Static Power Research on Nano Cryptographic Circuits

Neetu Srivastava, Kumar Neeraj, B.Hemalatha Hari, Shanker Srivastava

Abstract— In this present static power analysis of Nano circuit is presented. The attack is bused to obtain the secret key of a cryptographic core by measuring static power loss. These attack take leakage current from the integrated circuit depends upon input to extract secrete key called as Leakage Power Analysis (LPA) Since the leakage power expands a lot quicker than the dynamic power at each new innovation age, LPA assaults are a genuine risk to the data security of cryptographic circuits in sub-100-nm advancements. In this paper a leakage power attack is well demonstrated and simulated on different integrated circuits and an analytical model of LPA attack is presented to understand the effectiveness of this technique as a threat to cryptographic integrated circuits . The effect of innovation scaling is expressly tended to by methods for a straightforward analytical model and Monte Carlo simulation. Simulation on a 45nm, 65-and 90-nm technology and trial-experimental results are introduced to legitimize the suppositions and approve the leakage power models

1. INTRODUCTION

POWER analysis attacks have been widely appeared to be a noteworthy danger to the security of information that are prepared what's more, put away in cryptographic gadgets, for example, Smart Cards [1]–[4]. These attacks misuse the coorelation with input and the dynamic power on the contributions of a cryptographic calculation, i.e., the input cipher text (plaintext) that will be decoded (encoded) what's more, the secret key. The expense as far as hardware and computational exertion are fairly low; thus, these attack can be effectively performed [4].

In the power analysis attack the known input bit sequence is applied to circuit and respective instantaneous power is measured during encryption and decryption and will be stored.

After that post processed technique are applied to obtain the secret key from power analysis, which is stored internally in cryptographic circuit, which is used during encryption/decryption phase. Among the existing post processing technique, the correlation power analysis(CPA) is a simple and very effective to create a power model which is adopted to analyze the signal generated inside cryptographic chip. Which is a function of input and secret keys[5].

Then a small fraction of secret keys guess and calculated. The static power in circuit and then measured and calculated. static power on correlated with known correlation model to find out correlation coefficient between the calculated and measured. If correlation is good then the secret key is protected , matched means. we guess the secret key. In nm technology ,the static power is more dominant to dynamic power to the total chip power budget [6]-[9]. and it's strength goes on increasing with scaling of technology e.g. 65nm leakage power is approx half of total power. which goes on increasing with technology advancement. According to international technology of semiconductor industry.[9]

Due to strong dependency of leakage current on input bit sequence in digital electronics circuits. This leakage current provide very useful information about secret key. This was first discussed by [5], that leakage depend upon processed data is first given by [10]. This technique was first applied by [11] on crypto core for analysis of CPA [12]. Similarly a DPA(differential power analysis technique) when adopted as by[12] to simulate the circuit to obtain secret key. All the about paper represent only simulated results. With consider any physical coefficient of temperature as process variation.

In this paper LPA attack is modeled and compare with real scenario in systematic manner. Problem related to LPA attack will discuss to better evaluate the functionality of LPA under standard assumption. The paper is organized as Sec II The leakage in MOS device and simulation of standard logic gate to analyze static power depend on input. Sec III approach to LPA attack and its setup will be discuss and the practical measurement of LPA attack is performed and analyzed. sec IV deals with simulation result and comparison.

II Leakage source of Nano CMOS circuits.

The major cause of leakage in MOS transistor is due to sub threshold region, gate tunnel & inverse junction[13].

$$I_{leakage}\ of\ MOS = I_0 \left(\frac{W}{L}\right) e^{-V_{th}/nkT/q}$$

In above to all three the sub threshold current is more dominant when came to leakage to CMOS. Above equation indicate that leakage is very sensitive to temperature and process variation in exponential manner.

II. Leakage in Static CMOS circuit

Leakage power statistics in basic logic gate and the bit sliced logic circuits. The basic CMOS circuit for analysis is choose as a inverter and NAND gate shown in figure 1 and are simulated in 90nm,65nm and 45nm technology and in

Revised Manuscript Received on July 10, 2019.

Neetu Srivastava, Anurag Group of Institution, Hyderabad India. (**e**-mail: neetuece@cvsr.ac.in)
Kumar neeraj, Anurag Group of Institution, Hyderabad India. (**e**-mail: Kumarneerajece@cvsr.ac.in)
B.Hemalatha Hari, Anurag Group of Institution, Hyderabad India. (**e**-mail : hemabandarii@gmail.co)
Shanker Srivastava, Anurag Group of Institution, Hyderabad India. (**e**-mail: harishankerece@cvsr.ac.in)

different temperature condition. From the table I,II and III it is observed that the leakage is more when input is low. The cause of this is due to lower threshold value of NMOS as compare to PMOS.

Some realistic result we will get when, we have tested the that cryptographic chip delay on different technology of 45nm, 65nm & 90nm.Similarly the leakage is NAND gate is more if one input is fixed at a logic and other change from 0 to 1, at 0 we will get more static power loss(same as inverter circuit).

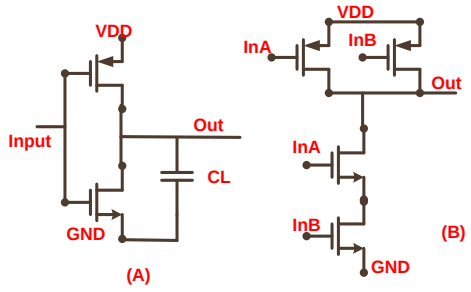


Fig 1 (A) Schematic of the CMOS inverter (B) CMOS NAND

TABLE 1

Leakage Current (nA) in various CMOS Logic gates 90nm

Inverter Gate			
InA	$T=0^0C$	$T=25^0C$	$T=50^0C$
0	1.36	3.19	6.52
1	0.24	0.73	1.90
NAND Gate			
InA	InB	$T=0^0C$	$T=25^0C$	$T=50^0C$
0	0	0.17	0.47	1.1
0	1	1.36	3.19	6.52
1	0	1.02	2.44	5.09
1	1	0.48	1.47	3.79

TABLE II

Leakage Current (nA) in various CMOS Logic gates 65 nm

Inverter Gate			
InA	$T=0^0C$	$T=25^0C$	$T=50^0C$
0	2.67	2.98	3.66
1	0.13	0.47	1.40
NAND Gate			
InA	InB	$T=0^0C$	$T=25^0C$	$T=50^0C$
0	0	2.37	2.45	2.59
0	1	2.65	2.98	3.66
1	0	2.52	2.77	3.29
1	1	0.26	0.94	2.81

TABLE III

Leakage Current (nA) in various CMOS Logic gates 45 nm

Inverter Gate			
InA	$T=0^0C$	$T=25^0C$	$T=50^0C$
0	2.89	2.67	2.94
1	.09	.32	1.14
NAND Gate			
InA	InB	$T=0^0C$	$T=25^0C$	$T=50^0C$
0	0	2.46	2.52	2.87
0	1	2.89	3.10	3.85
1	0	2.95	3.07	3.95
1	1	.19	.79	2.23

Leakage in Bit-Sliced Logic Circuit

In bit slice large circuits we found a strong leakage depends on input pattern ,this help us to under the behavior of complex circuit. In bit slice circuit, the overall leakage current is some of individual leakage for through value high value of leakage current (I_H) and for low input low value of leakage current (I_L) so, when we apply any bit steam in bit slice circuit.

$$I_{leakage,Total} = \frac{(No.of\ 1's)I_H}{Slice\ with\ bit\ high} + \frac{(No.of\ 0's)I_L}{Slice\ with\ low\ bit}$$

This expression can be written in the form of Hamming weight. As

$$I_{leakage,Total} = wI_H + (m-w)I_L$$

m = total no. of bits in slice circuit
w = no. of 1's in bit sequence.
(m-w) = no. of 0's in bit sequence.

$$I_{Total,leakage} = w(I_H - I_L) + mI_L$$

From above equation it is clear that leakage linearly depend on Hamming weight. From the above tables I,II and III it apparent that there is an approx linear relationship between leakage current and hamming weight's shown in figure 2.A experimental measurements is performed on 8 bit register. IC of family on ON Semiconductors MC74 series with different temperature value, so measurement were performed on the chip. The standard deviation for this 50 iteration of measurement of leakage is found very low indicates that, the measurement are reliable.

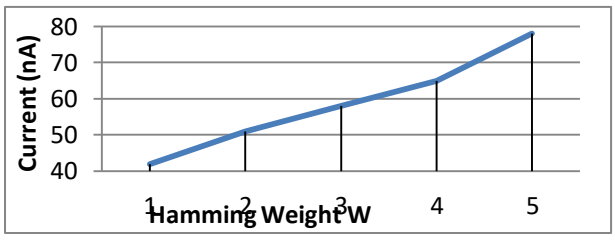


Fig 2 Simulated Leakage versus Hamming weight in 4-bit register at 27oC 65nm technology

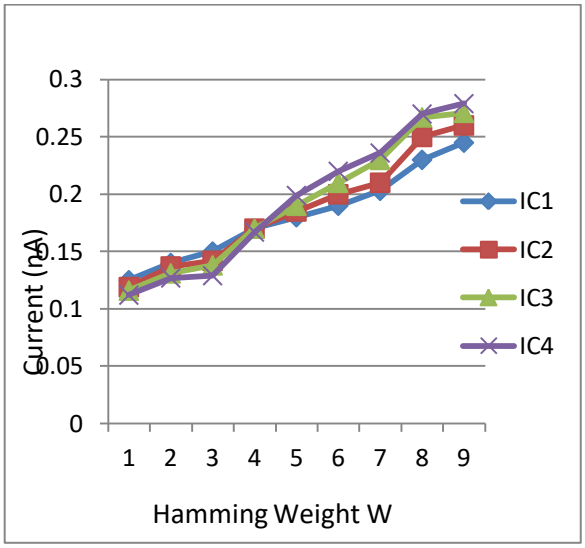


Fig 3. Measured leakage versus Hamming weight in an ON semiconductor 8-bit register for % different chips at 45°C

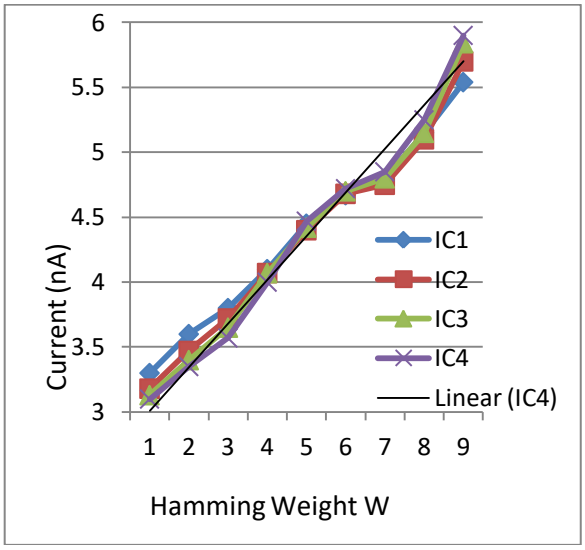


Fig4. Measured leakage versus Hamming weight in an ON semiconductor 8-bit register for % different chips at 75°C

TABLE III
Simulated Register Leakage for different input data value (45 nm technology at 27°C)

Input X	Hamming Weight w=H(X)	$I_{Leakage,TOT}$(nA)
0000	0	43.68
0001	1	50.19
0010		50.67
0100		50.65
1000		50.71
0011	2	58.61
0101		58.92
0110		58.78
1001		59.12
1010		58.76
1100		58.78
0111	3	69.39
1011		69.56
1101		69.71
1110		69.45
1111	4	79.30

2. LPA ATTACK & TEST RESULTS

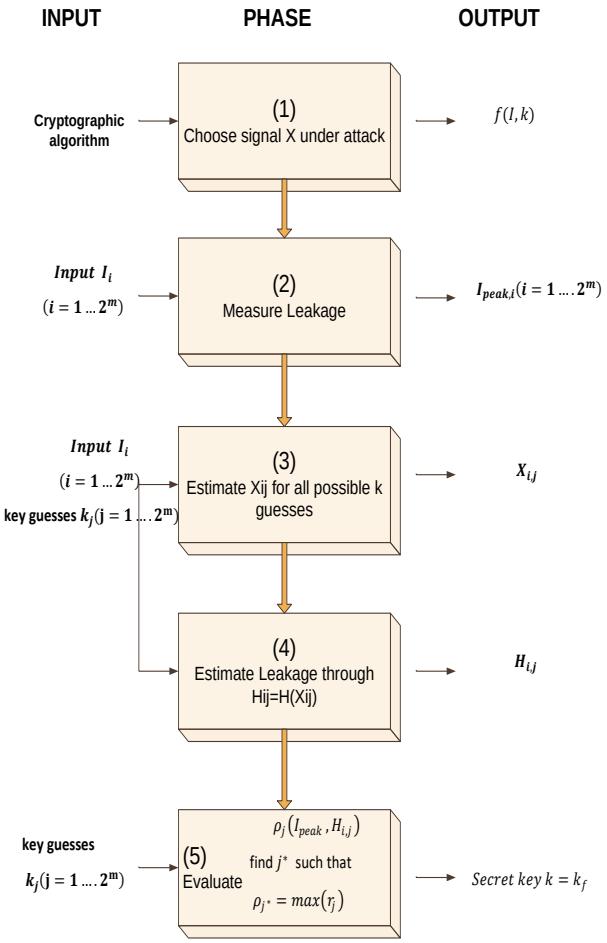


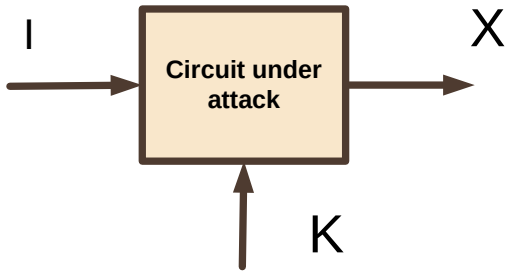
Fig5 . Leakage power attack procedure

As discuss above the leakage current weight of m bit data X which is processed in the block.

Hence the leakage will provided the useful information related to secret key of cryptographic device. What it is

process of data X.

In real circuit the process data X which is generated in block of function of input and secret key K.



It is not possible inside the block to access the power at each node, hence the adversary have to measure the overall chip leakage.

So overall chip leakage depend on hamming weight H(x).

$$I_{leakagr} \propto H(X)$$

where w= H(x)

X = signal under attack

H= Hamming operator

When apply a known input value the chip leakage and H(x) provide us a static correlation between them, explain in CPA attack[4][5]This similar power analysis attack process is used in LPA attack. The LPA attack procedure is shown in figure5.

1 Step : The adversary choose M bit signal to generate signal X, which is generated in the cryptographic circuit under attack. As

$$X = f(I, K)$$

where f= algorithm known to adversary.

K= secret key

I = input bit

2 Step: Adversary apply all 2^{nd} different input value I_i (from i=1.....2^m) and measure the reflected leakage current in cryptography chip. This will be only measurement adversary have known of clock.

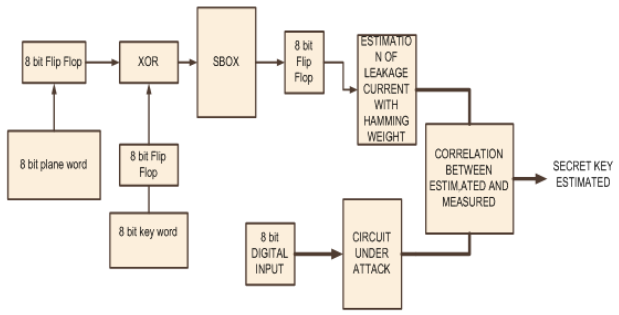


Fig 6 Working setup block Diagram for LPA

3 Step: The physical value X is obtained from

$$X = f(I, K)$$

and for different value of I_i which is known and with guess value of secret key k a 2-D array is obtain

$$X_{i,j} = (I_i K_j)$$

4 Step: Now as with $X_{i,j}$ with linear relation between leakage current is stimulated

$$H_{ij} = H(X_{ij})$$

i=1.....2^m , J=1.....2^{2m}

Now a 2D array of hamming weight of X is generated with input and secret keys.

5 Step: The measure leakage $I_{leakage,i}$ and estimated leakage H_{ij} are compare for given key guess K_i.

If the measured leakage $I_{leakage,i}$ and estimated H_{ij} leakage current have maximum correlation equal to one key guess is exact likely and if minimum correlation less than 0.2 we have to repeat it again. So $f(I_{leakage,i}, H_{ij})$ and all possible guess K_j must be high to ensure the correct guess of K_j so

$$\rho_{ij} = \rho(I_{peak}, H_{i,j})$$

Under condition of good correlation function must be used,[13]-[17].

Practical setup for LPA attack

The working setup diagram of the circuit description is shown in figure 6

1st step:- the signal under test are taken as XOR of I & K as,

$$X = f(I, K) = I\ (XOR)\ K$$

this technique is generally used in data encryption standard (DES) and Advanced standard for encryption (AES)

2nd step: The time of observation /calculation of leakage current must be less than the clock period of the circuit so that we can measure steady state current measure all the leakage current with different possible input combination which is used in S-BOX.

3rd & 4th step: With all possible input combination and key combination a 2D matrix is formed here of size 64 by 64 as

$$X_{i,j} = (I_i K_j)$$

now the with respect to $X_{i,j}$ equivalent hamming weight and its associated current is estimated with the help of S-table in S box as H_{ij}.

5th step: In this step we correlate the measured leakage current in step and estimated leakage current in step 4 "Spearman rank correlation" which is further extension to Pearson correlation function if the parameters are purely linear here we uses the coefficients and the process discussed in reference [17]. Simulation of circuit is done on cadence environment on 45 nm NCSU technology and then all comparison and correlation is performed on Microsoft excel 2007. Figure 7 shows correlation coefficient in a simulation attack.

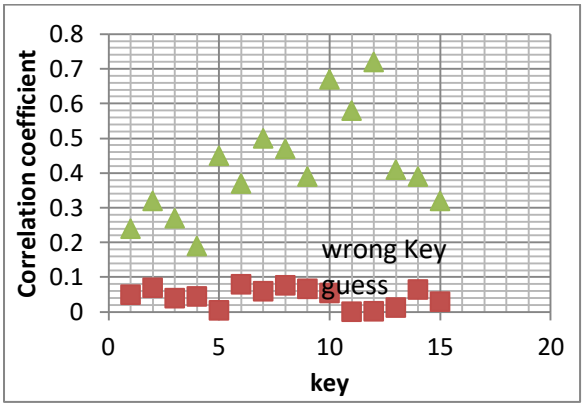


Fig 7 Correlation coefficient after simulation in leakage power attack

3. COMPARISON WITH REFERENCE {17}

The correlation comparison is more prominent in spearman correlation as compared to Pearson correction the

The correlation coefficient ρ wrong obtained in Pearson is	The correlation coefficient ρ wrong obtained in sperman is
$\rho\ wrong = 1 - 2/m$ m= length of slice structure	$\rho\ wrong = .6325/\sqrt{m-1}$
Percentage of wrong guess is less in spearman correlation	

4. CONCLUSION

In this paper a detail description of LPA attack to cryptographic circuit with detail theoretical background is discussed and presented experimentally . A attack producer based on correlation to understand the behavior of circuit is examined and simulated to extract the crypto key the simulation is done on 45nm technology of TSMC on Cadence 6.15

REFERENCES

1. Alix. “Predictive estimation of protein linear epitopes by using the program PEOPLE”. Vaccine, 18:311–4, 1999.
2. Argos, P., Rossmann, M.G., Grau, U.M., Zuber, H., Frand, G., & Tratschin, J.D. (1979) Biochemistry **18,** 5698-5703
3. Atassi, M. Z. & Lee, C. L. (1978) Biochemistry 171, 429-434.
4. Atassi, M. Z. (1975) Immunochemistry 12, 423438.
5. Atsushi Ikai(1980).., “Thermostability and Aliphatic Index of Globular proteins”.., Biochem. 88, 1895-1898 (1980)
6. B. Peters, J. Sidney, P. Bourne, H. Bui, S. Buus, G. Doh, W. Fleri, M. Kronenberg, R. Kubo, O. Lund, et al. “The Immune Epitope Database and Analysis Resource: From Vision to Blueprint”. PLoS Biology, 3:e91, 2005.
7. Bachmair.A., Finley,D. and Varshavsky.A. (1986) Science, **234,** 179-186.
8. Baranyi L, Campbell W, Ohshima K, Fujimoto S, Boros M, Okada H. “The antisense homology box. a new motif within proteins that encodes biologically active peptides”. Nat. Med 1995, 1, pp. 894901.
9. Barlow,D.J., Edwards, M.S., and Thornton,J.M., 1986 “Continuous and discontinuous protein antigenic determinants’. Nature, Vol 322, pp747-748.
10. Berchanski A, Shapira B, Eisenstein M. “Hydrophobic complementarity in protein protein docking”. Proteins 2004, 56, pp. 130142.
11. Chen. J, H. Liu, J. Yang, and K. Chou.” Prediction of linear B-cell epitopes using amino acid pair antigenicity scale”. Amino Acids, 33:423–428, 2007.
12. Chou PY, Fasman GD. 1974. “Conformational parameters for amino acids in helical, &sheet and random coil regions calculated from proteins”. Eiochemistry 13:211-223.
13. Clements JD, Martin RE. “Identification of novel membrane proteins by searching for patterns in hydropathy profiles”. Eur. J. Biochem 2002, 269, pp. 21012107.
14. Creighton.T.E. (1988) BioEssays, 8, 57-63.
15. Curr ..,”Design of synthetic peptides for diagnostics”, Protein Pept Sci, 4(4):253-260, 2003.
16. D. Flower. “Immunoinformatics: “Predicting immunogenicity in silico”. Quantum distributor, 1st edition, 2007.