

A Countermeasure Against Power Analysis Attacks for FSR-Based Stream Ciphers

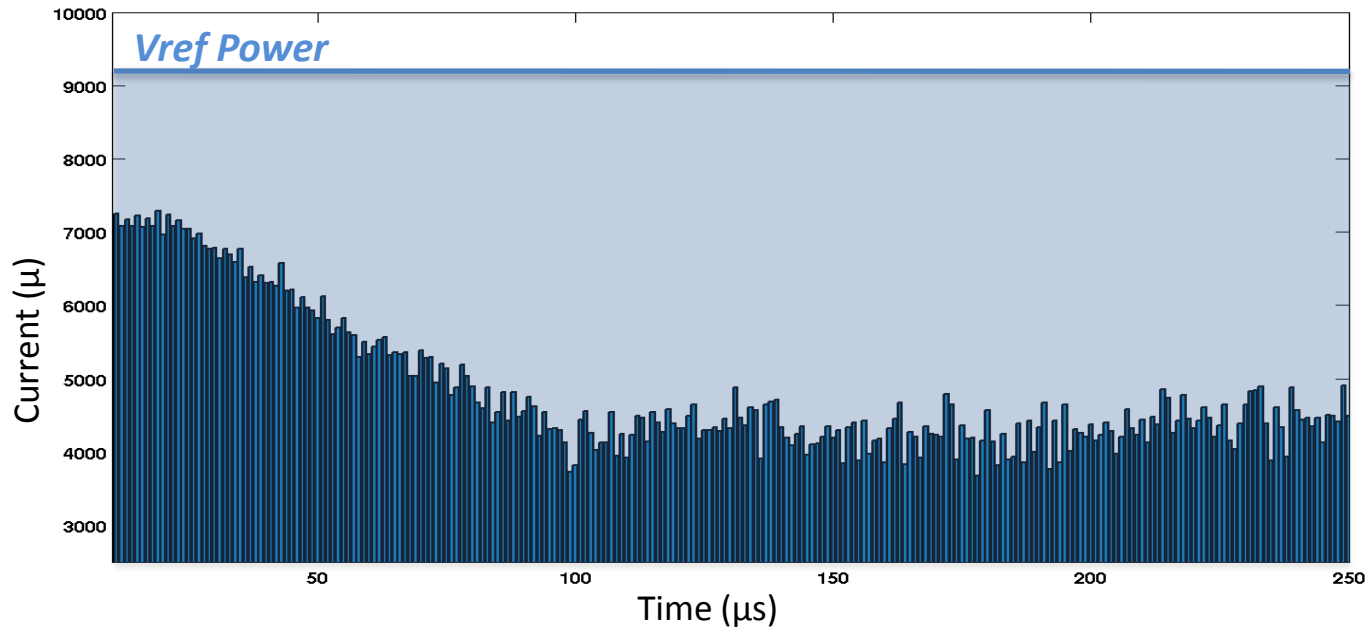
Shohreh Sharif Mansouri and Elena Dubrova
Department of Electronic Systems, School of ICT,
KTH - Royal Institute of Technology, Stockholm
Email:{shsm,dubrova}@kth.se

The Main Goal

- Protecting stream ciphers against side channel attacks.
- A side channel attack is an attack on the physical implementation of a cryptosystem.
- Power consumption is one of the physical characteristics of a system which can be used as a source of information to reveal its structure (Differential Power Analysis).
- In DPA attack an observer records a large number of power traces while the device encrypts or decrypts data.

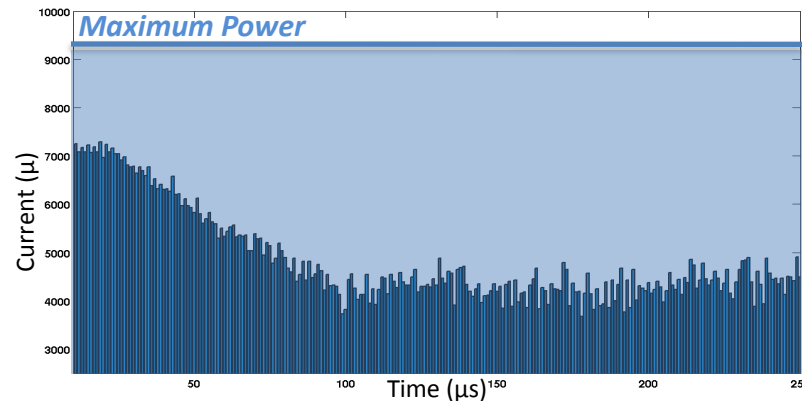
Typical Solution

- Masking the power variations by pushing the current consumption always to a constant value (maximum).

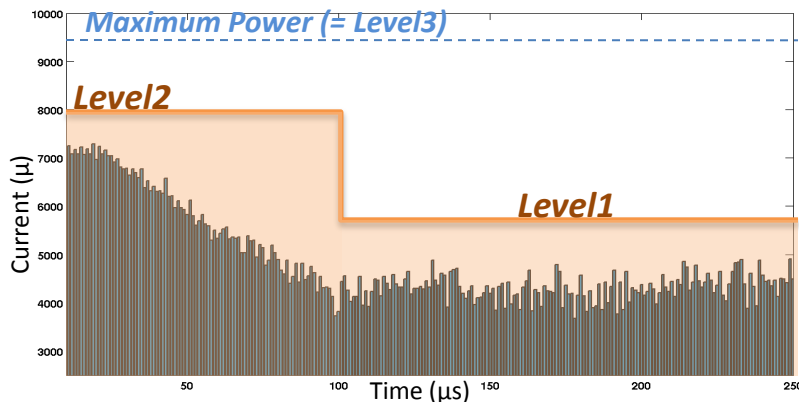


Our Idea

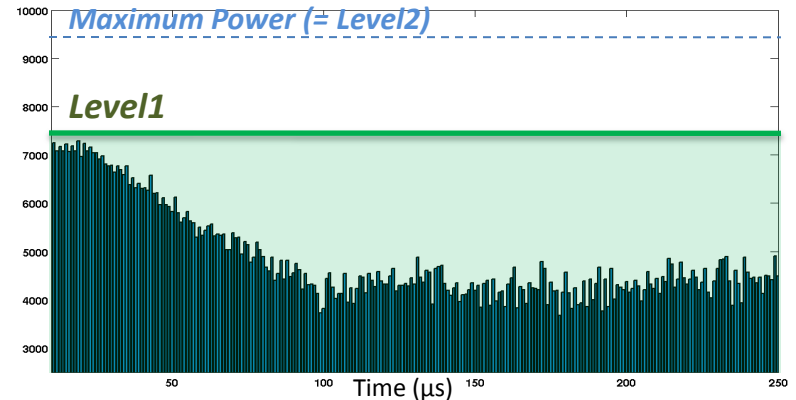
- We mask the power in 2 or 3 different levels by defining the current level of the cipher based on the switching activity of its FSRs.
- We have lower power overhead compared to other methods.



Protected Grain-80 with 1 power level



Protected Grain-80 with 3 power levels

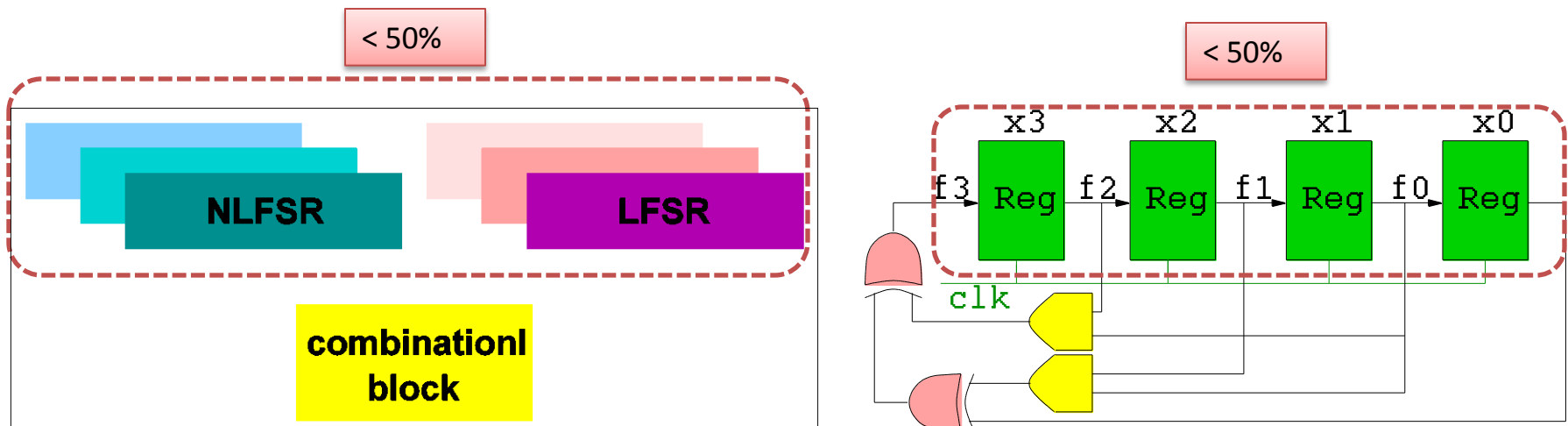


Protected Grain-80 with 2 power levels

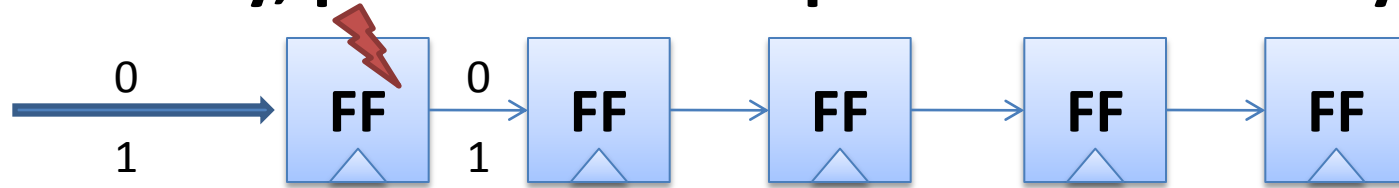
Stream Cipher Architecture

- The FSRs take more than 50% of the total area and power of the cipher.
- FSR hardware contains
 - Sequential blocks (shift registers)
 - Combinational blocks (feedback function)
- Sequential blocks take more than 50% of the total area of FSRs.
- Therefore :
 - Cipher total power \approx FSRs power consumption \approx FSRs Switching activity

FSRs Switching activity \approx cipher total power

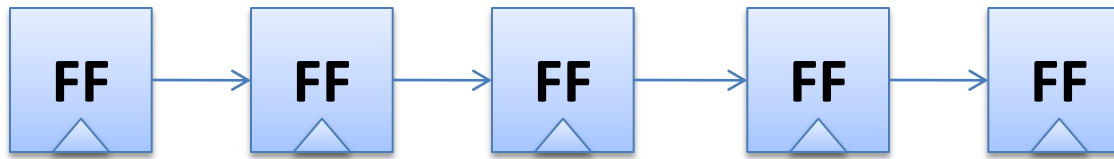


Relation between FSR internal values, switching activity, power consumption and security



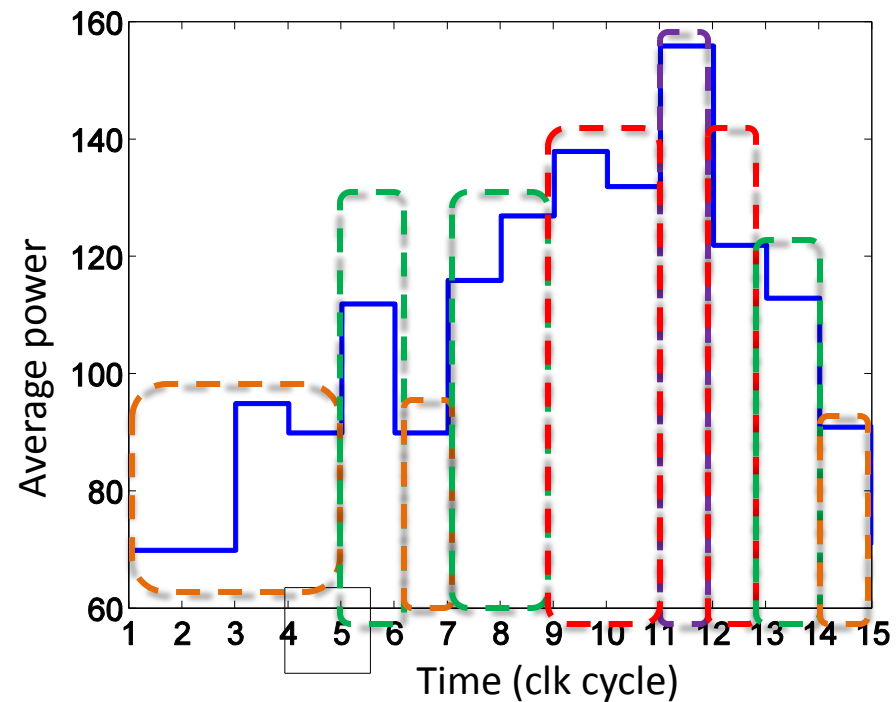
Initial value (Key with switch activity 0)	1	1	1	1	1
Switching activity = 1	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
Switching activity = 2	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
Switching activity = 3	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
Switching activity = 4	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
Switching activity = 5 (the only case)	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Average power consumption of a 5 bits FSR in each clock cycle.



internal value Switch activity

01111	1
00111	1
00011	1
00001	1
10000	2
11000	1
01100	2
00110	2
10011	3
01001	3
10100	4
11010	3
11101	3
11110	2
11111	1



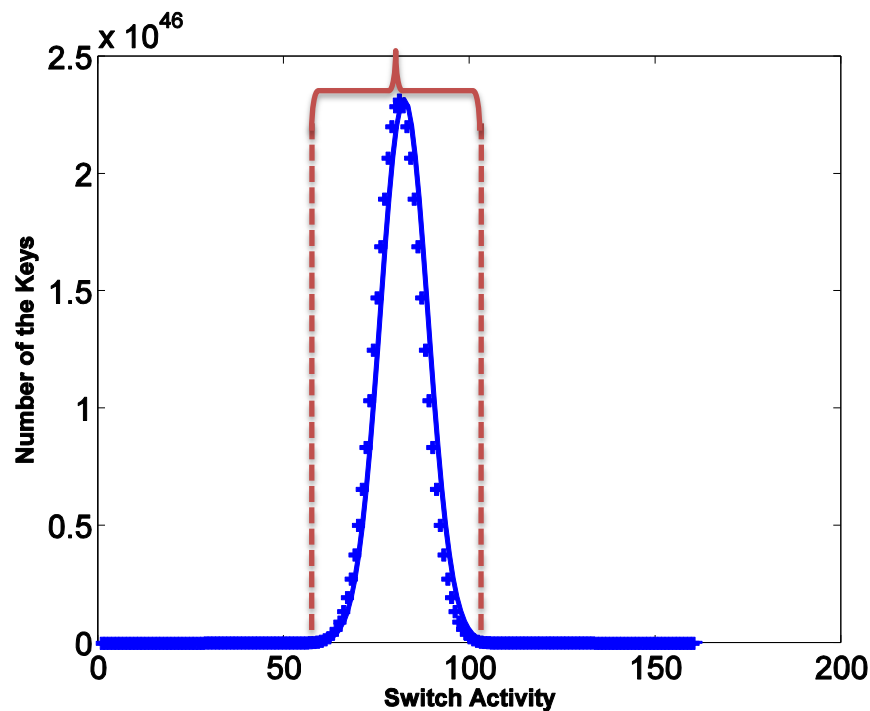
Switch = 4 Switch = 3
 Switch = 2 Switch = 1

Keys and Switching Activity

- In n bits FSR, the number of cases with switching activity i is equal to binomial coefficients of i out of n

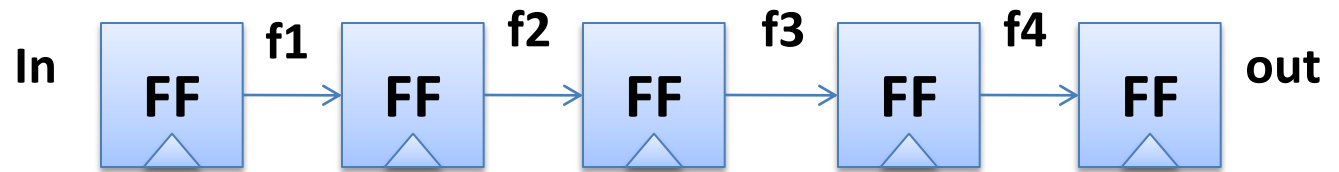
$$\binom{n}{i} = \frac{n!}{i! \times (n - i)!}, \quad 0 < i < n$$

90% of the keys have switching activity between 50 and 100. Therefore they have a same range of power.



160 bit FSR

- In each clock cycle, the switching activity of the FSR can:



	In	f1	f2	f3	f4	out	status	switching	time
	1	1	1	1	1	-	-	0	<i>initial</i>
increase by one	→ 0	1	1	1	1	1	+1	1	t1
remain constant	→ 0	0	1	1	1	1	No change	1	t2
decrease by one	→ 1	1	1	0	0	1	-1	2-1=1	t5
remain constant	→ 1	0	1	1	1	0	No change	1	t7
							(+1-1)		

Relation between switching activity and total power in 160 and 256-bits FSRs.

FSR	Property	3 Level			2 Level	
		L1	L2	L3 (Max)	L1	L2 (Max)
160 bits	# state	50%	49%	1%	98%	2%
	Power (PL/Pmax)	65%	83%	100%	74%	100%
256 bits	# state	50%	50%	~0%	99%	1%
	Power (PL/Pmax)	64%	75%	100%	70%	100%

Power Masking Algorithm and Implementation

Our design contains analog and digital blocks:

❑ Digital Blocks:

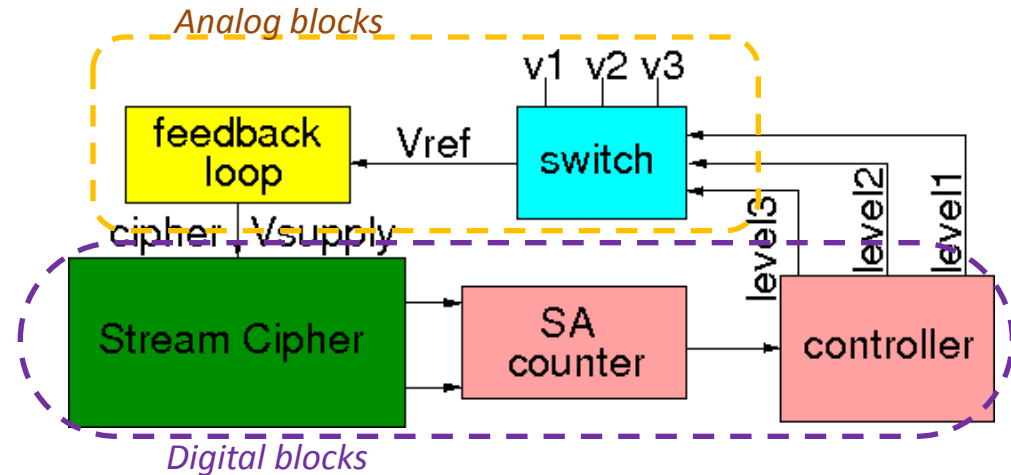
- It keeps track of the switching activity in cipher.
- we use an adder-subtractor which counts the series of 1,0 or 0,1 in the FSRs.

❑ Suppression Circuit*:

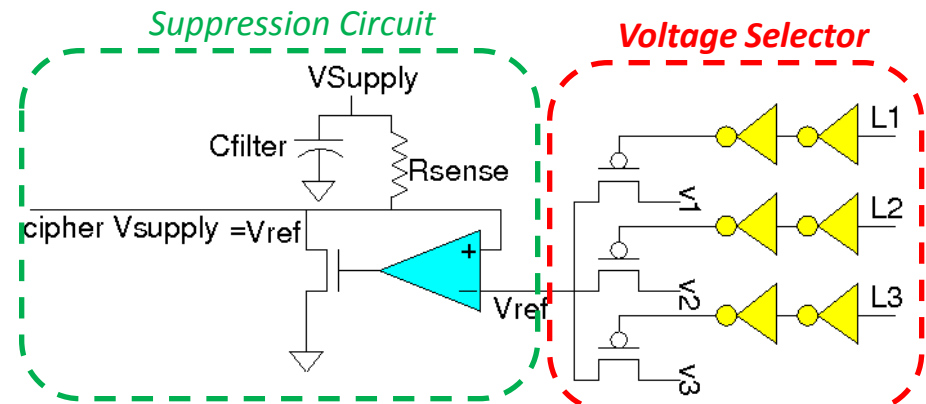
- It is based on a feedback loop made of a shunt transistor and an operational amplifier.

❑ Voltage Selector:

- It receives three input signals from the digital blocks. The active signal corresponds to the appropriate voltage which is necessary as V_{ref} to guarantee that the correct current is shunted.



Schematic diagram of the suggested countermeasure.

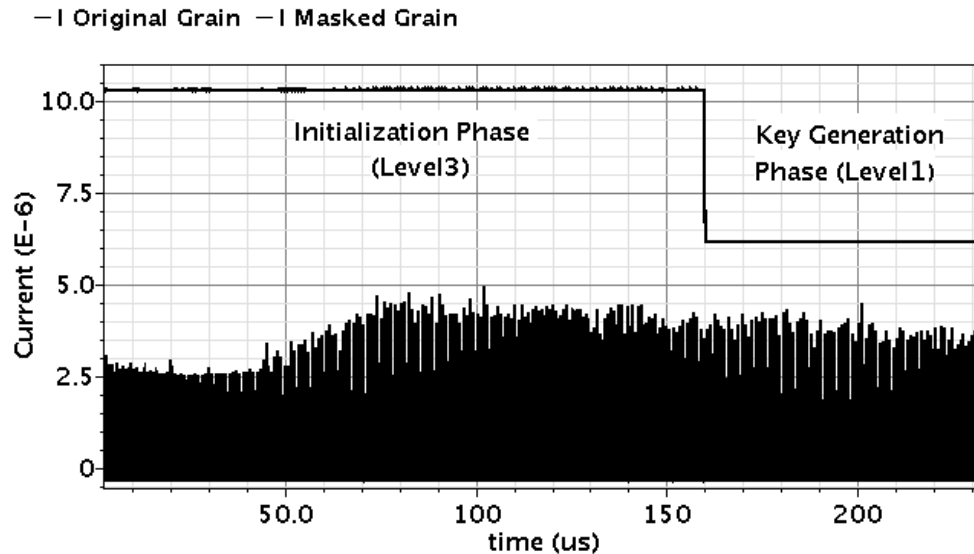


Analog block containing the voltage selector and the suppression circuit*.

*G. B. Ratanpal and et Al., "An on-chip signal suppression countermeasure to power analysis attacks," TDSC 2004.

A SPICE Simulation

- A SPICE simulation of the current pattern of Grain-80 using our countermeasure.
- The cipher always has switching activity lower than 60. Therefore, after the initialization phase is completed at time 160 μs , the cipher switches to Level 1 and the current consumption decreases by 31%.



Experimental Results

Improvement compared to Protected Grain with only one power level:

- Grain- 80

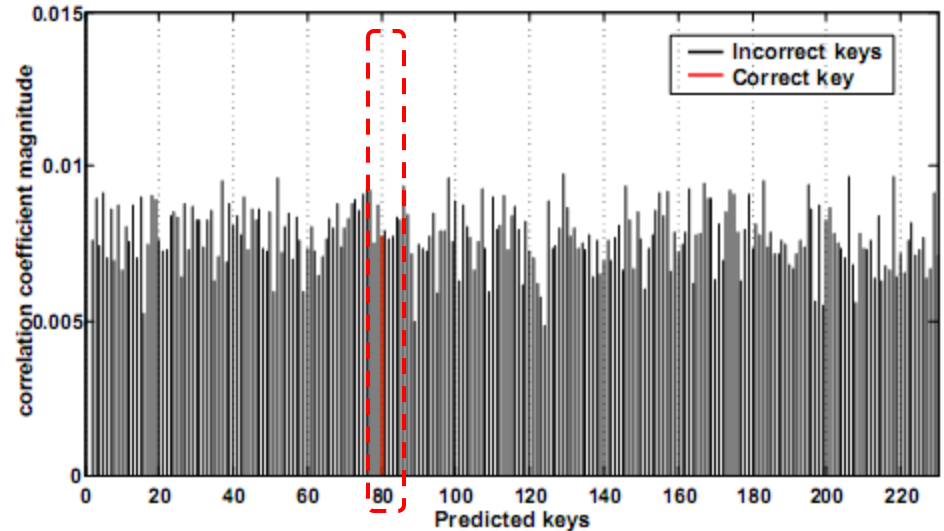
- Average power improvement : 20%
- Maximum power improvement : 31%
- Area overhead (the comparison is done only between digital blocks): 16%

- Grain- 128

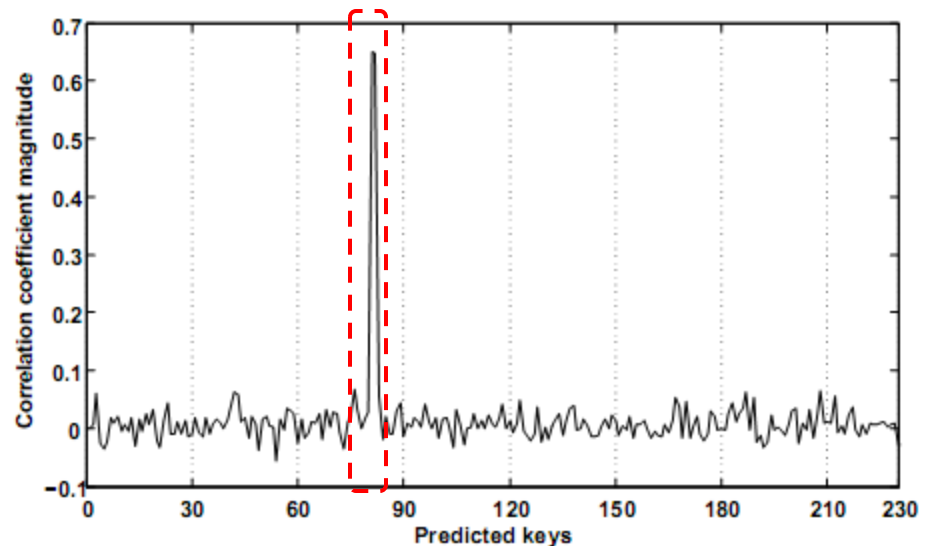
- Average power improvement : 25%
- Maximum power improvement : 35%
- Area overhead: 14%

Security Considerations

Correlation coefficients of the 230 guessed keys on 2-levels protected Grain-80 after 1M encryptions.



Correlation coefficients of the 230 guessed keys on unprotected Grain-80 after 5k encryptions.



Security Considerations

Grain-80	Levels	Measurements To Disclosure (MTD)
Unprotected	$L1 \geq 0$	188
Protected with two power level	$L1 < 110$ $L2 > 110$	> 1M
Protected with three power level	$L1 < 81$ $80 < L2 < 128$ $L3 > 129$	556
	$L1 < 64$ $65 < L2 < 128$ $L3 > 129$	8k

Conclusion

- We masked the power in different power levels
- Hardware:
 - For Grain-80: Average power improvement : 20%
 - For Grain-128: Average power improvement : 25%
- Security :
 - Grain-80 with three power levels has MTD equal to 556.
 - Grain-80 with two power levels has MTD higher than 1M.

How does the switching activity change during operation?

- For Grain-80, in average the switching activity increases by 33 while the cipher produces 10k bits data.

