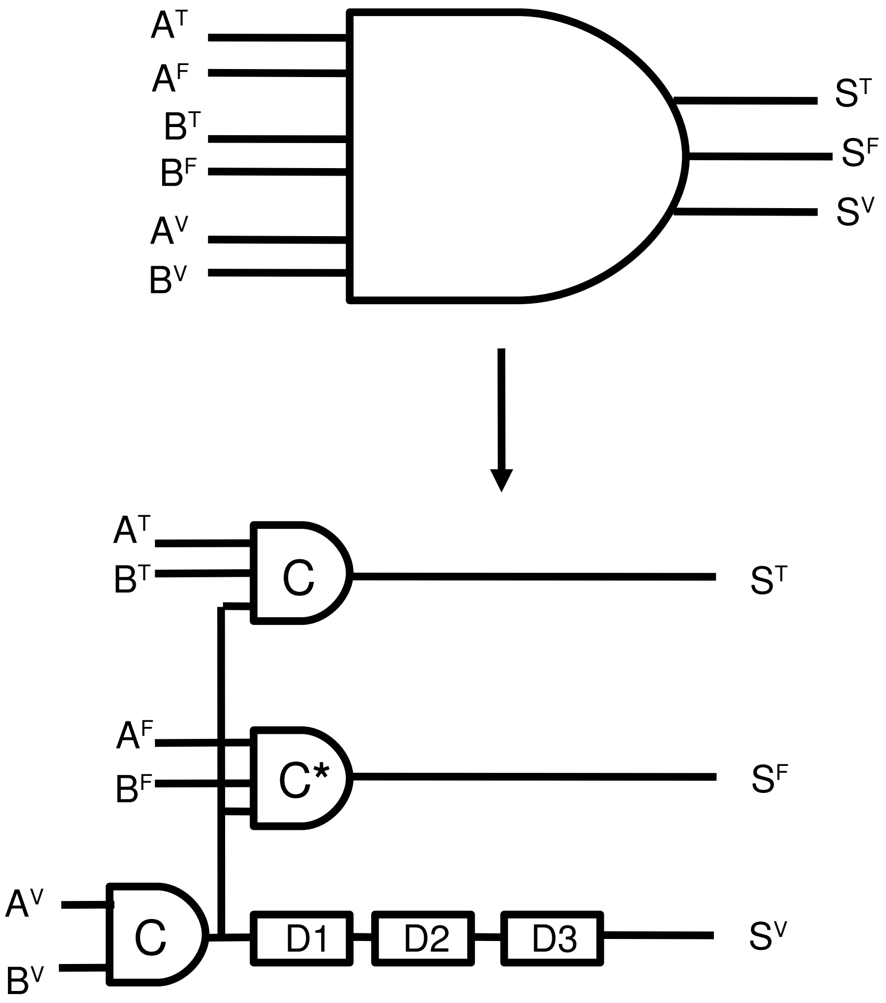
Mapping on FPGA : STTL AND2 gate v1



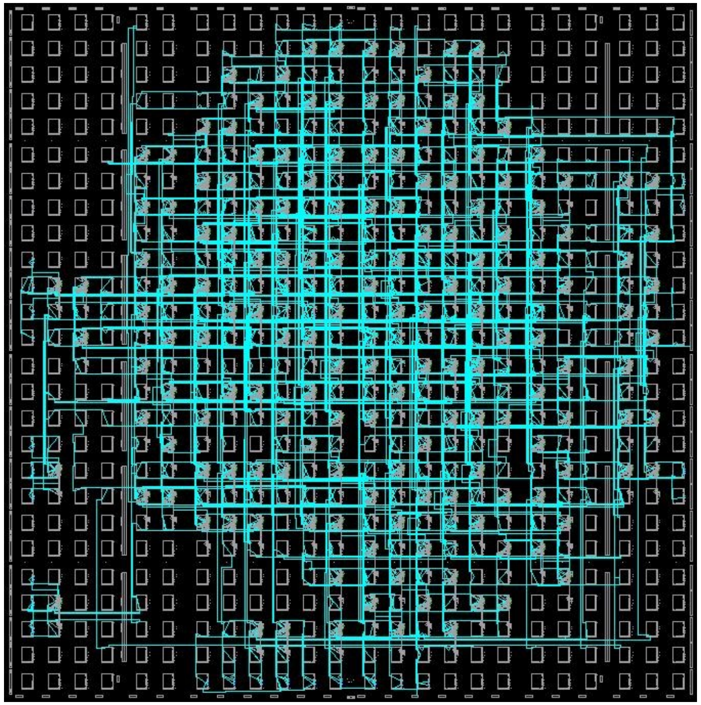


3. Secure Triple Track Logic

STTL v2 AND2 GATE :



STTL sub-module
after Place & Route



Outline

- 1. Power & EM analysis flow
- 2. Hiding at the cell level
- 3. Secure Triple Track Logic
- **4. Results**
- 5. Conclusion

4. Results

Timing analyses & required area for sub-module in different logic styles :

	SR	DR	STTL v1	STTL v2
Average (ns)	22,23	54,56	102,64	83,05
Min (ns)	15,62	50,36	102,64	83,05
Max (ns)	26,60	58,26	102,64	83,05
Area (slices)	175	504	994	529
Area (%)	9.00%	26.00%	51.00%	27.00%

Percentage of successful attacks functions on logic style :

	Single Rail	Dual Rail	STTL v1	STTL v2
DPA	75.00%	90.00%	6.00%	5.00%
DEMA	99.00%	NA	70.00%	NA

Outline

- 1. Power & EM analysis flow
- 2. Hiding at the cell level
- 3. Secure Triple Track Logic
- 4. Results
- **5. Conclusion**

5. Conclusion

- STTL seems robust against DPA & CPA
  - Quasi data independant computation time
  - Quasi data independant power consumption

- EM analysis seems more efficient than Power analysis
  - Contactless analysis
  - Local analysis rather than full chip analysis
  - SEMA provides a good idea of the chip floorplan

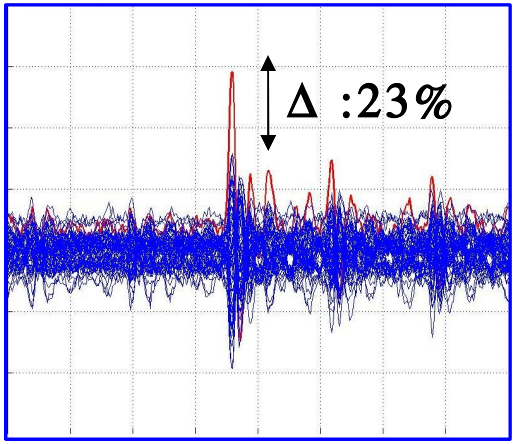
- STTL is more resistant to EM analysis than Single Rail logic, however it is not sufficient
  - 30% of successful analyses -> 70% of keys are disclosed
  - The (power & EM) balancing vanishes with the probe positionning ?

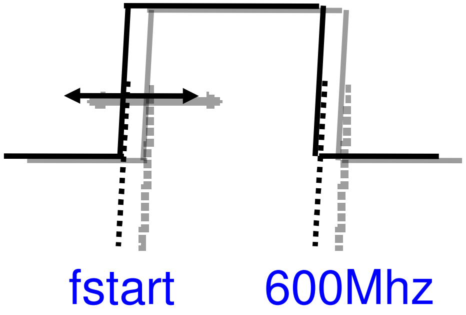
Thank you for your attention !

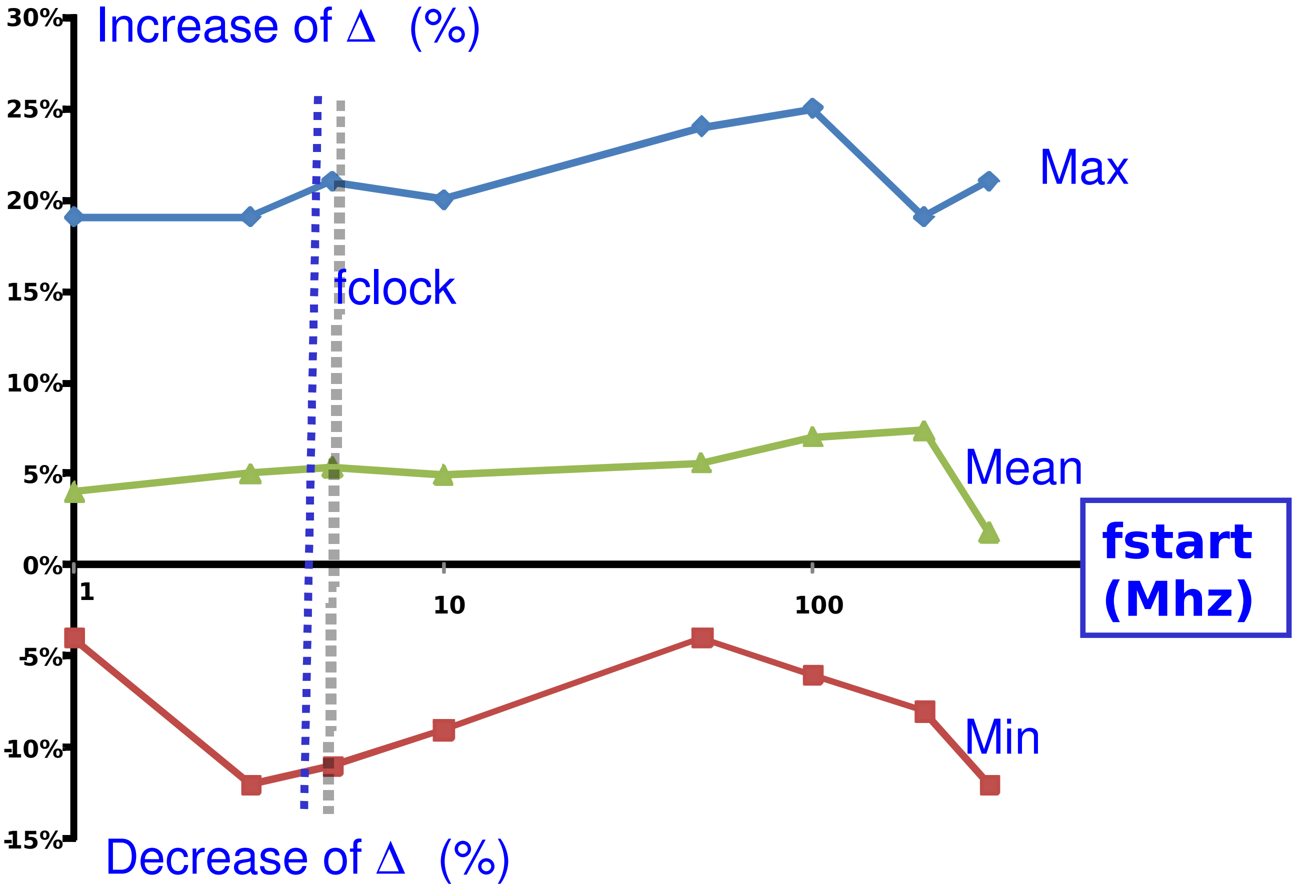
Any questions ?

Appendices A

Filtering of low frequencies







Filtering low frequencies may increase success of DPA & CPA