A very low cost DPA countermeasure to secure hardware AES cipher

Lilian Bossuet, Najeh Kamoun, Adel Gazel

Outlines

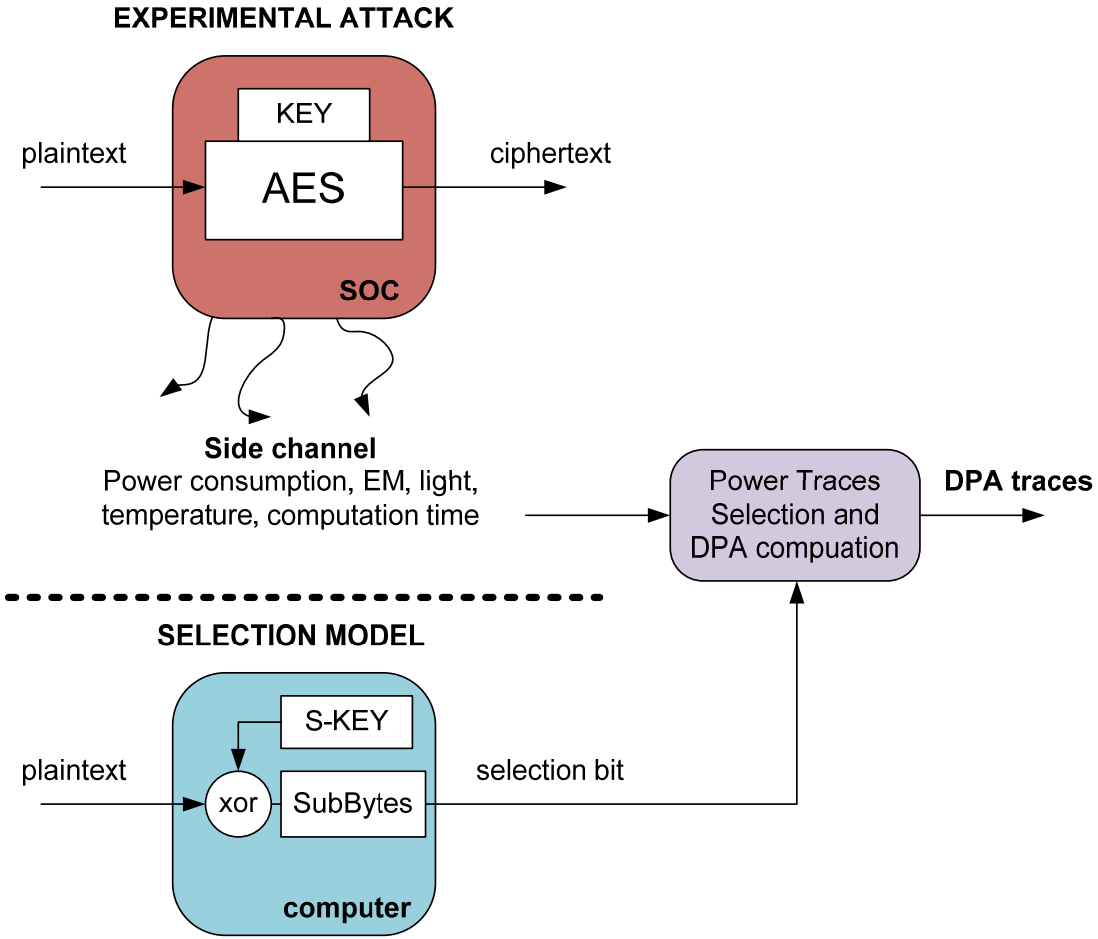
- The DPA context, how to practice, how to protect …
- A short survey of DPA countermeasures
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion

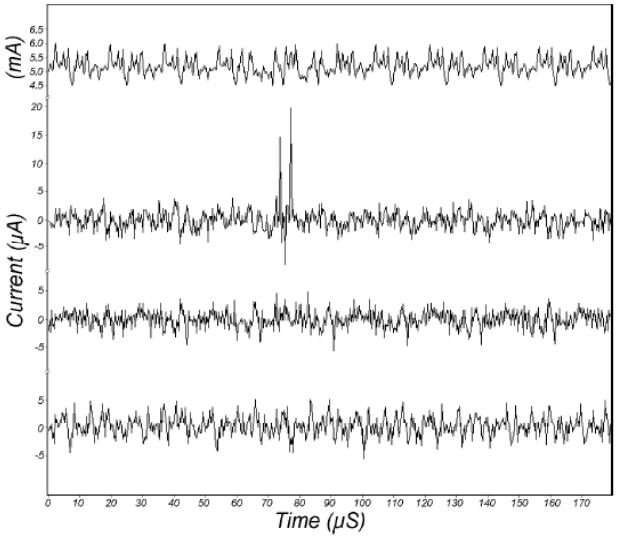
Outlines

- **The DPA context, how to practice, how to protect …**
- A short survey of DPA countermeasures
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion

Differential Power Analysise

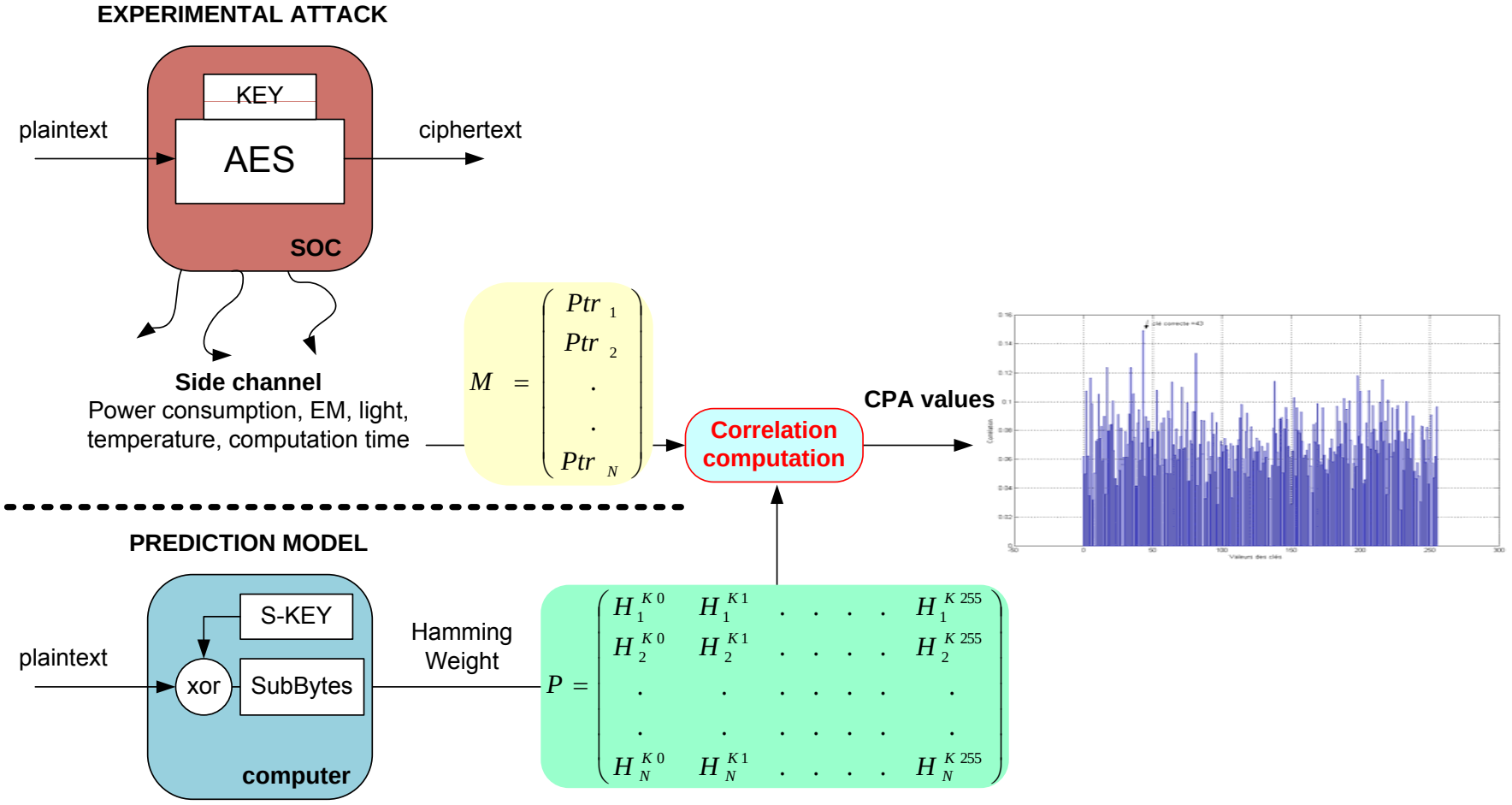
- During CRYPTO 1999 Paul Kocher et al. introduced the Differential Power Analysis attack against symmetric cipher (min distance)





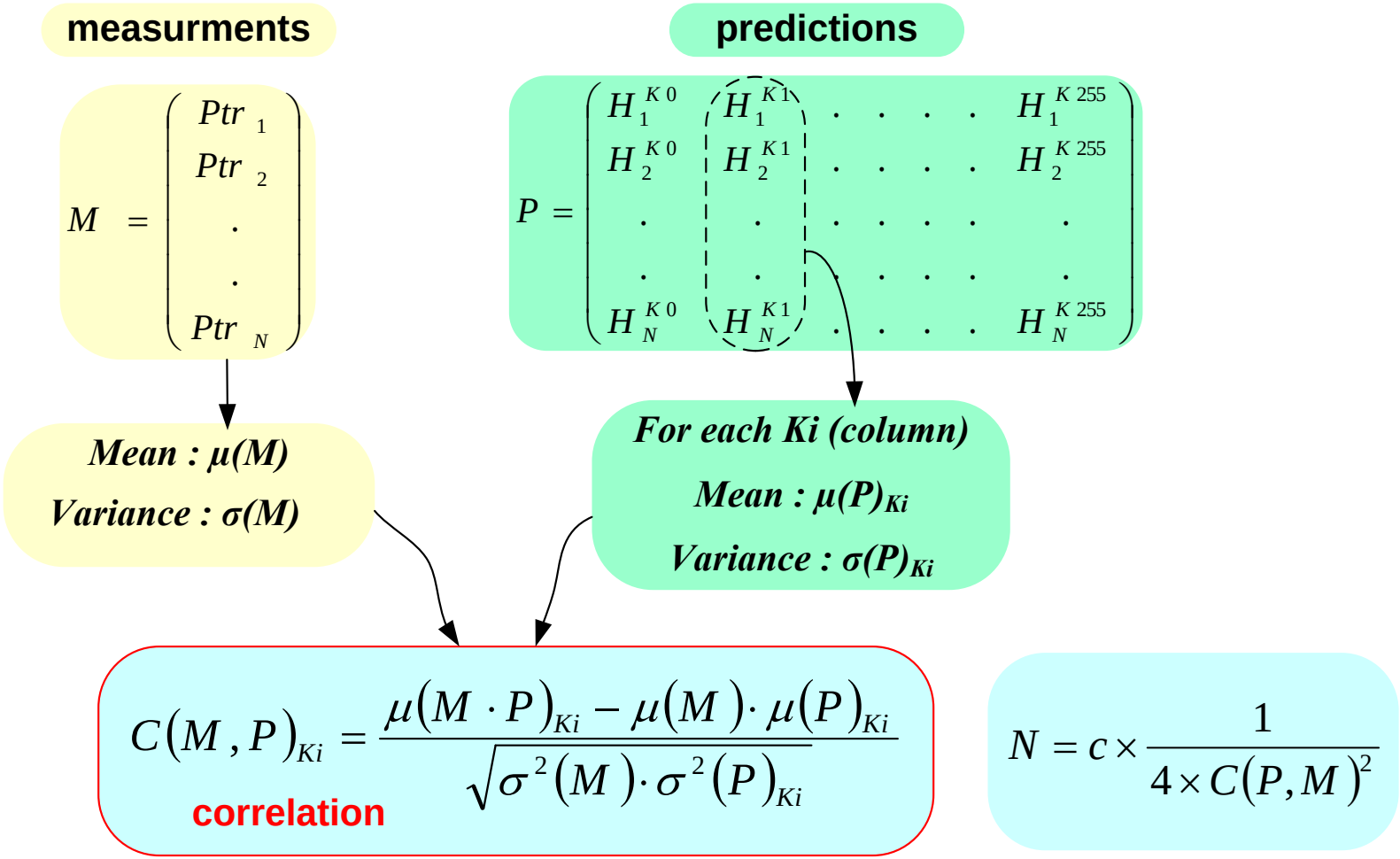
Correlation Power Analysis

- During CHES 2004 Eric Brier et al. (from Gemplus) introduced the Correlation Power Analysis attack against symmetric cipher



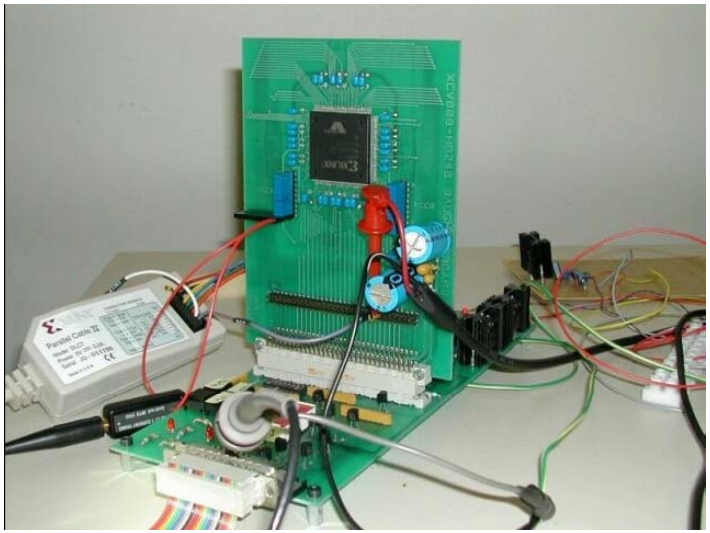
Correlation Power Analysis

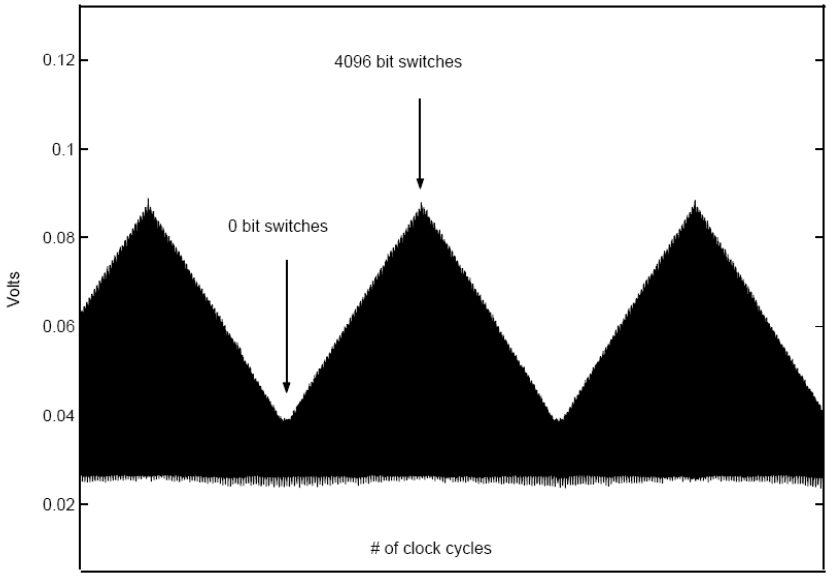
- Correlation computation with the *Pearson Coefficient*



Attack against FPGA

- During CHES 2003 and CHES 2004 Siddika Berna Örs, François-Xavier Standaert et al. experimented the Power Analysis attack on a SRAM FPGA (Xilinx Virtex 800)

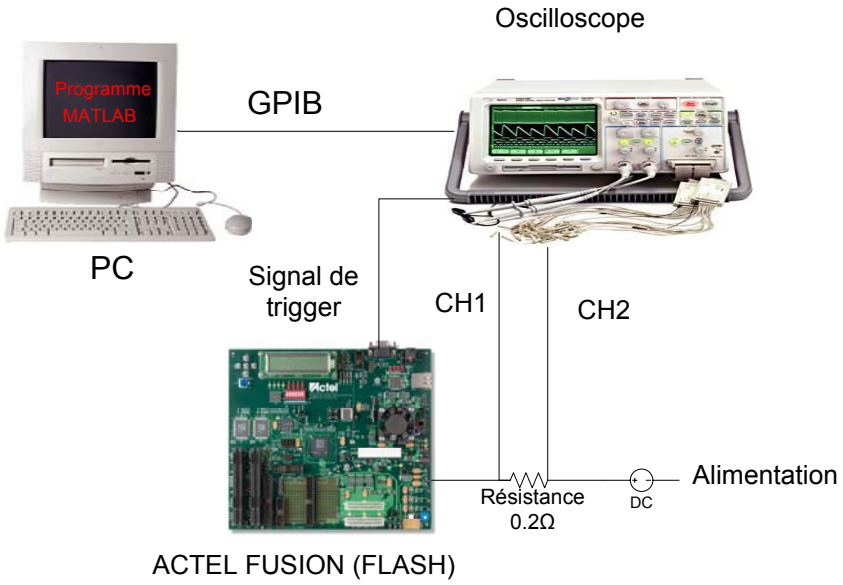




- The difficulty of obtaining good power consumption measurements for FPGA ?

IMS lab FPGA experimentation

- We have tested DPA and CPA attack with some FPGA



- DPA attack (N = 15 000 plaintexts)

√ Altera Stratix EP1S25
  ➔ SRAM Technology 0,18 µm

- CPA attack (N = 1 000 plaintexts)

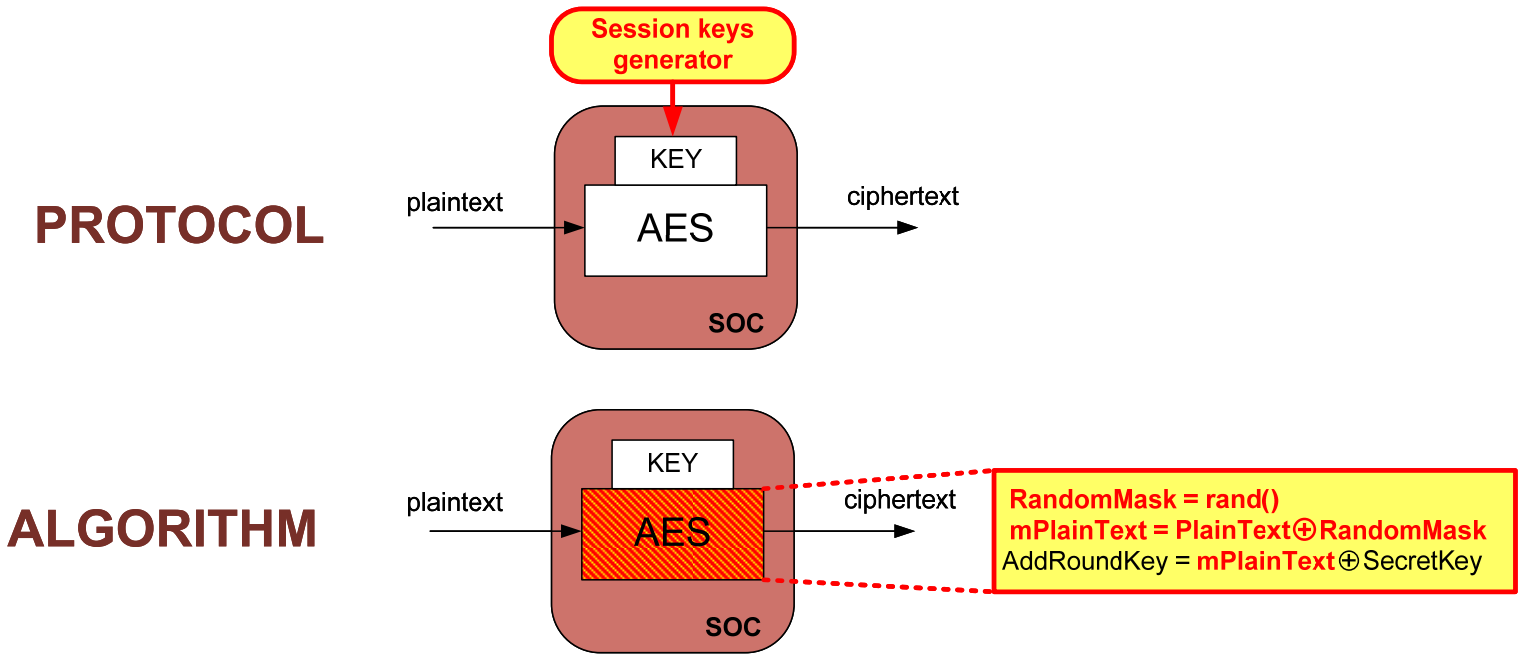
√ Xilinx Virtex-II 2VP30
  ➔ SRAM Technology 0,15 µm

√ Xilinx Virtex-4 SX25
  ➔ SRAM Technology 90 nm

√ Actel Fusion S600
  ➔ **Flash** Technology 0,13 µm

Level of protection 1/2

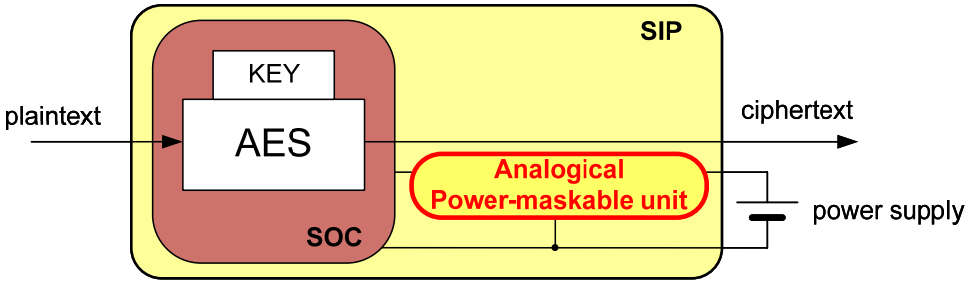
- At the protocol and algorithmic levels : software level



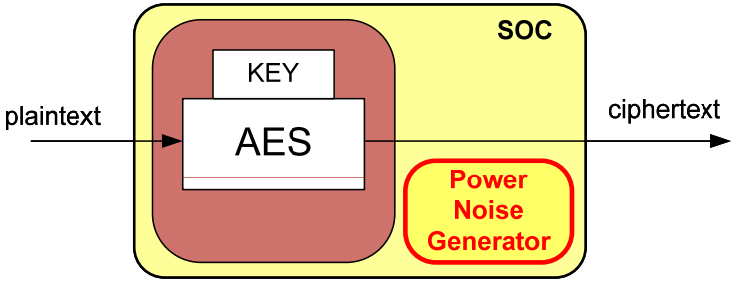
Level of protection 2/2

- From the system to the logic level : hardware level

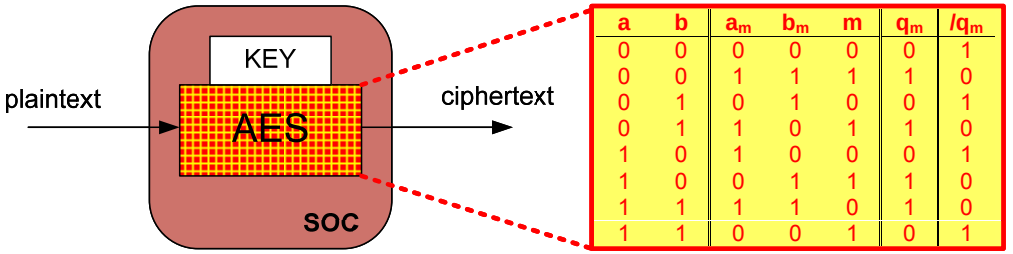
SYSTEM



ARCHITECTURE



LOGIC



a	b	a_m	b_m	m	q_m	$/q_m$
0	0	0	0	0	0	1
0	0	1	1	1	1	0
0	1	0	1	0	0	1
0	1	1	0	1	1	0
1	0	1	0	0	0	1
1	0	0	1	1	1	0
1	1	1	1	0	1	0
1	1	0	0	1	0	1

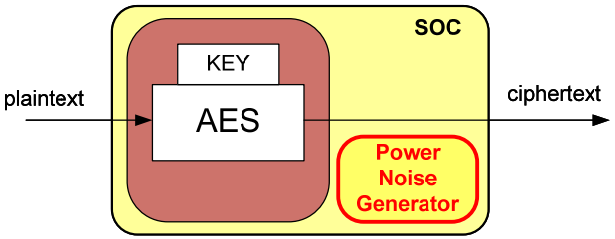
Outlines

- The DPA context, how to practice, how to protect …
- **A short survey of DPA countermeasures**
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion

Outlines

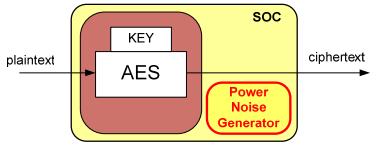
- The DPA context, how to practice, how to protect …
- **A short survey of DPA countermeasures**
  - ➔ **Make a power noise**
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion

ARCHITECTURE

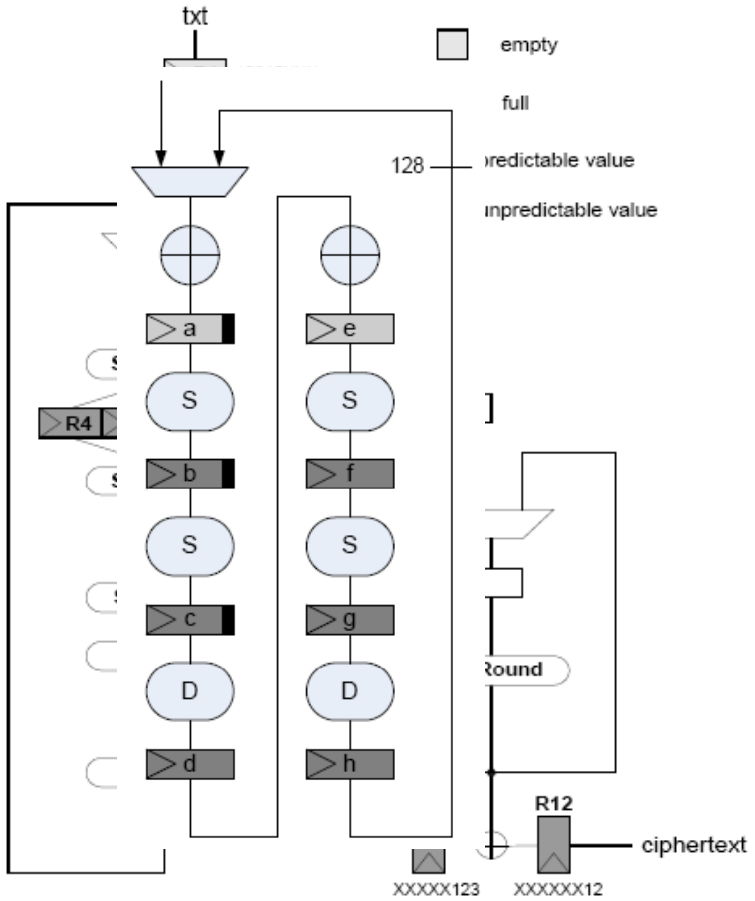


Make a power noise

- Use an additive power noise feel interesting to resist DPA



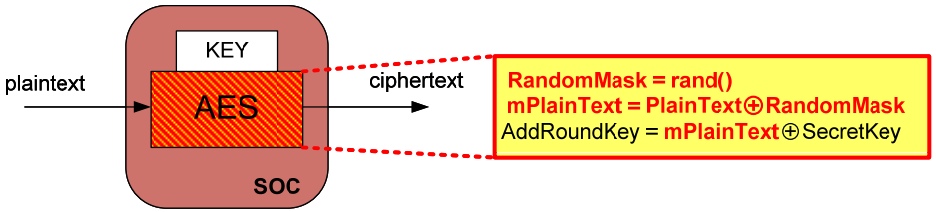
- First idea : use a pipelined architecture
  - ➔ Proposed by Standaert et al. In CHES 2004
- But most of registers are predictable
- Second idea : unrolled and pipelined implementation (cost-less protection !)
  - ➔ Standaert et al. CHES 2004
- Noise addition does not fundamentally counteract DPA
  - ➔ The averaging in DPA filters out uncorrelated noise from the differential power trace
- Nevertheless it reduces the correlation between prediction and measurement
  - ➔ Need more power traces



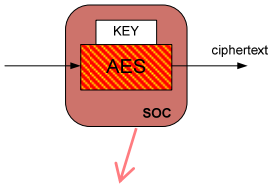
Outlines

- The DPA context, how to practice, how to protect …
- **A short survey of DPA countermeasures**
  - ➔ Make a power noise
  - ➔ **Use an algorithmic mask to reduce the correlation between the data and the power consumption**
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion

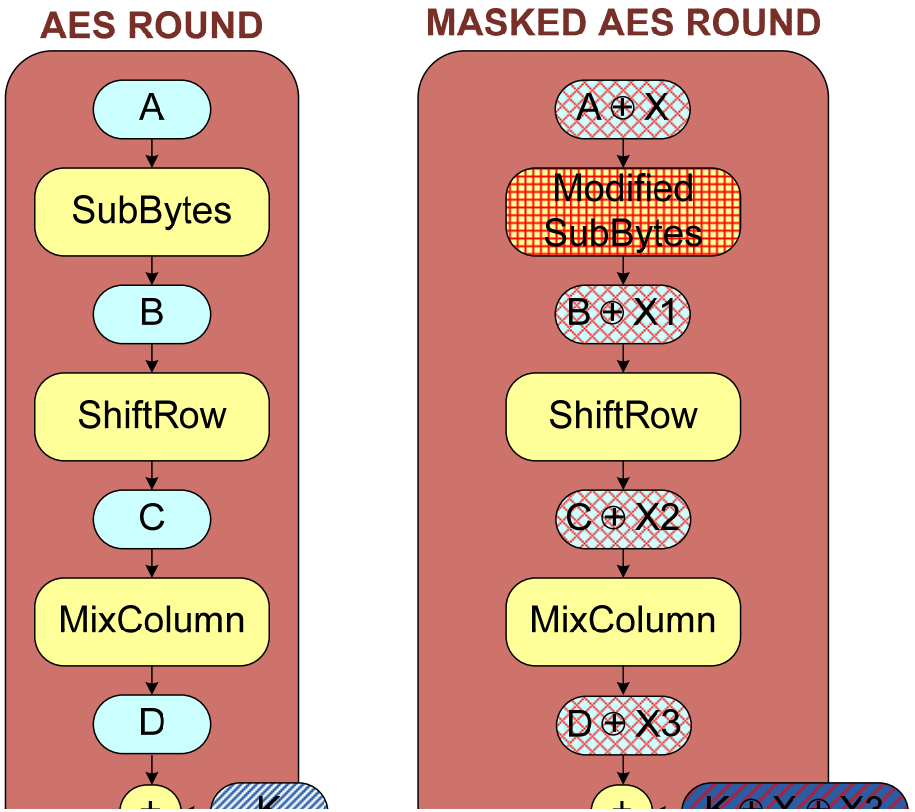
ALGORITHM



Use a algorithmic random mask



- The idea is to randomize the intermediate values that the cryptographic devices processes
  - ➔ Initially was done by adding a random value to the intermediate value (simple additive masking Messerges in FSE 2000) but it does not work for rijndael as SubBytes is not completely linear
  - ➔ The first article describing a complete masking scheme for AES (additive and multiplicative mask) was published by Akkar and Giraud in CHES 2001.
  - ➔ It was a software implementation
  - ➔ More than 3 time slower !!!

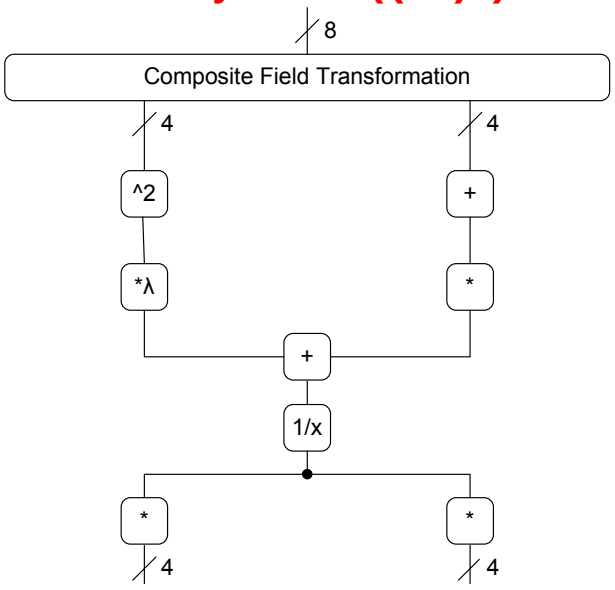


Type of AES	Timing at 5 Mhz	Space of ROM in bytes	Space of RAM in bytes
Normal AES	18.1 ms	730	41
AES with CM2	58.7 ms	1752	121

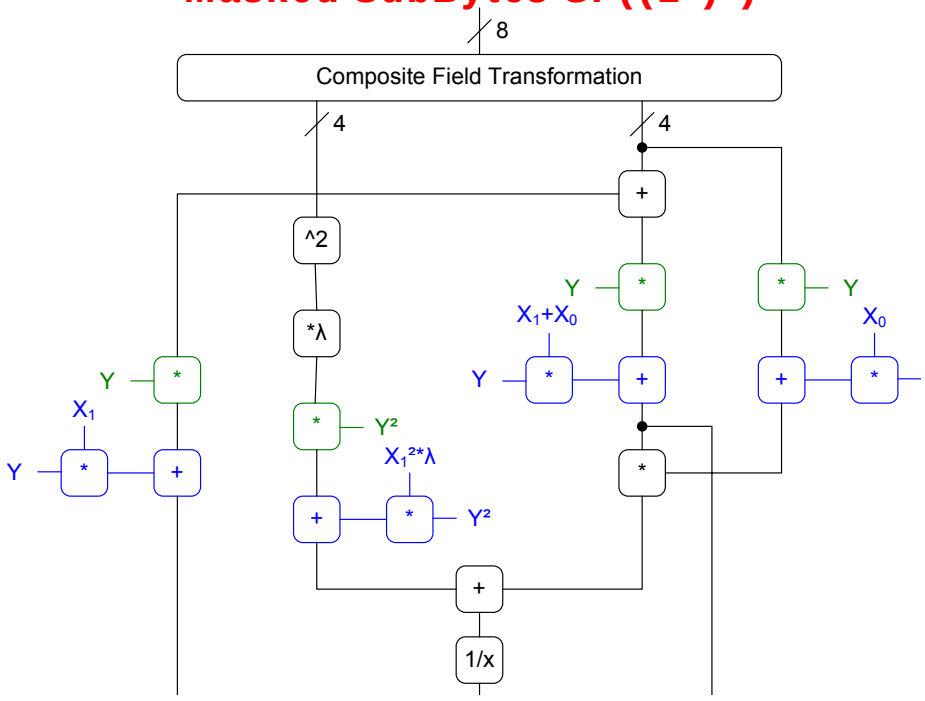
Hardware masked SubBytes

- Mentens and al. Workshop PDS 2004

SubBytes GF((2⁴)²)



Masked SubBytes GF((2⁴)²)



Impl.	unsecured	secured
Frequency (MHz)	33	23
Throughput (Mbit/s)	41	29
Number of CLBs	908	1113
Number of clock cycles	102	102

More about masking scheme

- To compare our proposed countermeasure, we have implemented a very low area-cost masked Sbox witch work in GF(2)
  - ➔ Proposed by Canright and Batina. in ACNS 2008.

- We give the result with Xilinx Virtex 4 FPGA (without the mask generator cost)
  - ➔ Published by Kamoun and Bossuet in IDT 2008

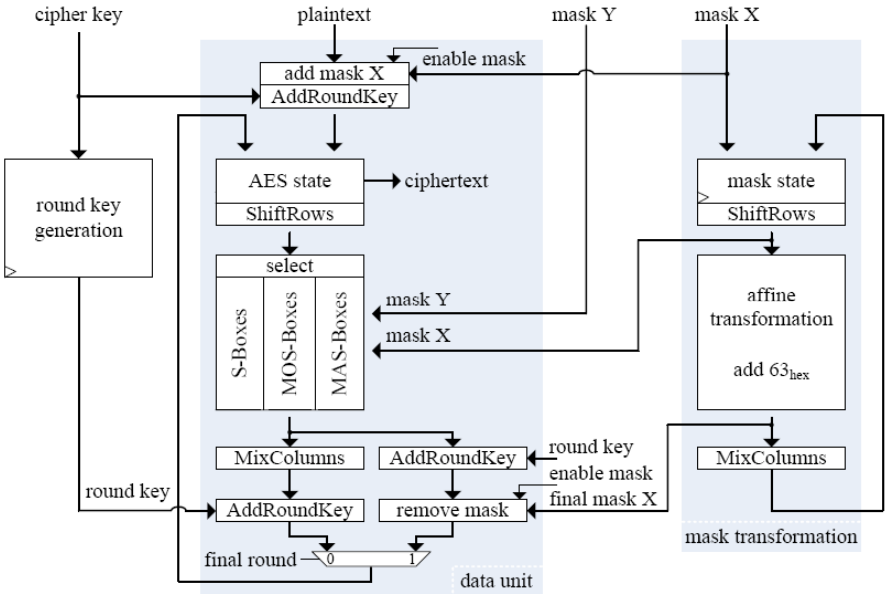
Performance AES S-Box	Area (#V4-slices)	Area Overhead	Frequency (MHz)	Speed Overhead
Unsecure	36		184	
Masked (Canright 08)	100	+ 170 %	122	-33 %

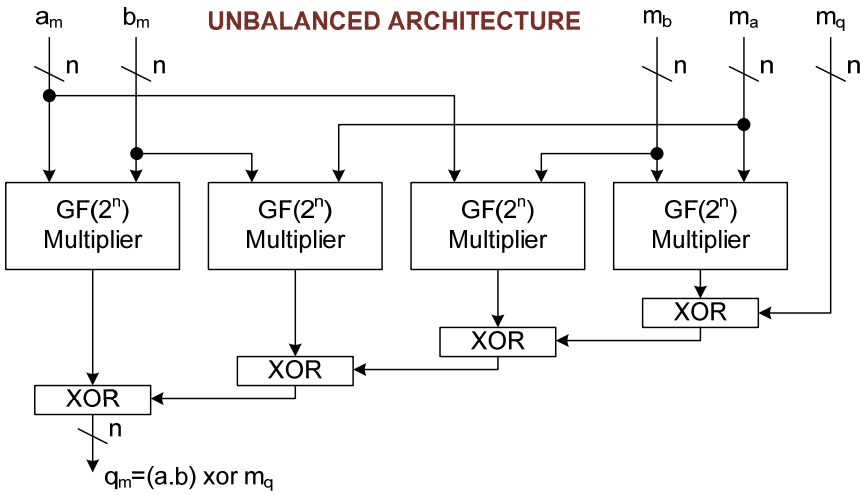
Performance AES (16 S-Box)	Area (#V4-slices)	Area Overhead	Frequency (MHz)	Speed Overhead
Unsecure	1424		110	
Masked (Canright 08)	2281	+ 60 %	97	-11 %

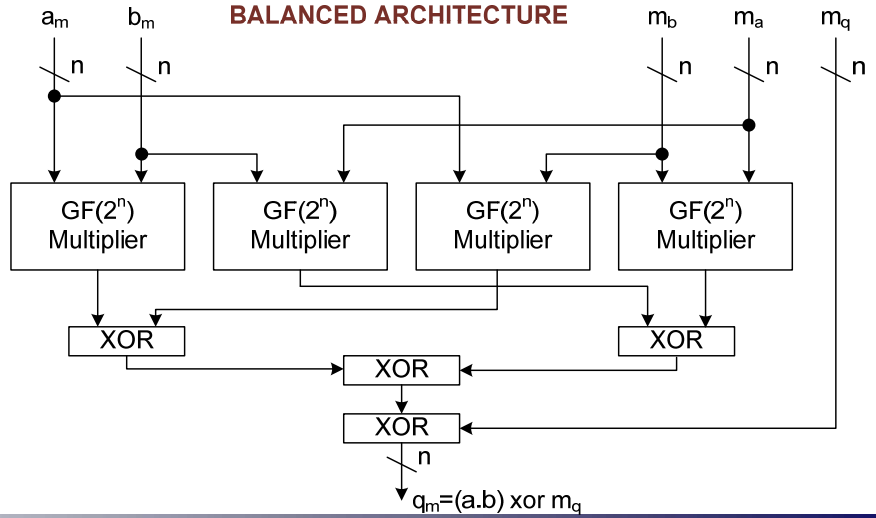
More about masking chain

- Warning : Masking the AES S-Boxes does not prevent DPA attacks if glitches occur in the circuit
  - ➔ Mangard et al. CHES 2005

- But glitches are due to bad design

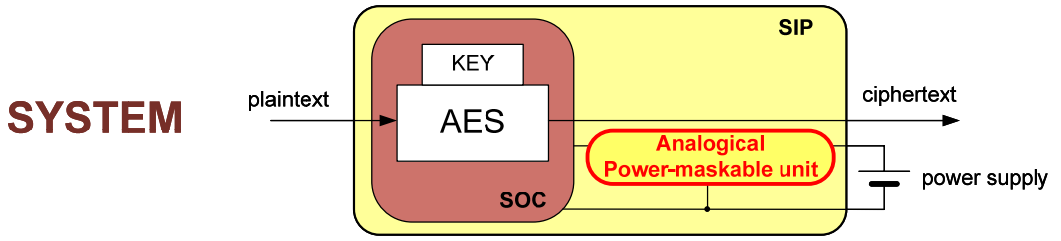




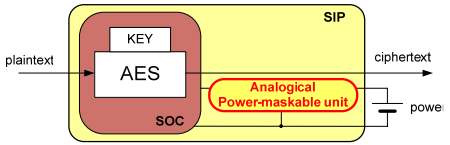


Outlines

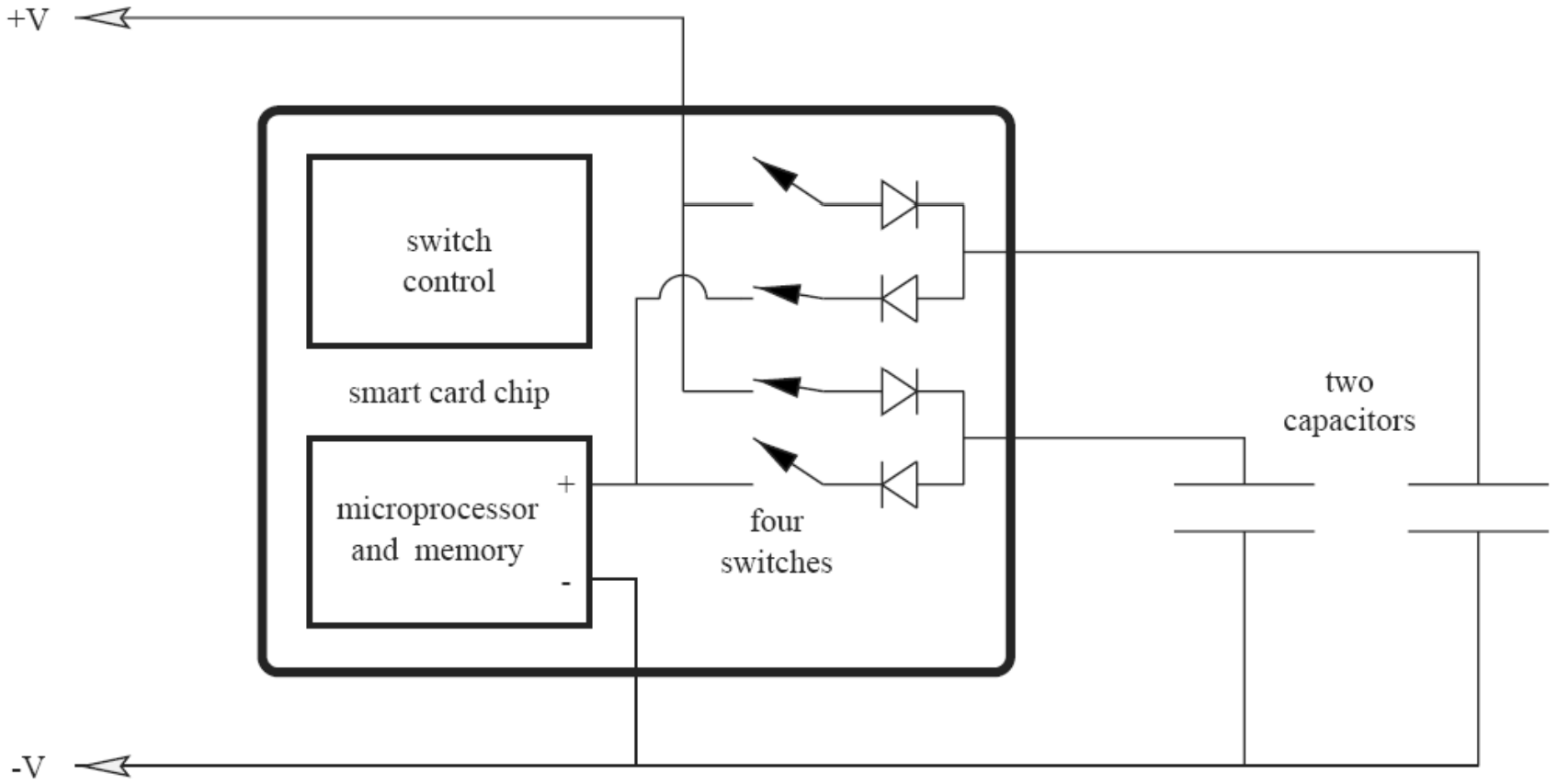
- The DPA context, how to practice, how to protect …
- **A short survey of DPA countermeasures**
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ **Maximization smoothing of the power consumption signal**
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion



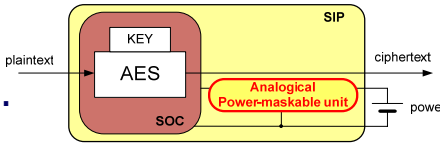
Power consumption smoothing



- First proposition by Shamir in CHES 2000
  - ➔ He proposed a method in witch the power supply is isolated from the cryptographic hardware of a smart card by using capacitors to supply current

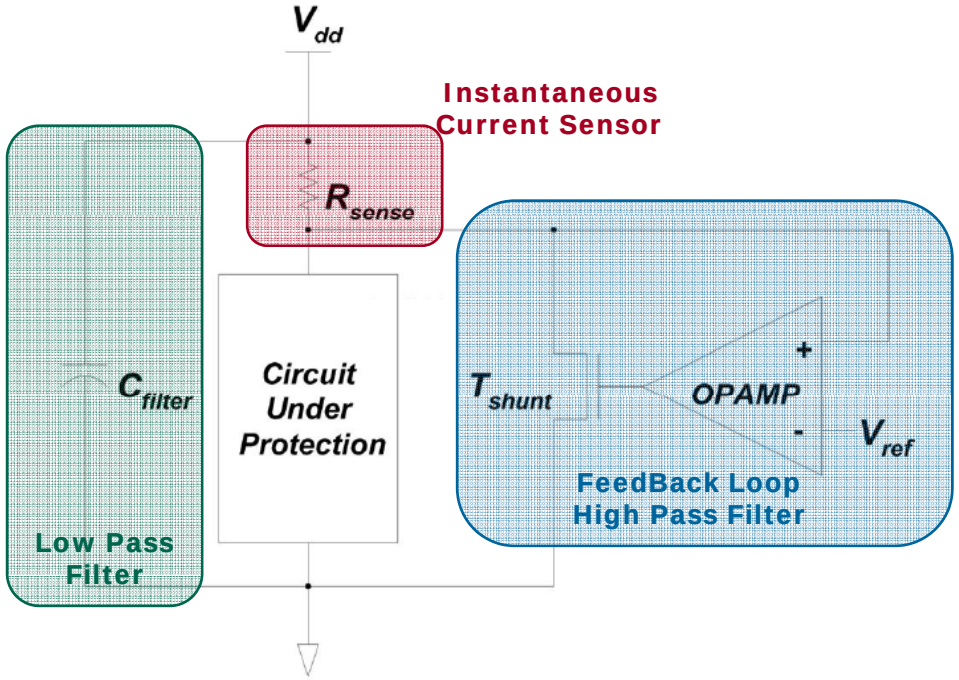


Power consumption smoothing



- An other solution is proposed by Ratanpal et al. in IEEE Trans. On DSC 2004
  - ➔ They presented a circuit that can be added to crypto-hardware to suppress information leakage through the power supply pin side channel.

- Rsense = current sensor
- Rsense + Cfilter = low pass filter
- OPAMP + T = feedback loop
  - ➔ HighPass filter

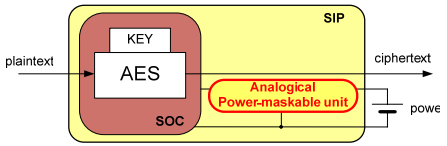


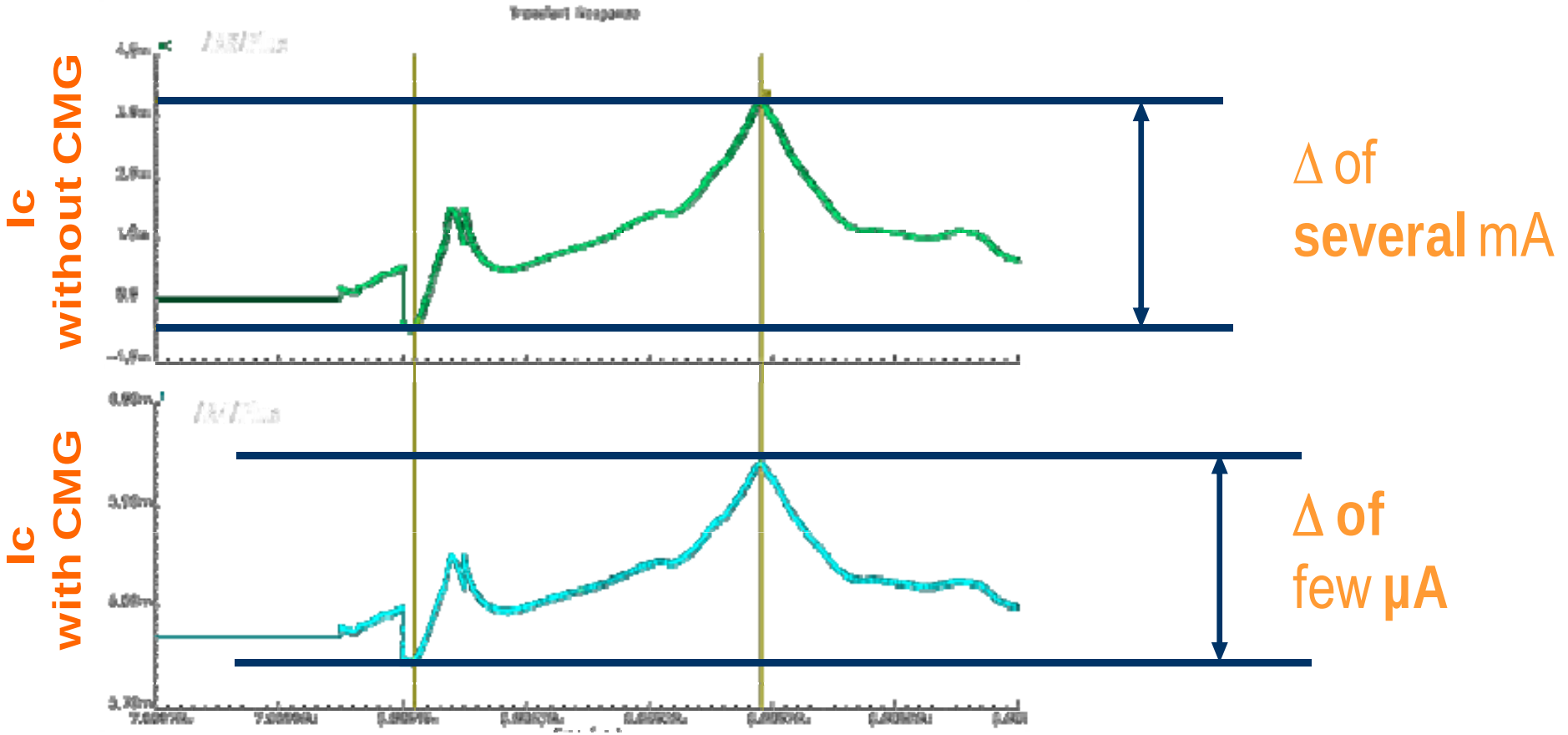
- Power Consumption Increase

- This countermeasure does not make the DPA attack impossible
  - ➔ The attacker requires 203 times more sample.

Power consumption smoothing

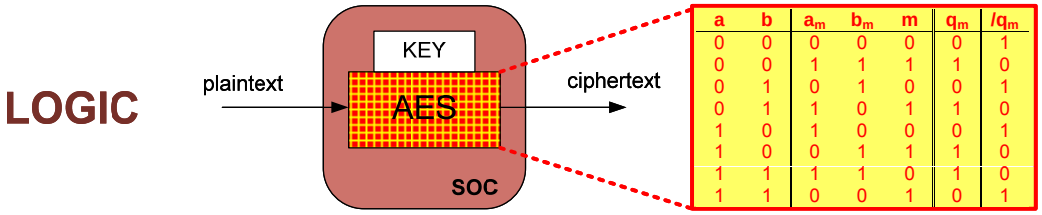
- In VLSI 2005, Mesquita et al. improve the Ratanpal solution by using a current mirror





Outlines

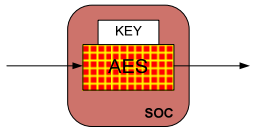
- The DPA context, how to practice, how to protect …
- **A short survey of DPA countermeasures**
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ **Counterbalance the logic gate output switching**
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion



a	b	a_m	b_m	m	q_m	$/q_m$
0	0	0	0	0	0	1
0	0	1	1	1	1	0
0	1	0	1	0	0	1
0	1	1	0	1	1	0
1	0	1	0	0	0	1
1	0	0	1	1	1	0
1	1	1	1	0	1	0
1	1	0	0	1	0	1

Counterbalance the logic gate output switching

- Main objective: making a cell's power consumption identical in every clock cycle



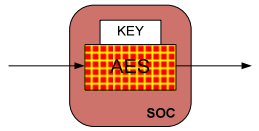
- First structured approach was the use of hidding logic styles
  - ➔ Masking the instantaneous power consumption of the cells in each clock cycle
  - ➔ As a result, the device power consumption has a maximal value in each clock cycle

- Types of hiding logic styles
  - ➔ Dual-rail precharge (DRP) – SABL (custom logic) and WDDL (standard)
  - ➔ Asynchronous logic
  - ➔ Current-mode logic styles

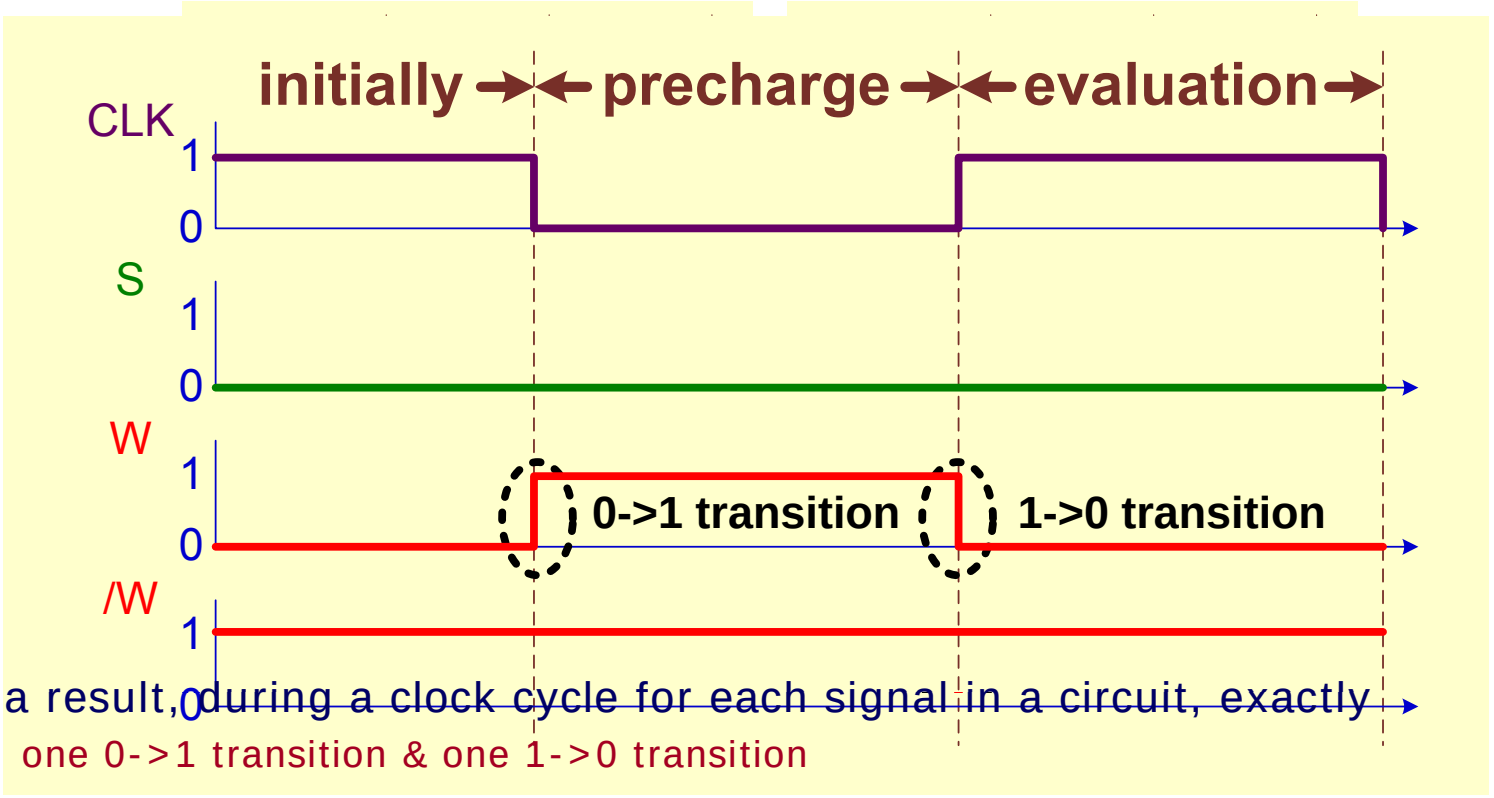
- Second approach was the random masked logic style
  - ➔ Each intermediate value is masked by a random mask
  - ➔ Could be use with DRP – MDPL
  - ➔ Random switching logic RSL

Dual-Rail Precharge (DRP) concept

- Every signal S is encoded in a differential manner on two complementary wires W and /W
  - ➔ Two phases : PRECHARGE & EVALUATION



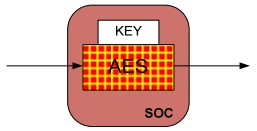
- Exemple, initially S=0 and the precharge sets W et /W to 1



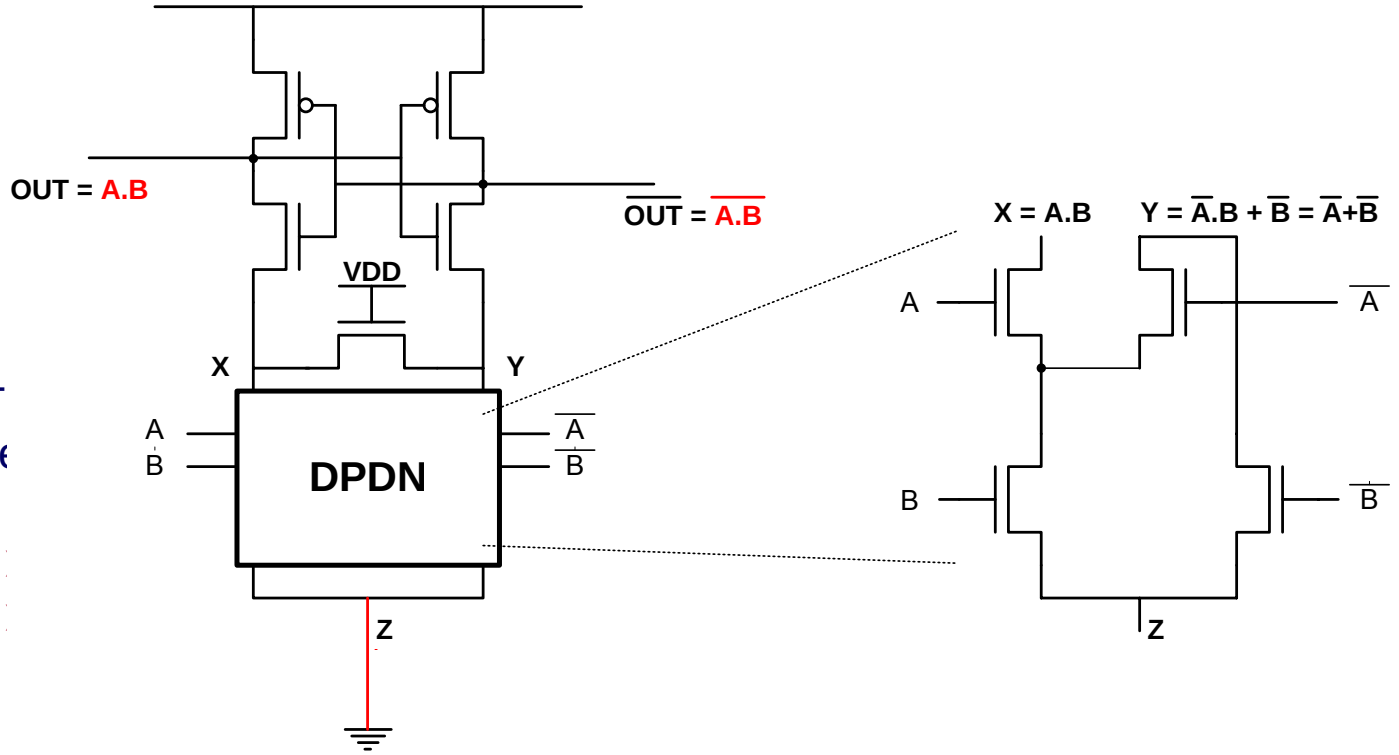
- As a result, during a clock cycle for each signal in a circuit, exactly
  - ➔ one 0->1 transition & one 1->0 transition

Sense Amplifier Based Logic *SABL*

- SABL custom logic was first presented by Tiri et al. in ESSCIRC 2002
  - ➔ Use custom logic: Differential Pull Down Network *DPDN*
- Example of a SABL AND gate X=A.B



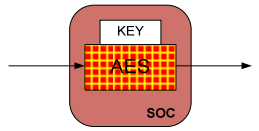
EVALUATION: clk = 1



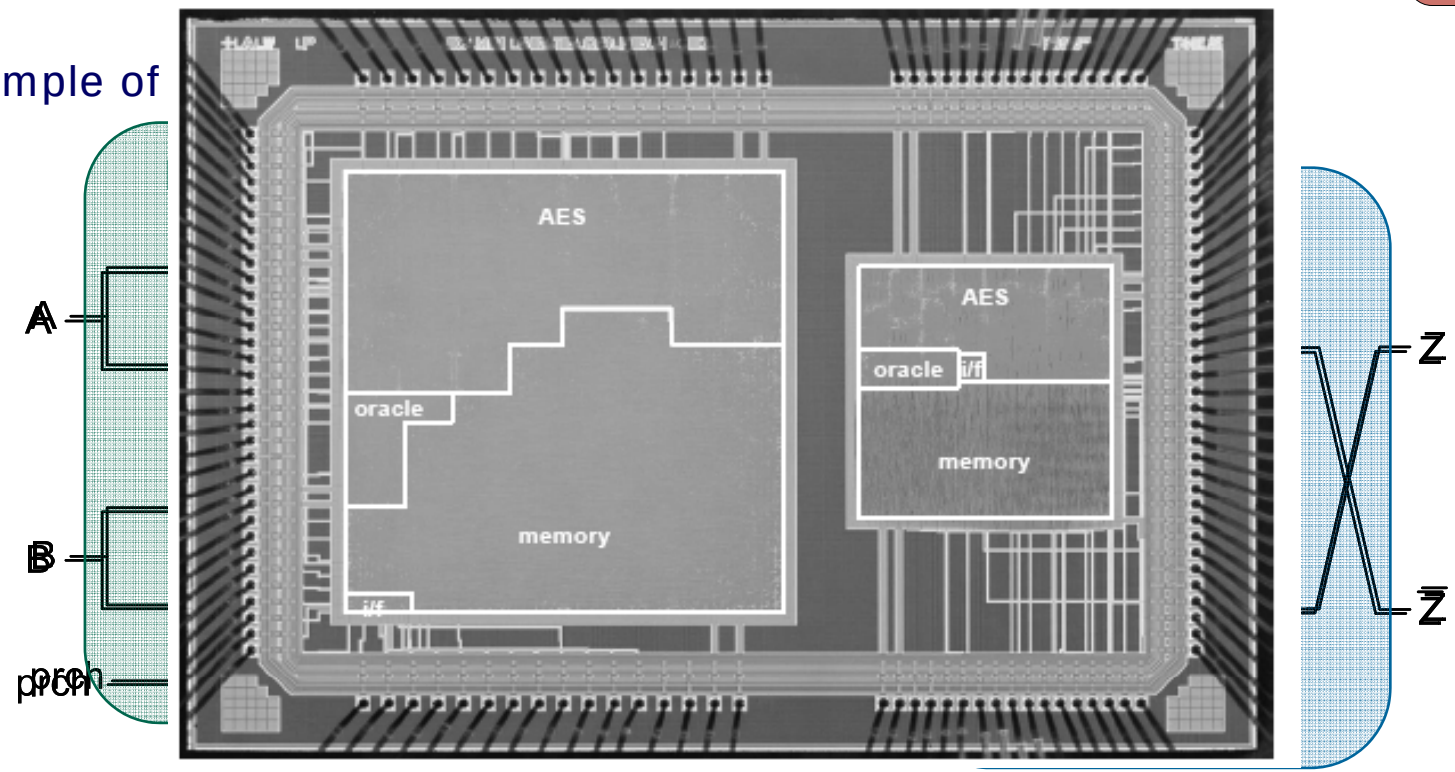
- T
  r

Wave Dynamic Differential Logic *WDDL*

- WDDL was first presented by Tiri et al. in DATE 2004
  - ➔ Use Standard cell



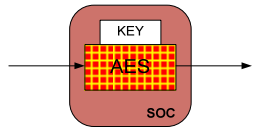
- Example of



- Tiri et al. gave the following results (0,18 µm) in CHES 2005
  - Area overhead = +310 % (3,1 time more eq. gate)
  - Power consumption overhead = + 370 % (estimated)

Masked Dual-Rail Pre-Charge Logic *MDPL*

- MDPL logic was first presented by T. Popp and and S. Mangard in CHES 2005 (implementation ISCAS 2006)
  - ➔ Use additive random mask and majority gate



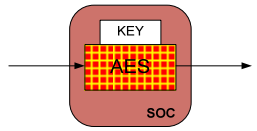
- The majority gate **q=*MAJ*(a,b,c)**

a	b	c	q	/q
0	0	0	0	1
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

$$q = a.b + b.c + a.c$$

Masked Dual-Rail Pre-Charge Logic *MDPL*

- MDPL logic was first presented by T. Popp and and S. Mangard in CHES 2005 (implementation ISCAS 2006)
  - ➔ Use additive random mask and majority gate



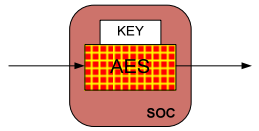
- The majority gate **q=*MAJ*(a,b,m)**

a	b	m	q	/q
0	0	0	0	1
0	1	0	0	1
1	0	1	1	0
1	1	1	0	1
0	0	1	1	0
0	1	1	1	0
1	0	0	0	1
1	1	0	1	0

$$q = a.b + b.m + a.m$$

Masked Dual-Rail Pre-Charge Logic *MDPL*

- MDPL logic was first presented by T. Popp and and S. Mangard in CHES 2005 (implementation ISCAS 2006)
  - ➔ Use additive random mask and majority gate



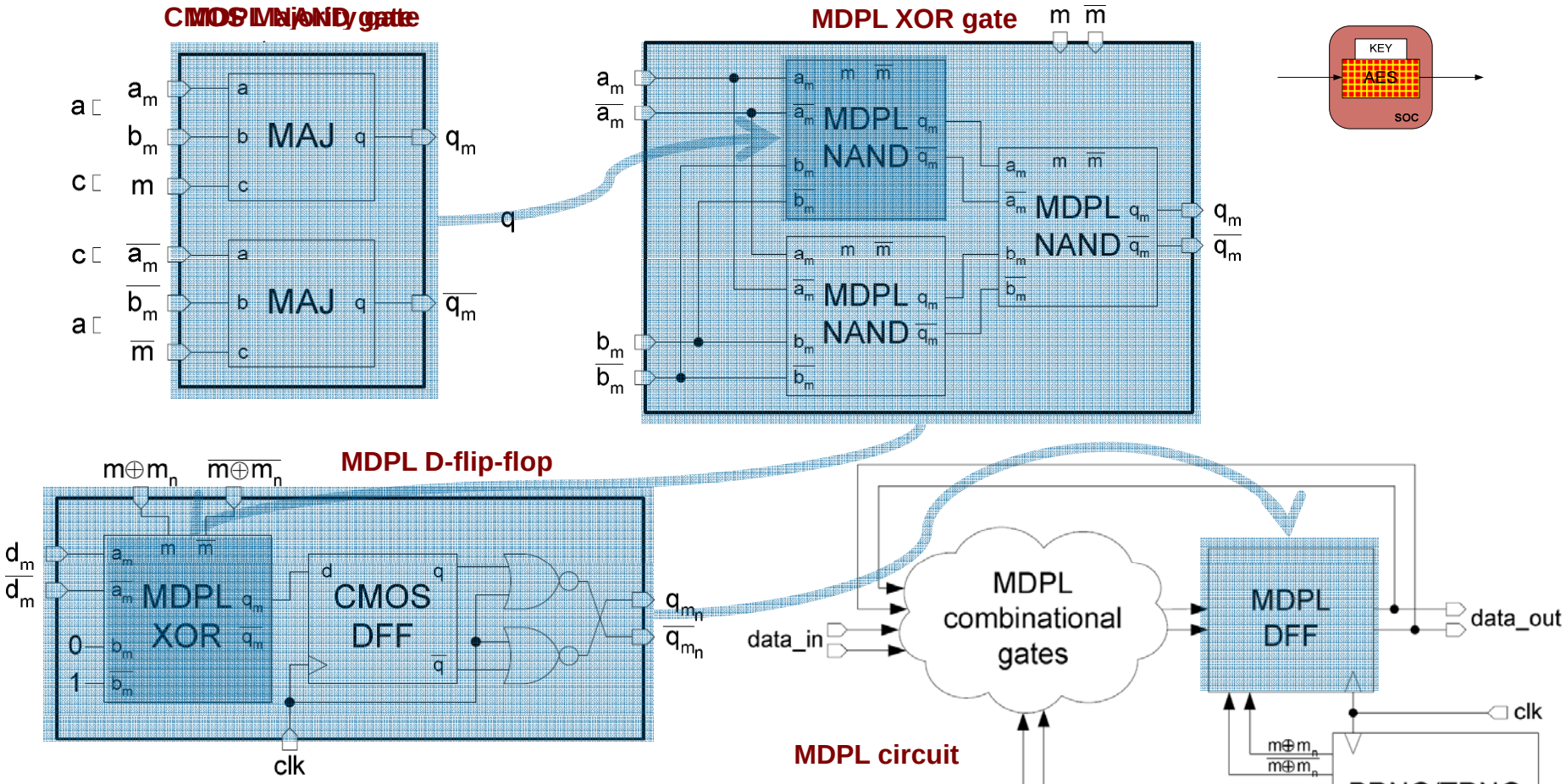
- The **MASKED** majority gate $q_m = MAJ(a_m, b_m, m)$

a	b	q	a_m	b_m	m	q_m	$/a_m$	$/b_m$	/m	$/q_m$
0	0	0	0	0	0	0	1	1	1	1
0	1	0	0	1	0	0	1	0	1	1
1	0	0	0	1	1	1	1	0	0	0
1	1	1	0	0	1	0	1	1	0	1
0	0	0	1	1	1	1	0	0	0	0
0	1	0	1	0	1	1	0	1	0	0
1	0	0	1	0	0	0	0	1	1	1
1	1	1	1	1	0	1	0	0	1	0

$a_m = a \oplus m$ $\quad$ $b_m = b \oplus m$

$q_m = (a.b) \oplus m$ $\quad$ $/q_m = (a.b) \oplus /m$

MDPL Implementation (Popp ISCAS 2006)



- Popp and Mangard gave the following **estimations**
  - Area overhead = 4,76 time more eq. gate
  - Power consumption overhead = 17,43 time more
  - Speed = 0,59 time less

Outlines

- The DPA context, how to practice, how to protect …
- **A short survey of DPA countermeasures**
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ **Synthesis**
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- Conclusion

Synthesis ...

LEVEL OF ACTION	NAME	CONCEPTS	MAINS SECURITY SENSIBILITY	REMARKS	AREA OVERHEAD	FREQUENCY OVERHEAD	POWER CONSUMPTION OVERHEAD
ALGORITHM	Masqued SBox	Use an algorithmic random mask (additive and multiplicative)	HODPA Glitches	Cipher modification Need a TRNG	+60 % Canright2008	-11 % Canright2008	Probably low overhead
SYSTEM	CMG	Power consumption maximally smoothing	DPA	SiP design	Depends of the capacitor size	~0	Very high!
ARCHITECTURE		Add a power consumption noise to the cipher power consumption	DPA	Very simple, can be an auto-protection	Null	Null	Null
LOGIC	SABL	Dual Rail Precharge	Glitches Capacity mismatch	Custom Logic (ASIC)	+180 % Tiri2002	?	190 % Tiri2002
	WDDL	Dual Rail Precharge	Glitches Routing mismatch	Standard Cell (ASIC & FPGA)	+310 % Tiri2005	?	+370 % Tiri2005
	MDPL	Masked Dual rail Precharge	Glitches Routing mismatch	Standard Cell (ASIC & FPGA)	+476 % Popp2005	-59 % Popp2005	+1 743 % Popp2005

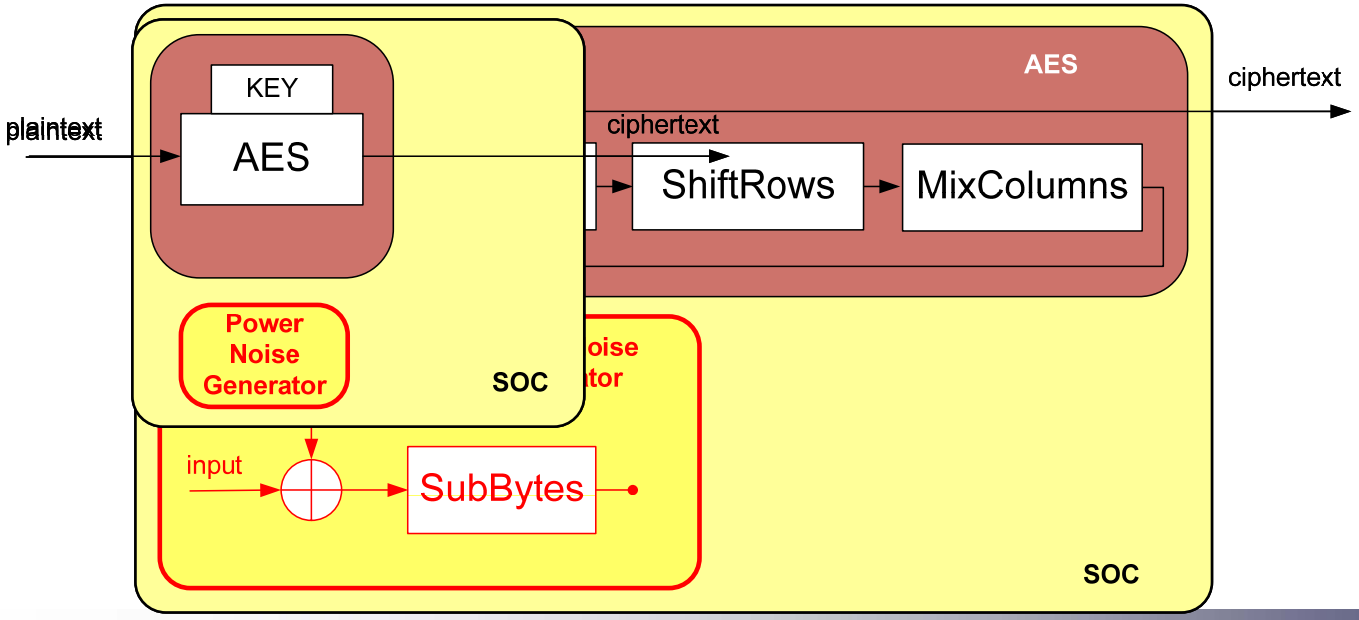
Outlines

- The DPA context, how to practice, how to protect …
- A short survey of DPA countermeasures
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- **Proposition of a new hardware countermeasure**
- FPGA Implementation results
- Conclusion

Addressing the architecture level …

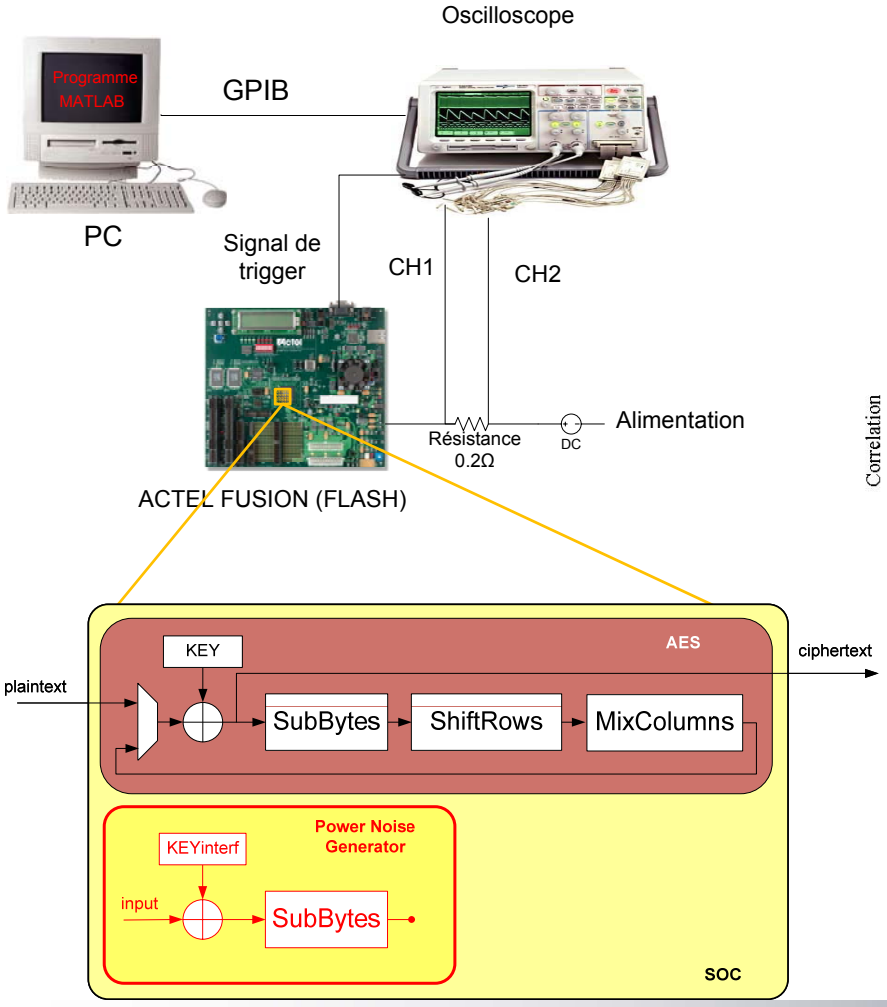
- Like the previous synthesis has showmen, architecture countermeasures are
  - ➔ The lowest area consuming
  - ➔ The lowest power consuming
  - ➔ Not DPA EFFICIENT !!!

- First idea : investigate the Standaert proposition
  - ➔ Make noise with AES component …
  - ➔ Sbox is no-linear and DPA targeting

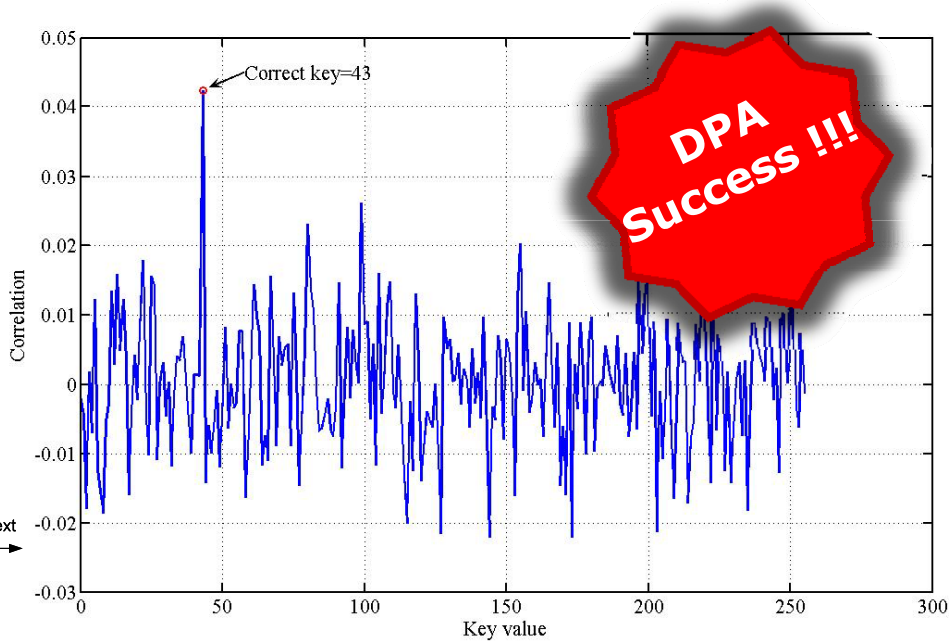


DPA test ?

- We have tested this countermeasure with CPA method



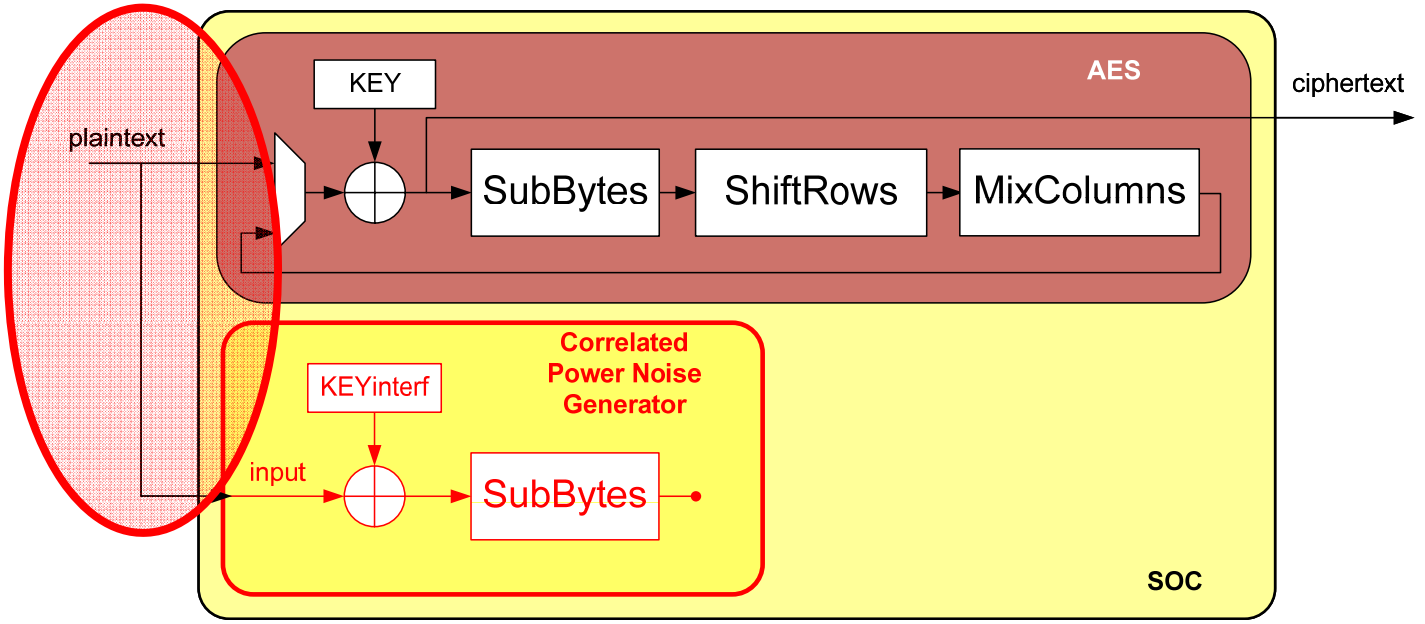
- CPA results with 12 000 power traces



- The averaging in DPA filters out **uncorrelated** noise from the differential power trace

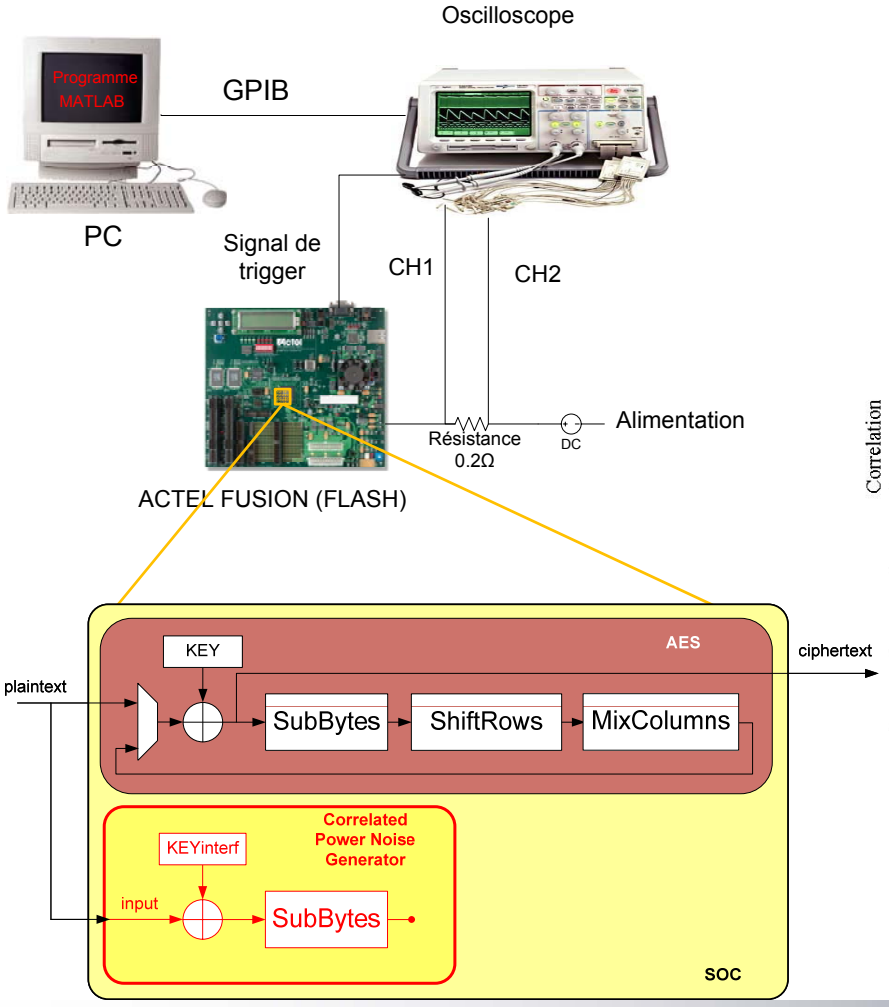
A new DPA countermeasure

- New idea : Add a **correlated** power noise
  - ➔ Use the same inputs for the AES core and the Power noise generator

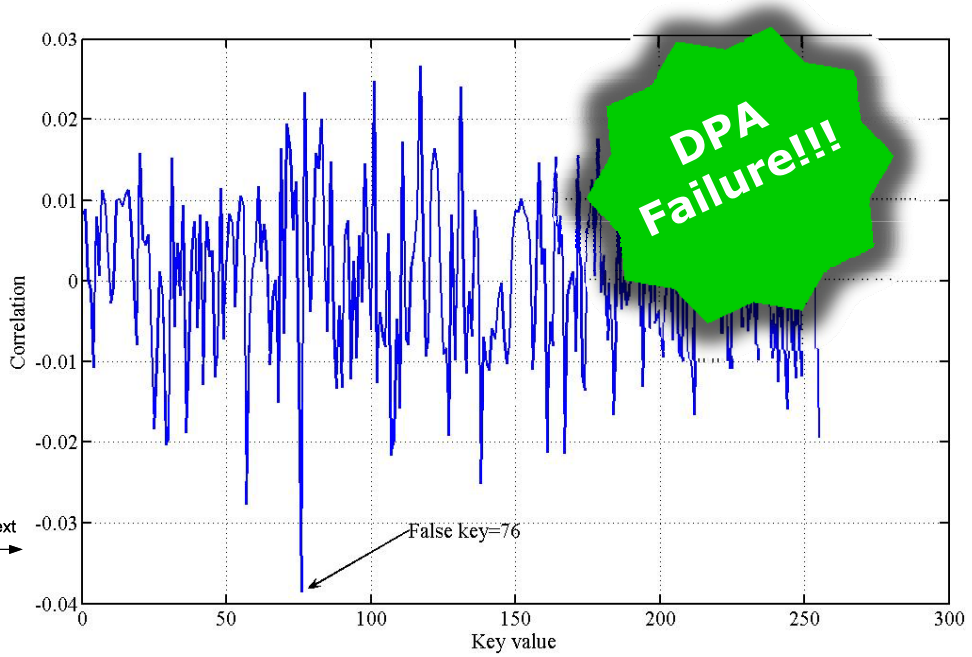


DPA test ?

- We have tested this countermeasure with CPA method



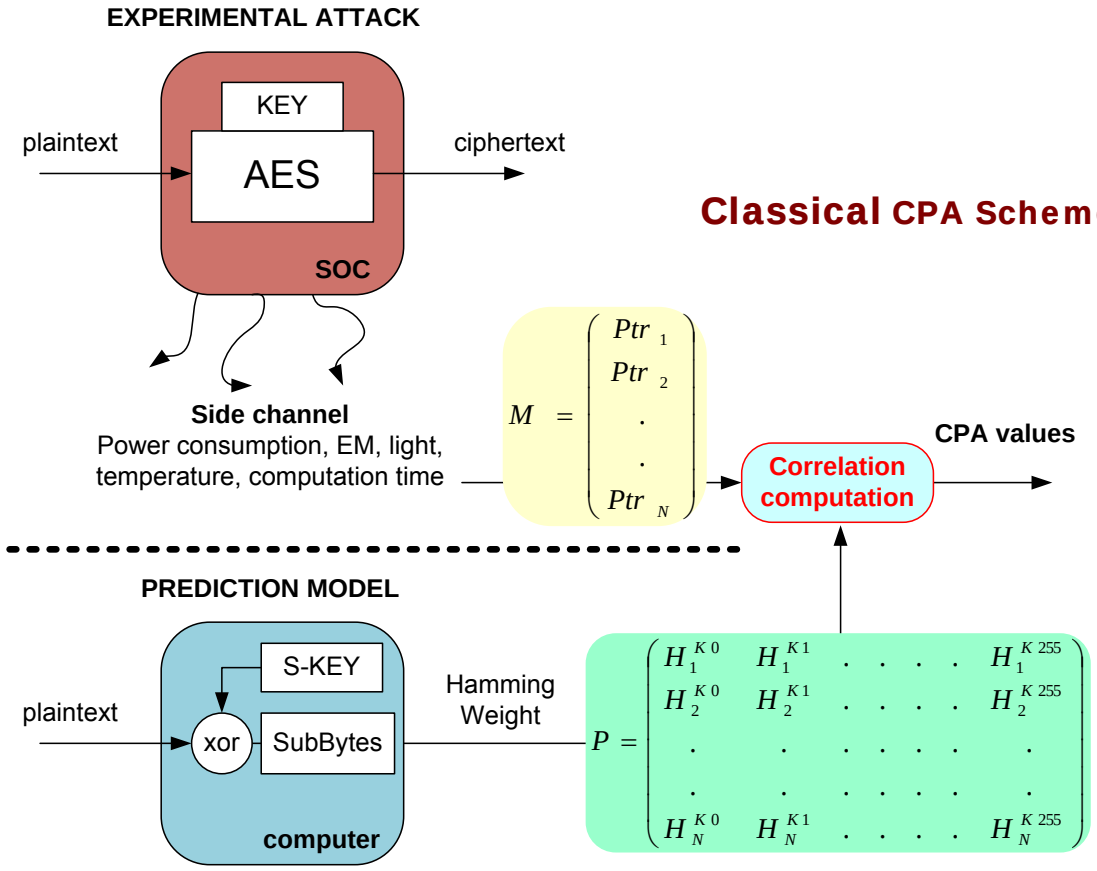
- CPA results with 100 000 power traces



- It is not possible with the power model use in the DPA attacks to filter out the correlated power noise

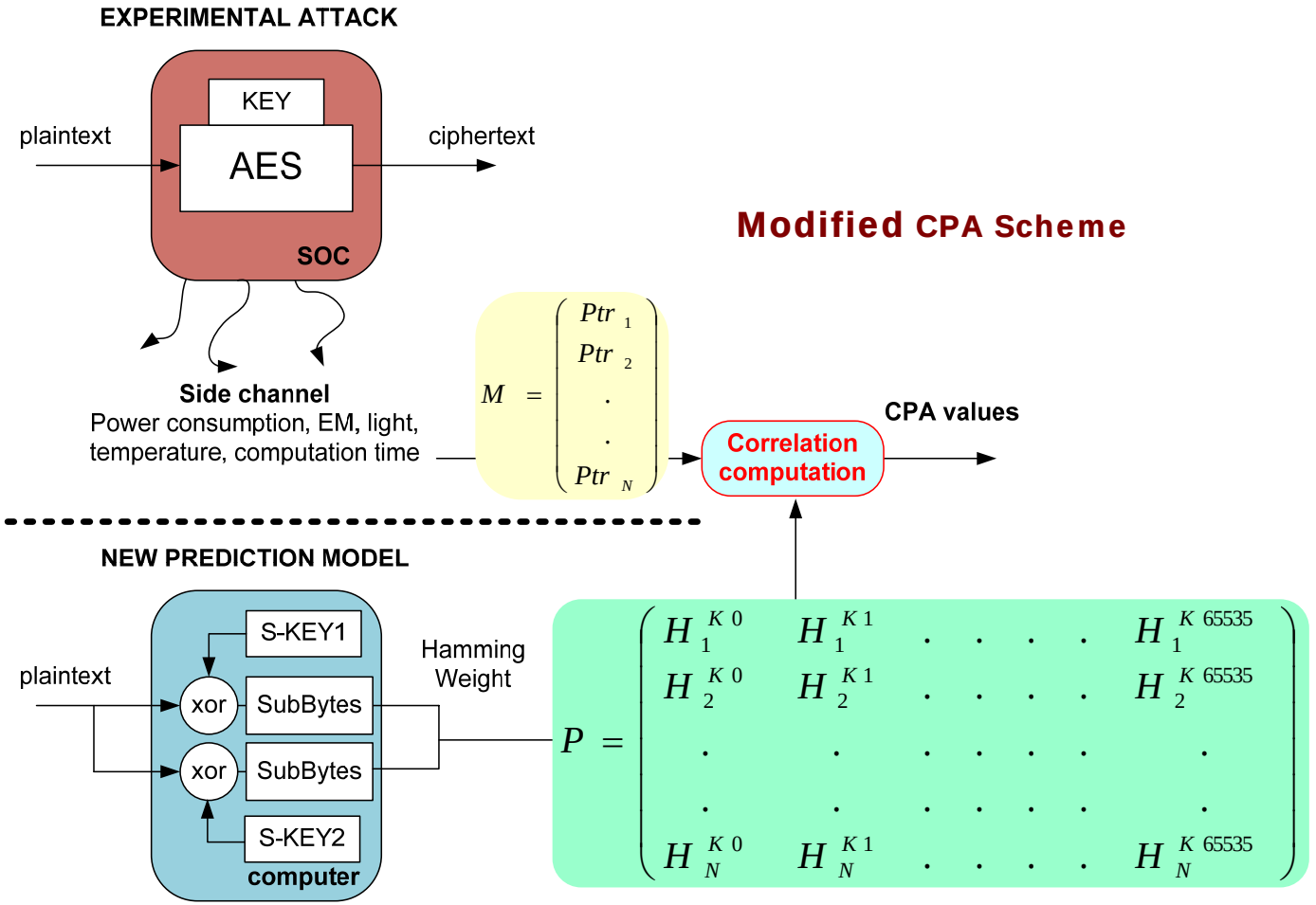
How to attacks this design ?

- DPA failures with our design because now the DPA power model is wrong !
  - ➔ Is the attacker perform an intrusive physical attacks, he can understand the modified AES architecture with the correlated power noise



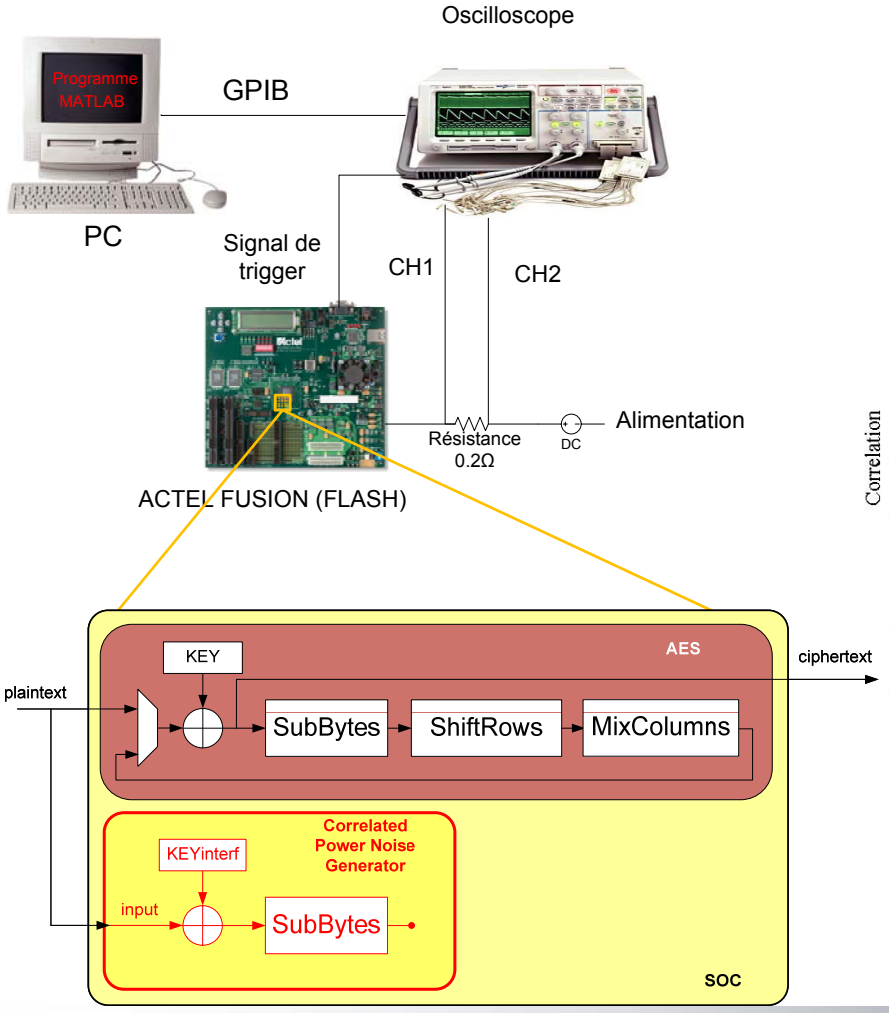
How to attacks this design ?

- DPA failures with our design because now the DPA power model is wrong !
  - ➔ Is the attacker perform an intrusive physical attacks, he can understand the modified AES architecture with the correlated power noise

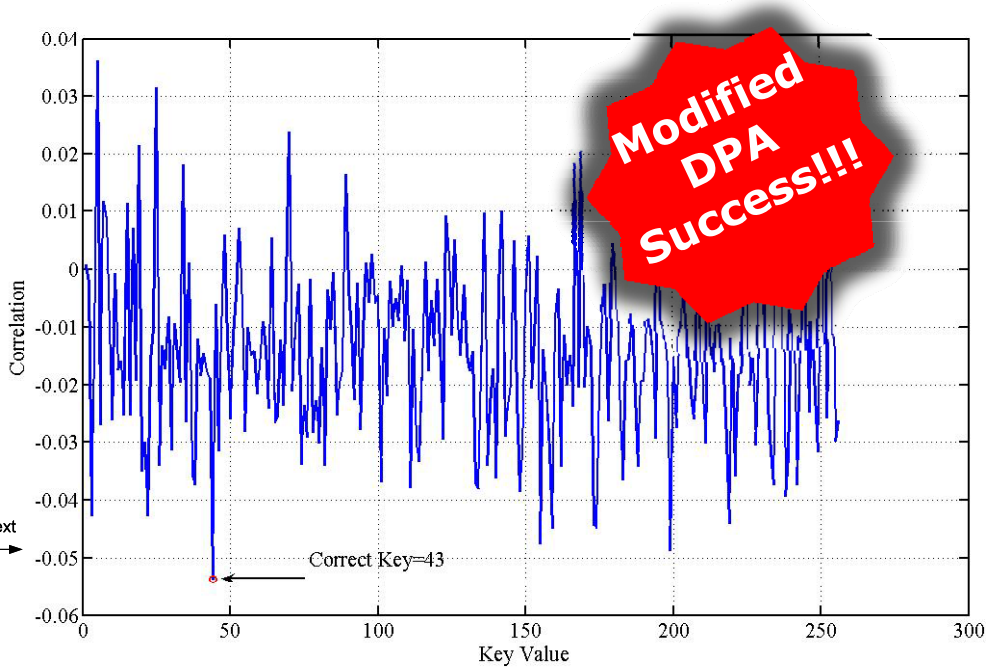


Modified DPA test ?

- We have tested this countermeasure with modified CPA method



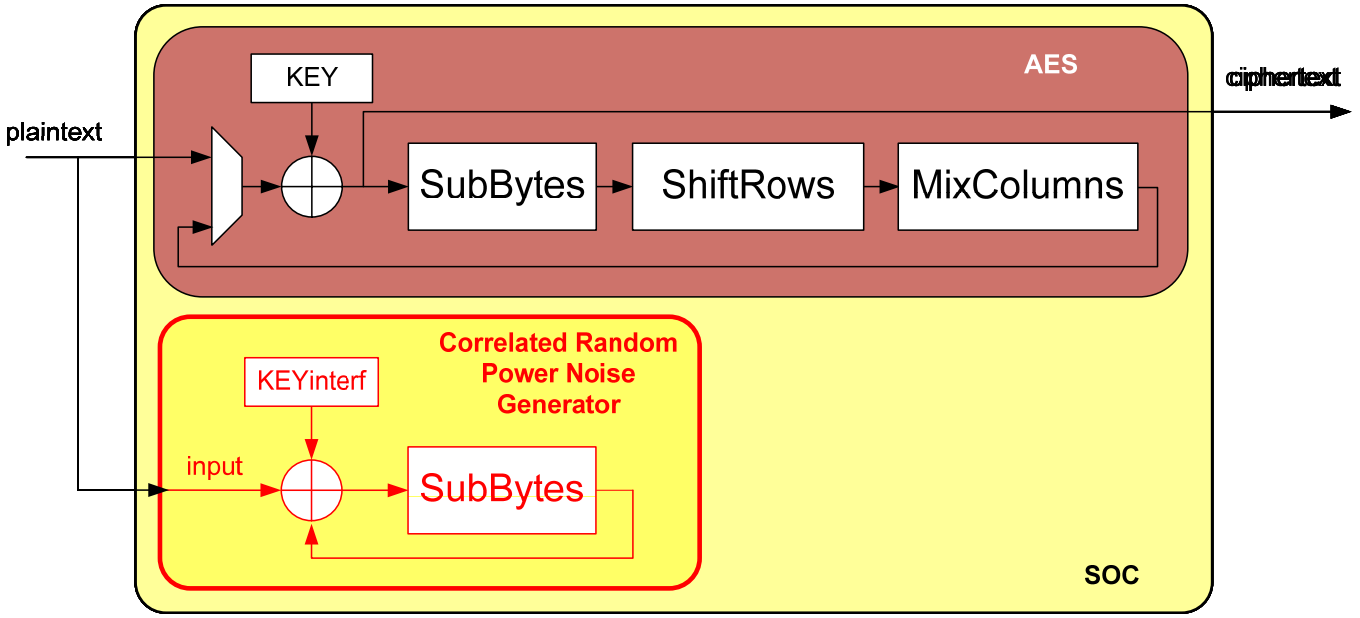
- CPA results with 12 000 power traces



- We have to improve the countermeasure

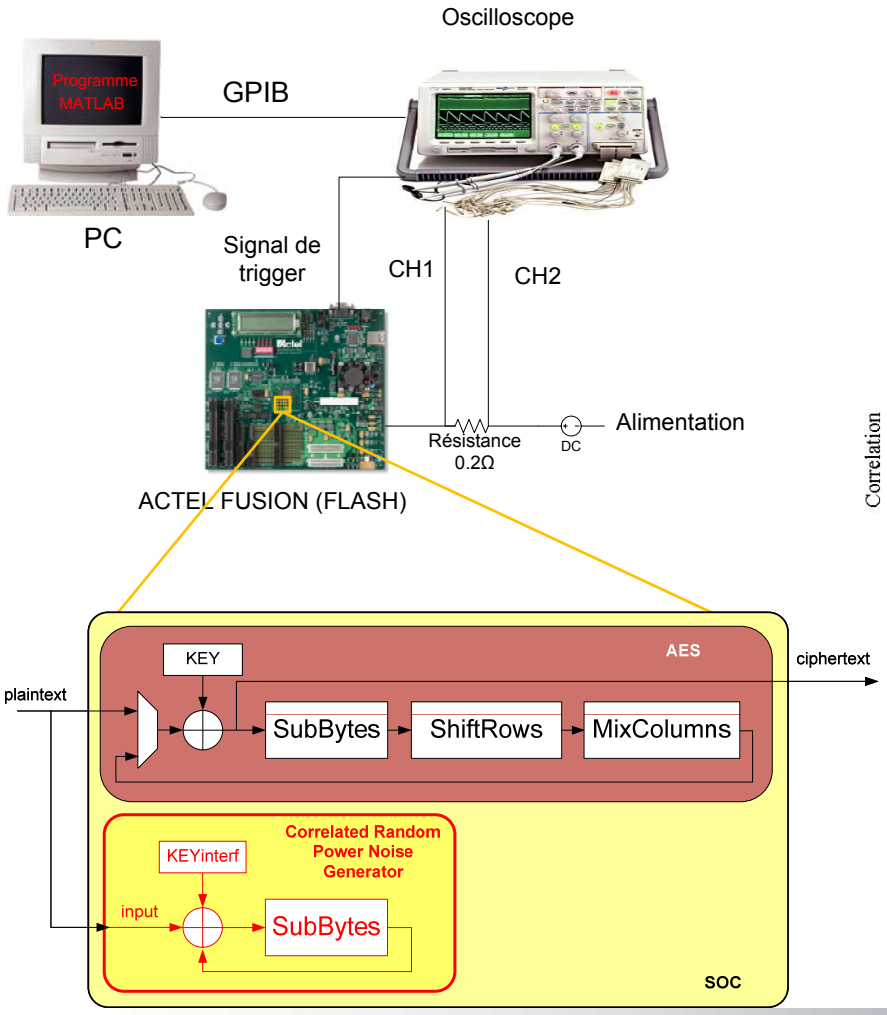
Countermeasure improvement

- To avoid modified DPA we need to add random noise
  - ➔ Use a TRNG

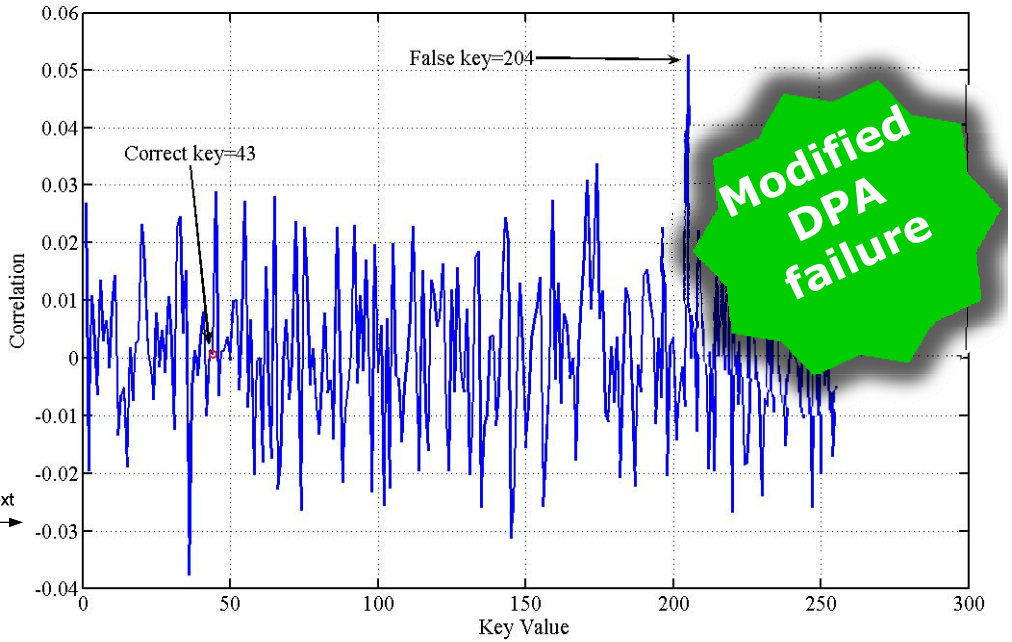


Modified DPA test ?

- We have tested this simulated countermeasure (without TRNG) with modified CPA method



- CPA results with 100 000 power traces



Outlines

- The DPA context, how to practice, how to protect …
- A short survey of DPA countermeasures
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- **FPGA Implementation results**
- Conclusion

FPGA implementation results

- To compare our proposed countermeasure we have implemented a very low are cost masked Sbox witch work in GF(2)
  - ➔ Proposed by Canright and Batina. in ACNS 2008.

- We give the following results with Xilinx Virtex 4 SRAM FPGA (without TRNG)

Performance AES (16 S-Box)	Area (#V4-slices)	Area Overhead	Frequency (MHz)	Speed Overhead
Unsecure	1424		143	
Masked (Canright 08)	2281	+ 60 %	97	-32 %
Proposed solution	1491	**< 5 %**	143	**0 %**

A new synthesis ...

LEVEL OF ACTION	NAME	CONCEPTS	MAINS SECURITY SENSIBILITY	REMARKS	AREA OVERHEAD	FREQUENCY OVERHEAD	POWER CONSUMPTION OVERHEAD
ALGORITHM	Masqued SBox	Use an algorithmic random mask (additive and multiplicative)	HODPA Glitches	Cipher modification Need a TRNG	+60 % Canright2008	-11 % Canright2008	Probably low overhead
SYSTEM	CMG	Power consumption maximally smoothing	DPA	SiP design	Depends of the capacitor size	~0 %	Very high!
ARCHITECTURE		Correlated random power consumption noise	???	Very low cost	< 5 %	0 %	Probably very low overhead (?)
LOGIC	SABL	Dual Rail Precharge	Glitches Capacity mismatch	Custom Logic (ASIC)	+180 % Tiri2002	?	190 % Tiri2002
	WDDL	Dual Rail Precharge	Glitches Routing mismatch	Standard Cell (ASIC & FPGA)	+310 % [Tiri2005]	?	+370 % Tiri2005
	MDPL	Masked Dual rail Precharge	Glitches Routing mismatch	Standard Cell (ASIC & FPGA)	+476 % [Popp2005]	-59 % [Popp2005]	+1 743 % Popp2005

Outlines

- The DPA context, how to practice, how to protect …
- A short survey of DPA countermeasures
  - ➔ Make a power noise
  - ➔ Use an algorithmic mask to reduce the correlation between the data and the power consumption
  - ➔ Maximization smoothing of the power consumption signal
  - ➔ Counterbalance the logic gate output switching
  - ➔ Synthesis
- Proposition of a new hardware countermeasure
- FPGA Implementation results
- **Conclusion**

Conclusion

- We propose a new very low cost DPA countermeasure
  - ➔ It uses a Correlated Random Power Consumption Noise Generator
  - ➔ Today, probably the lower cost DPA countermeasure : only 5 % of AES area overhead
- Nevertheless we need complementary investigations …
  - ➔ What is our countermeasure resistance against HODPA, glitches etc …
  - ➔ What is our countermeasure power consumption overhead with usual benchmarks?
  - ➔ Interference key generator cost with TRNG?
- To improve security aspect?
  - ➔ Adaptation to others cipher?
  - ➔ Protection against fault injection?
  - ➔ Include several countermeasure in a same time?

A very low cost DPA countermeasure to secure hardware AES cipher

lilian.bossuet@ims-bordeaux.fr