SUBTHRESHOLD DESIGN SPACE EXPLORATION FOR GAUSSIAN NORMAL BASIS MULTIPLIER

H. Kanitkar and D. Kudithipudi
Department of Computer Engineering, Rochester Institute of Technology, Rochester, NY-14623
Email: (hrk4712, dxkeec} @ rit.edu

***Abstract*— Digital circuits operating in the subthreshold region of the transistor are being used as an ideal option for ultra low power CMOS design. This paper discusses the use of subthreshold circuit design in cryptographic systems as a counter measure to power analysis attacks. A methodology for design of standard CMOS cell libraries in subthreshold is defined. These standard cells are used for implementing a digit-level *gaussian normal basis* (GNB) multiplier. The power consumption of the multiplier is 4.554 µW and speed of the multiplier is 65.1 KHz. The *signal-to-noise ratio* (SNR) for the subthreshold multiplier is 40 dB as compared to 200 dB for the superthreshold design. The reduced SNR increases the resistance of the subthreshold multiplier against power analysis attacks.**

***Index Terms*—subthreshold operation, minimum energy point, standard cell library, power analysis attacks**

I. INTRODUCTION

The use of subthreshold circuit design in cryptographic systems is gaining importance as a counter measure to power analysis attacks. The concept of power analysis attacks on cryptographic systems was proposed by Kocher [1] in the mid 1990s. A power analysis attack is non-invasive side channel attacks in which the power consumption of the cryptographic system can be analyzed to retrieve the encrypted data. Power analysis attacks are of two types: *simple power analysis* (SPA) attacks and *differential power analysis* (DPA) attacks [1]. In SPA attacks, the attacker observes the variation in power consumption of the micro-processor over a period of time. DPA is a more severe attack than the SPA, in which the attacker uses statistical methods and error correction techniques to determine information related to the encrypted data. DPA is much more difficult to prevent than the SPA. The typical countermeasures used in *elliptic curve cryptography* (ECC) at algorithmic level are the ones proposed in [2]: randomization of the private exponent, blinding the point and randomized projective co-ordinates. At circuit level, hiding and masking are two popular counter measures implemented that increase the resistance against power attacks but these techniques suffer from large areas and power overheads [3].

The main aim of this research is to understand the viability of implementing subthreshold systems for cryptographic applications. Standard cell libraries in subthreshold are designed and a methodology to identify the minimum energy point, aspect ratio, frequency range and operating voltage for CMOS standard cells is defined. As scalar multiplication is the fundamental operation in elliptic curve cryptographic systems, a digit-level *gaussian normal basis* (GNB) multiplier is implemented using the aforementioned standard cells. A similar standard-cell library is designed for the multiplier to operate in the superthreshold regime. The subthreshold and superthreshold multipliers are then subjected to a differential power analysis attack. Power performance and *signal-to-noise ratio* (SNR) of both these systems are compared to evaluate the usefulness of the subthreshold design. To implement the *digit-level gaussian normal basis multiplier with parallel output* (DLGMp) in subthreshold, first the minimum energy point, aspect ratios, frequency range and operating voltage for all the subcomponents of the multiplier are identified. Each sub cell is implemented using IBM 65nm technology with 1X, 2X and 3X fan-out of 4 (FO4) [4] delays.

Energy minimization is the enabling factor for sub-threshold design and identifying the operating voltage range for the optimal energy forms the design basis. Two commonly used terms in sub-threshold design are V_{min}, the voltage at which the energy of the circuit is minimum and $V_{dd,limit}$, the lowest supply voltage at which the circuit can be operated. In most cases the V_{min} is greater than $V_{dd,limit}$. V_{min} denotes the ideal supply voltage at which the circuit should be operated. Stacking of transistors raises the $V_{dd,limit}$ of a circuit well above that of a simple inverter.

The location of the energy minimum of any circuit is a compromise between the dynamic and leakage energies. Activity factor, α, V_{th}, L_{eff}, sub-V_{th} slope and I_{on} are interdependent and should be considered for determining the minimum energy point of any design [5].

The methodology used for designing circuits in subthreshold is explained in Section II. Section II also explains the standard cell library characteristics in subthreshold. Section III discusses the effects of process variations on subthreshold circuits. Section IV explains the characteristics of the Gaussian normal basis multiplier in subthreshold. Section V gives the concluding remarks.

II. METHODOLOGY

The methodology used for designing a standard cell library in subthreshold can be best summarized as follows. The standard cell library created consists of 32 CMOS cells. The methodology is summarized by the flowchart shown in Figure 1. A seven stage ring

oscillator is used as a test circuit for the INVERTER, NAND and NOR gates. The INVERTER is first simulated for optimal sizing i.e. the "ideal" aspect ratio at which the charging and discharging currents are equal and a symmetrical output is observed. The simulations are carried out for all process corners. The optimal sizing does not necessarily mean that the circuit operates at minimum energy. Therefore, the INVERTER was resized and re-simulated to find the minimum energy point. The simulations were also carried out for various activity factors. With INVERTER as the reference, the NAND and NOR gates were designed and simulated for minimum energy. The effect of increasing aspect ratio and transistor activity factor α on the minimum energy point were also observed. The INVERTER, NAND and NOR gates can now be used to design the remaining standard cells. For designing the XOR gate and flip-flops a different approach is used. The TINY XOR, commonly used in standard cell libraries, fails to operate correctly at voltages below 100mV. Hence, an XOR gate suitable for subthreshold operation is used. Charge keepers are required in the standard transmission gate flip-flops to make it suitable for subthreshold (flip-flop1).

III. STANDARD CELL LIBRARY

This section presents the characteristics of the standard cells in terms of minimum energy point, frequency, and operating voltage ranges.

A. INVERTER

The inverter operates at a $V_{dd,limit}$ of 60 mV. Optimal aspect ratio for the nominal case and worst case are identified for the inverter, shown in Figure 2 and Figure 3.

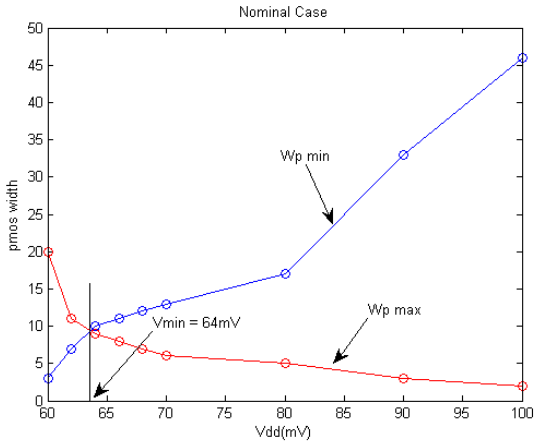

Figure 2: Inverter nominal case aspect ratio.

The width of the pmos is found such that the output of the ring oscillator is within 10% to 90% of the supply voltage. Maximum pmos width ($W_{p,max}$) is defined as the width at which the output of the ring oscillator is within 10% of the supply voltage [6]**.** Minimum pmos width ($W_{p,min}$) is defined as the width at which the output of the ring oscillator is at least 90% of the supply voltage [6]**.** As can be seen from the Figure 2, for the nominal case the optimum aspect ratio is 9 and the corresponding supply voltage is 64 mV. The ring oscillator is also simulated for worst case conditions. For $W_{p,max}$ the worst case process corner was taken as SF and for $W_{p,min}$ it was taken as FS. These two process corners are sufficient to characterize the behavior of the circuit, as the circuit behavior will be symmetrical at the other two corners, namely SS and FF.

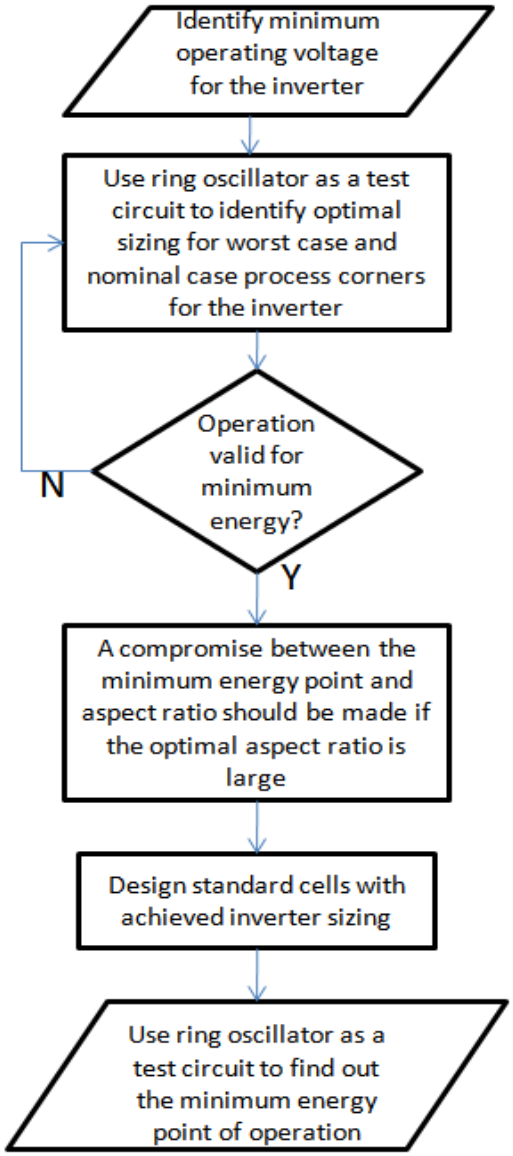

Figure 1: Design methodology for sub-threshold circuits.

As can be interpreted from Figure 3, the aspect ratio for the worst case remains as 9 but there is an increase in the minimum operating voltage to 137 mV. To conclude an aspect ratio of 9 is ideal for operating the inverter in sub-threshold. So far we have not considered the minimum energy point of operation.

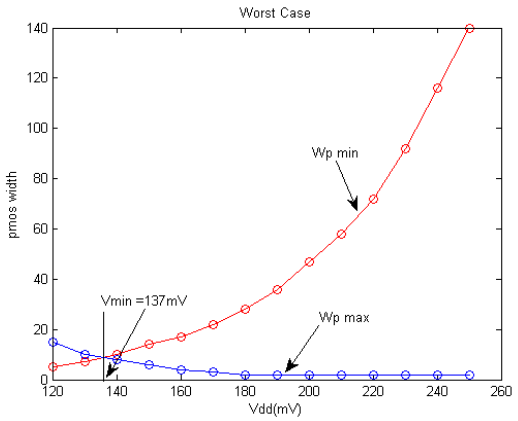

Figure 3: Inverter worst case aspect ratio

To characterize the inverter for minimum energy condition, the ring oscillator was re-simulated with aspect ratios of 2 and 5. The energy characteristics of the ring oscillator at aspect ratio of 2 are shown in Figure 4. The results indicate that leakage energy is dominant in sub-threshold and decreases as the supply voltage is increased into the superthreshold region. The point where the leakage and dynamic energy cross is the minimum energy point. The minimum energy point decreases from 195 mV to 185 mV as the aspect ratio is increased from 2 to 5. Also, the minimum operating voltage and hence the power will also decrease as the aspect ratio is increased. Thus, we can conclude that if the aspect ratio is further increased to 9 the oscillator will operate at the ideal minimum energy point. An aspect ratio of 9 is too high especially when the inverter is used as a reference for the other standard cell designs.

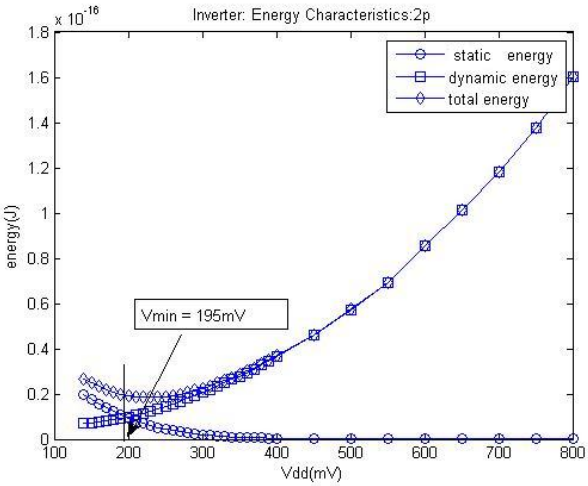

Figure 4: Inverter energy characteristics: aspect ratio 2.

To further understand the effect of aspect ratio on inverter characteristics, we tracked the voltage transfer characteristics for aspect ratios 2, 5, and 9 with a supply voltage of 140 mV shown in Figure 5 (a), (b), and (c) respectively. There is a shift in the midpoint voltage as the aspect ratio is increased. We can see that the aspect ratio of 2 provides a valid operating zone. For the optimum aspect ratio of 9, the midpoint voltage V_M is 74.45 mV which indicates symmetrical output.

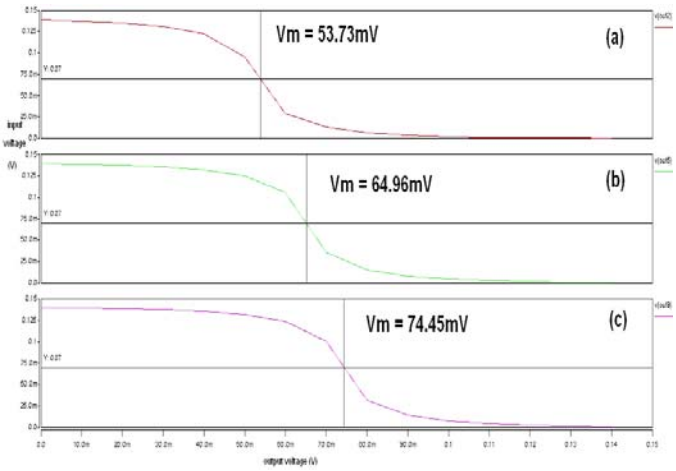

Figure 5: Inverter voltage transfer characteristics

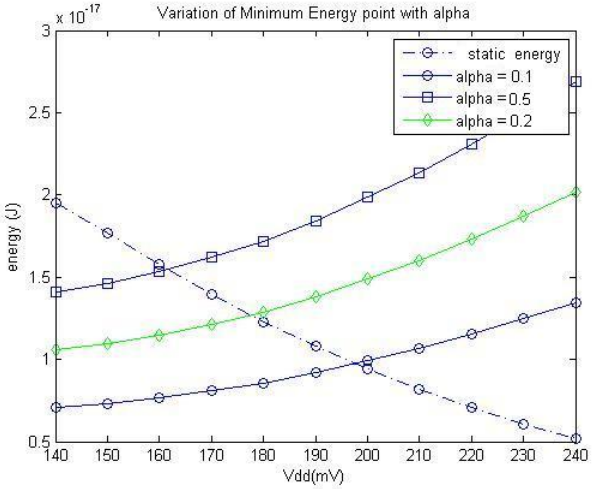

Figure 6: Variation of minimum energy point with alpha.

Variation of the minimum energy point with the transistor activity factor *α* is shown in Figure 6. The graph indicates that V_{min} increases from a value of 162 mV to 196 mV as the value of α decreases from 0.5 to 0.1. This is expected because with an increase in the value of *α*, the transistors in the circuit are utilized more, the circuit is less ideal and the dynamic energy increases. Thus, for a lower minimum energy point, the circuit should be utilized more.

B. NAND and NOR

The NAND and NOR gates were simulated using inverter size of 2 and 5. The V_{min} reduces from 242 mV to 235 mV as the size of the NAND gate increases from 2 to 5. This is expected as the optimal aspect ratio for the INVERTER is 9. As the aspect ratio goes closer to the reference value of 9 the minimum energy point will reduce. Similar observations were also noticed for the NOR gate. The V_{min} for the NOR gate reduces from 224 mV to 195 mV as the aspect ratio is increased from 2 to 5.

C. XOR

The simulation of the TINY XOR gate (Figure 7(a)) used in standard libraries is shown in Figure 8. At a voltage of 100 mV or lower, the tiny XOR gate fails to

operate correctly when the input bits change from 10 to 01. A XOR gate suitable for sub-threshold operation is

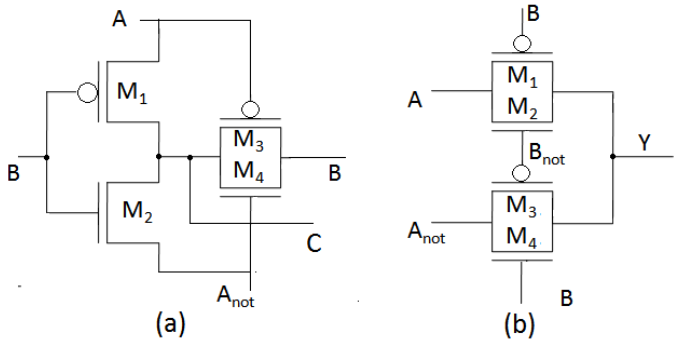

Figure 7: (a) Tiny XOR. (b) Subthreshold XOR.

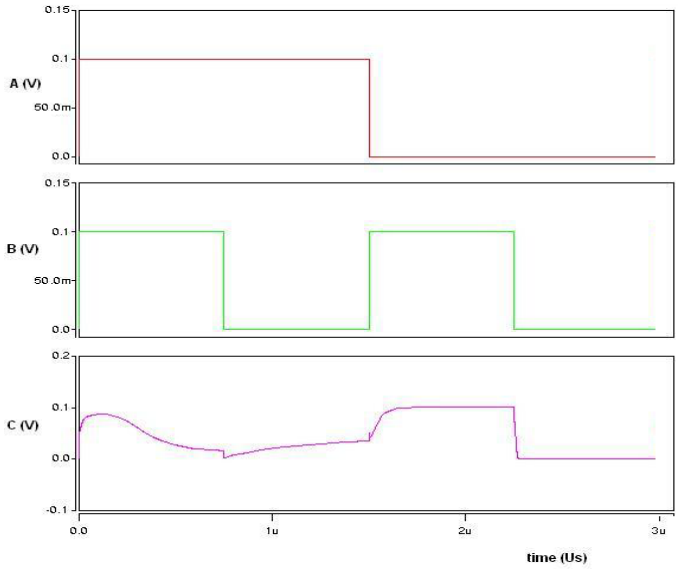

Figure 8: Tiny XOR output.

shown in Figure 7(b). As the results (Figure 9) indicate,

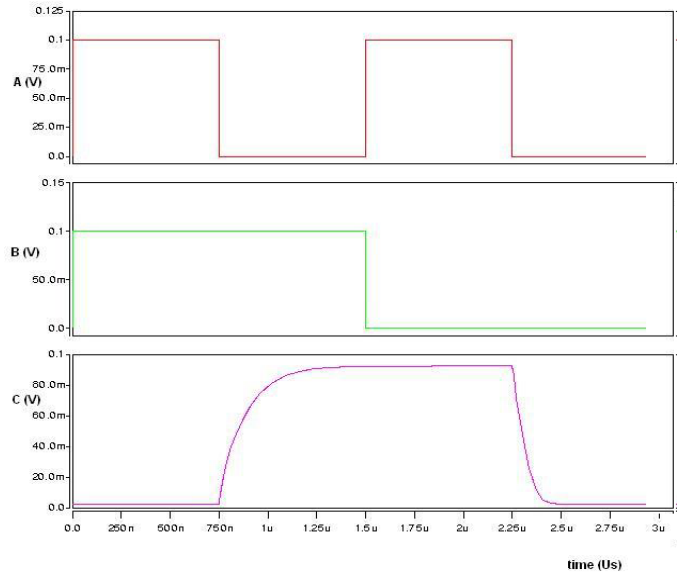

Figure 9: Subthreshold XOR output.

this gate is suitable for all input combinations at very low voltages [6]. Transmission gates and transistors of Figure 7 were designed using a minimum sizing of (1/1).

D. Flip-Flops

For the design of the D flip-flop, an approach similar to the one for XOR gate is used. Initially, a transmission gate based flip-flop is simulated. The optimal aspect ratio of (9/1) is used for sizing the inverters and for the transmission gates a minimum sizing of (1/1) is used. The output of the flip-flop follows the input, but, does not rise to the required 90% noise margin.

In order to pull the output up to the desired value two charge keepers, one at the output node and one in the feedback loop, are needed. This modified transmission gate flip-flop, flip-flop1, is shown in Figure 10. Minimum sizing of (1/1) is used for the charge keepers. The simulations of this modified transmission gate flip-flop are shown in Figure 11. As can be seen from Figure 11, with the help of the two charge keepers, the output is pulled up to the desired 90% noise margin.

For implementing the digit level gaussian normal basis multiplier the inputs need to be circularly shifted. For the

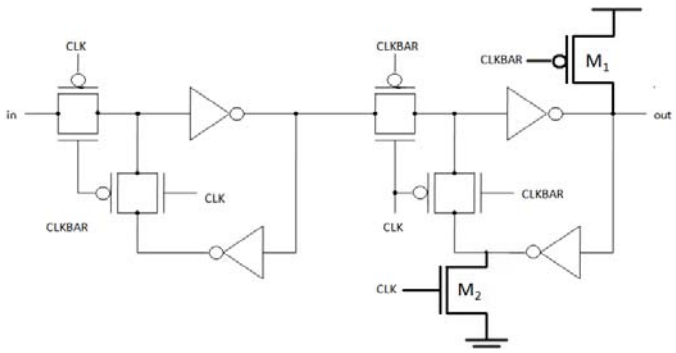

Figure 10: Modified transmission gate flip-flop, flip-flop1.

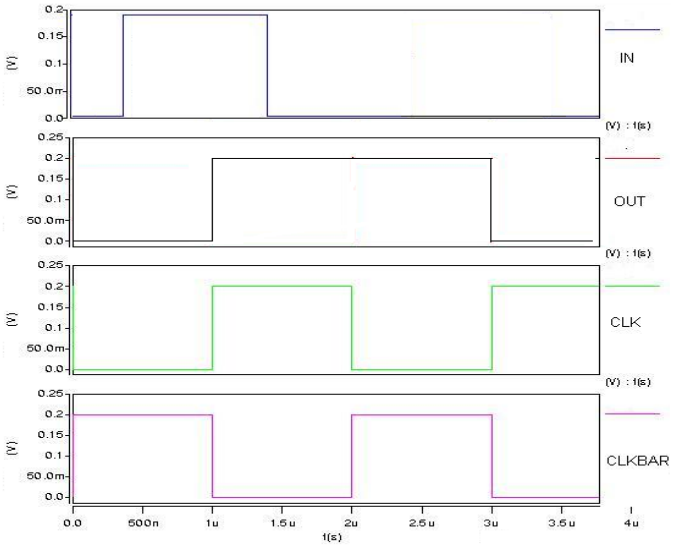

Figure 11: Flip-flop1 characteristics.

multiplication process, the multiplier and the multiplicand in the input registers need to be stable for the first clock cycle. The circular shift with flip-flop1 was implemented

and it was noted that the inputs do not remain stable for the first clock cycle. Hence, a flip-flop with preset and clear pins is required. This flip-flop, flip-flop2, is shown in Figure 12. Minimum sizing was used for the INVERTER, NAND and transmission gates in the design.

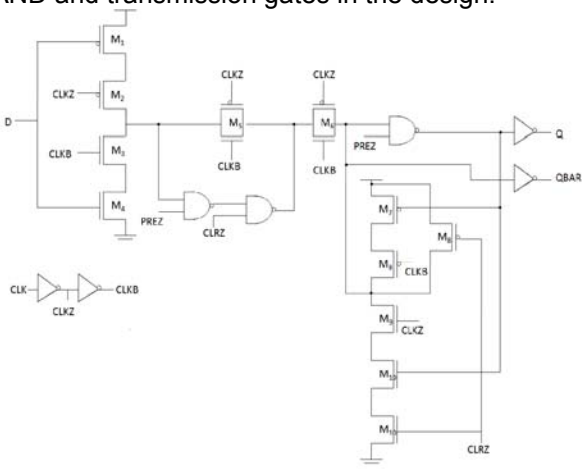

Figure 12: Flip-flop2.

E. STANDARD CELL LIBRARY RESULTS

The results of the subthreshold standard cell library are summarized in Table 1. Table 1 suggests that by increasing transistors in a stack, the minimum energy point and power increase and the speed of operation decreases.

Cell	$V_{ddlimit}$	Speed	Power
INVERTER	60mV	33.6 KHz	3.6e-12 W
NAND2	124mV	115 MHz	1.051e-8 W
NAND3	139mV	107 MHz	1.236e-8 W
NAND4	156mV	82.4 MHz	2.320e-8 W
AND2	133mv	109 MHz	9.188e-8W
AND3	149mV	87.6 MHz	9.877e-8 W
AND4	161mV	76.9 MHz	1.211e-7W
NOR2	108mV	114.6MHz	2.628e-8 W
NOR3	124mV	102.9MHz	4.198e-8 W
NOR4	137mV	76.3MHz	9.123e-8 W
OR2	121mV	66.4 MHz	1.011e-7 W
OR3	135mV	46 MHz	1.361e-7 W
OR4	153mV	29.6 MHz	1.426e-7W
AO21	210mV	46.1MHz	1.025e-7W
AO22	218mV	36.9 MHz	9.381e-8 W
AO32	235mV	112 MHz	1.199e-7 W
AOI21	289mV	181 MHz	1.137e-7 W
AOI22	214mV	76.8 MHz	4.480e-7 W
AOI32	237mV	84.1 MHz	4.768e-7 W
AOI221	300mV	77.6 MHz	3.139e-7 W
AOI321	290mV	47 MHz	2.235e-7 W
OA21	219mV	83.9 MHz	8.996e-8W
OA32	220mV	66.3 MHz	1.205e-7W
OAI21	210mV	43.2 MHz	3.254e-8W
OAI32	255mV	38.7 MHz	6.037e-8 W
AO221	309mV	80.8 MHz	3.944e-7 W
AO321	300mV	43 MHz	6.922e-7 W
NOR0211	289mV	98.4 MHz	2.049e-7 W
Flip-flop1	200mV	500 KHz	255e-9 W
Flip-flop2	229mV	858 KHz	652e-9 W

Table 1: Standard cell library characteristics

IV. PROCESS VARIATIONS

Subthreshold systems are sensitive to process variations. The process variations for a particular corner are defined by the parameter sigma. Sigma is a statistical notation for the standard deviation that is used to quantify how far a given process deviates from ideal behavior. We use six-sigma notation to indicate process variation. The inverter power characteristic for the positive values of 3σ is shown in Figure 13 and for the negative values of 3σ is shown in Figure 14. An increase in the inverter power is observed for constant V_{dd} as the value of sigma becomes more positive. At 300 mV, the power for a value of sigma of -3 is 9.92e-13 while the power at a sigma value of 3 is 2.07e-6, almost 2.08e6 times more. This substantial increase in power is due to an increase in current as the width increases and channel length reduces for a more positive sigma value. As can be observed from Figure 15 and Figure 16, the frequency increases with an increase in sigma value. For 300mV, the increase in frequency at sigma value 3 is 1.36e6 times the frequency at sigma value -3. As the sigma value becomes more positive, the series resistance and capacitance of the transistor reduce resulting in an increase in the frequency value for constant V_{dd}. These process variations need to be accounted for designing subthreshold circuits.

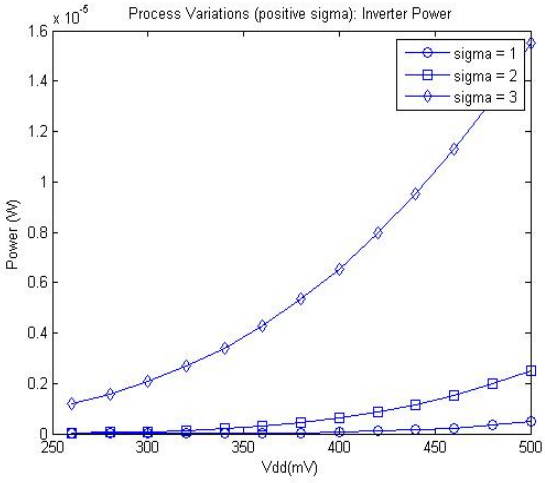

Figure 13: Inverter power for positive sigma values.

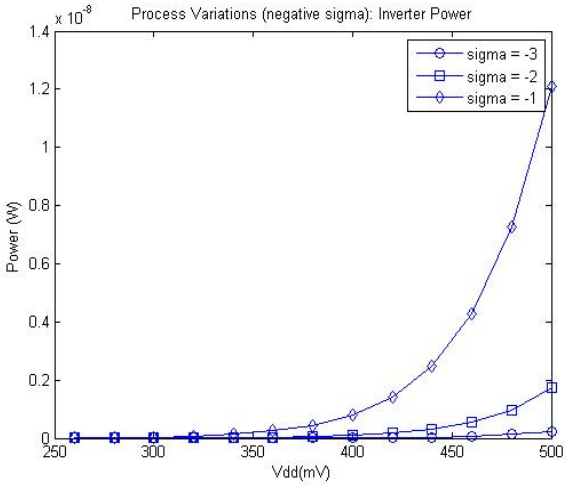

Figure 14: Inverter power for negative sigma values.

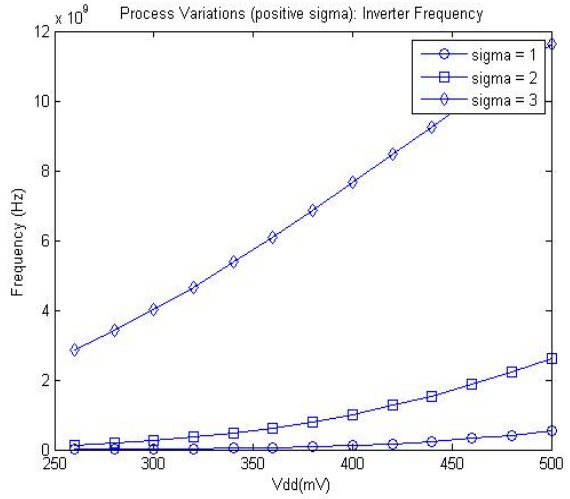

Figure 15: Inverter frequency for positive sigma values.

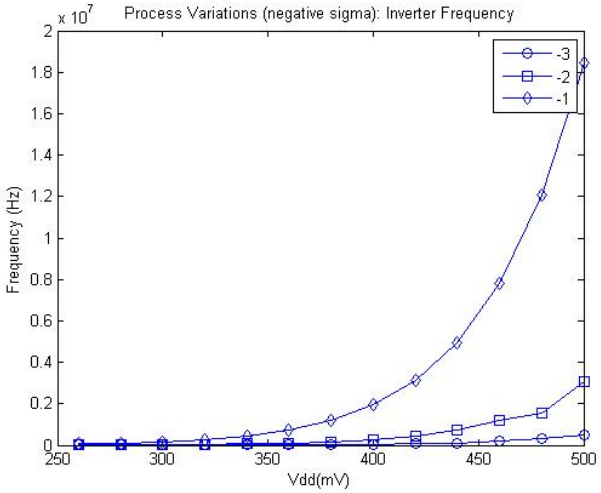

Figure 16: Inverter frequency for negative sigma values.

V. GAUSSIAN NORMAL BASIS MULTIPLIER

The Guassian Normal Basis multiplier, DLGMp (Figure 17), can be best understood by the following equations. Let *A*, *B*, *C* and *D* be elements of galois field, $GF(2^m)$, where *m* is the number of bits needed to represent each element in $GF(2^m)$. Then the product *C* can be represented as

$$C_{j+1} = C_j^{2d} \text{ XOR } D(A_j;B_j) \quad (1)$$

where $D(A_j;B_j)$ represents an ANDing operation.

$$A_{j+1} = A_j^{2d} \quad (2)$$
$$B_{j+1} = B_j^{2d} \quad (3)$$

where A_{j+1} and B_{j+1} are d-fold right cyclic shift operators.

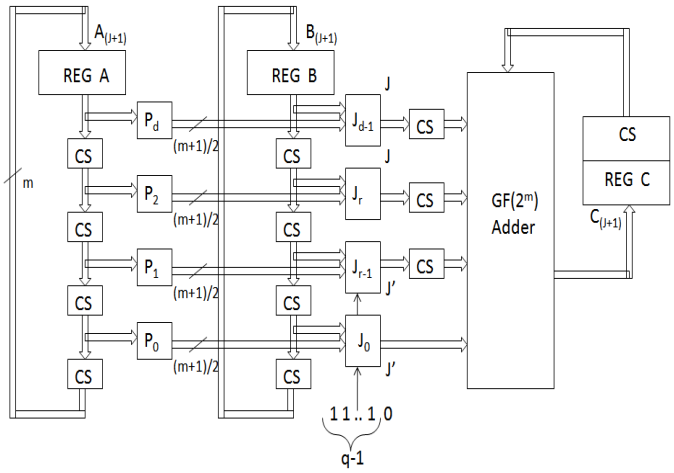

Figure 17: Digit-level gaussian normal basis multiplier with parallel output DLGMp. Adapted from [7].

The DLGMp contains three registers *A*, *B* and *C*. Registers *A* and *B* store the multiplicand and the multiplier and the register *C* stores the output. Block *P* consists of XOR gates and manipulates *A* in a manner that it can be used for the ANDing operation of equation 1. Blocks *J* and *J'* are used for the ANDing operation of equation 1. $GF(2^m)$ adder consist of an array of XOR gates that implement Equation 1 and CS blocks represent the logic needed to implement cyclic shifts for *A*, *B* and *C*. In the block diagram, *q* represents the number of clock cycles required for multiplication, *d* represents the number of bits in each digit, $1 \le d \le m$ and *r* is a number between 0 and $(d - 1)$ such that $m = (qd - r)$. Blocks *J* and *J'* are similar but for the fact that *J'* is controlled by signal *q* and its output is zero at the end of $(q - 1)$ clock cycles. The main components of the multiplier are registers, AND gates and XOR gates. These components will be used from the standard cell library to implement the multiplier.

A 7 bit prototype DLGMp multiplier was designed and simulated for analysis. The multiplier operates at a $V_{dd,limit}$ of 267 mV. At this voltage the power consumption of the multiplier is 4.554 µW and speed of the multiplier is 65.1 KHz. In comparison, at 1.2 V, i.e. in the superthreshold region, this multiplier operates at a speed of 330 MHz and power consumption of 4.005 mW. Thus, a power saving of is observed for the subthreshold multiplier at the cost of reduction in speed.

A simple power analysis example is shown in Figure 18. The graphs in the figure represent the supply current trace of the superthreshold multiplier. A change in the current trace is clearly visible for a change in input. Thus, an attacker can easily find a correlation between the change in the supply current to the input applied. In a differential power analysis the attacker observes thousands of such current (power) traces and using sophisticated statistical methods to find a correlation between the operation performed and the current (power) trace.

The supply current graphs for the subthreshold and superthreshold multipliers for 1000 random input combinations are shown in Figure 19 and Figure 20 respectively. As can be observed from the figures, the supply current of the subthreshold multiplier is 33 times less than that of the superthreshold multiplier. At such

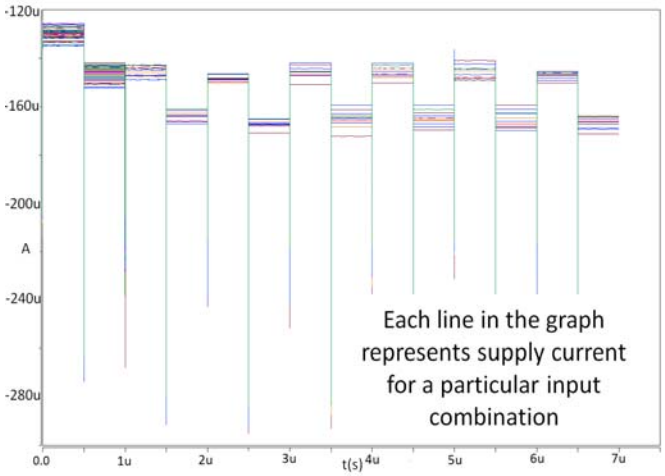

Figure 19: Current traces for 1000 random input combinations at V_{DD} = 0.3 V.

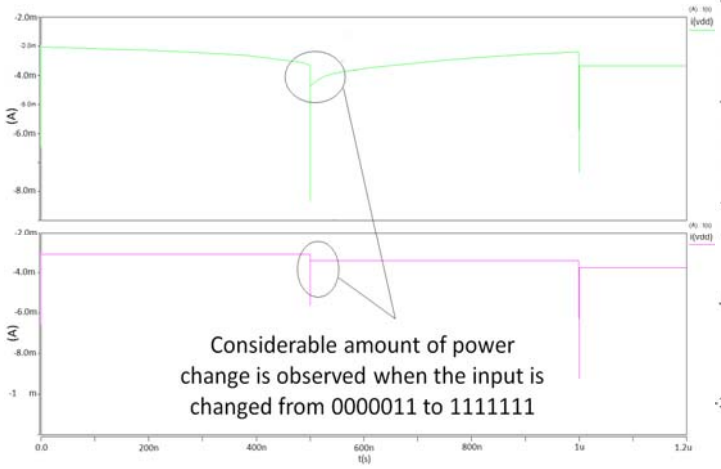

Figure 18: Simple power analysis.

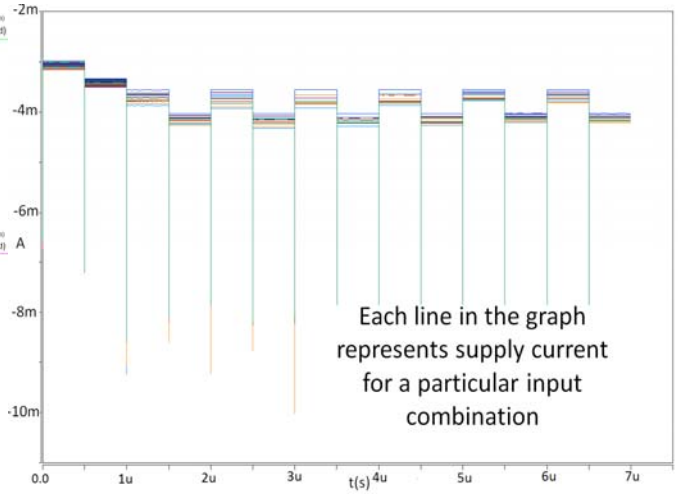

Figure 20: Current traces for 1000 random input combinations at V_{DD} = 1.2V.

low current values, the attacker might need infinitely large current traces to perform the differential power analysis.

. The SNR for the subthreshold multiplier is 40 dB as compared to 200 dB for the superthreshold case. Thus, by operating the multiplier in subthreshold, the signal magnitude becomes comparable to noise. At such low magnitudes it is very difficult for an attacker to correlate the outputs of the multiplier to the change in inputs. By operating cryptographic systems at subthreshold, the difficulty in mounting DPA attacks against them is greatly increased.

VI. Conclusion

This research outlines a basic methodology for design of standard cells in subthreshold, which are used in the implementation of the DLGMp multiplier. The design of the standard cells is a compromise between sizing, energy and frequency of operation. The lowest minimum energy point is observed for an aspect ratio of 9 for the inverter. However such a large sizing is not suitable for circuits which use the inverter as their reference. Therefore for the standard cells designed we have used a sizing of 5 to achieve minimum energy and integral performance. For a given aspect ratio, the minimum energy point decreases as the transistor activity factor increases. This is expected because as α increases, the circuit is being utilized more and there is an increase in the dynamic energy at the cost of leakage energy. For high switching activity circuits it is more feasible to operate at the minimum energy point compared to low switching activity circuits. The minimum energy point increases with stacking of transistors and therefore highly stacked designs are not preferred.

A 7 bit prototype DLGMp multiplier is implemented in subthreshold and superthreshold regions of operation. In subthreshold, the multiplier operates at a minimum supply voltage of 267 mV. At this voltage the power consumption of the multiplier is 4.554 µW and speed of the multiplier is 65.1 KHz. In comparison, at 1.2 V, i.e. in

the superthreshold region, this multiplier operates at a speed of 330 MHz and power consumption of 4.005 mW. Thus, a significant amount of power saving is observed for the subthreshold multiplier at the cost of reduction in speed. The SNR for the subthreshold multiplier is 40 dB as compared to 200 dB for the superthreshold case. By operating the multiplier in subthreshold, the signal magnitude becomes comparable to noise and hence it is very difficult to correlate the outputs of the multiplier to the change in inputs. Thus, cryptographic systems at subthreshold increase the difficulty in mounting DPA attacks against them.

REFERENCES

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential power analysis", Annual International Cryptography Conference *Advances in Cryptology:CRYPTO*, pages 388–397, 1999.

[2] C.K. Koc and C. Paar. "Cryptographic Hardware and Embedded Systems", volume1717 of Lecture Notes in Computer Science. Springer Berlin/Heidelberg, 1999.

[3] Thomas Popp, Elisabeth Oswald and Stefan Mangard," Power analysis attacks and countermeasures". IEEE Design and Test of Computers, vol.. 24, No. 6, pages 535–543, November-December 2007.

[4] David Harris, Ron Ho, Gu-Yeon Wei, and Mark Horowitz.,"The fanout-of-4 inverter delay metric", http: www.vlsi.stanford.edu/papers/dh_vlsi_9.pdf

[5] S.Hanson, B. Zhai, K.Bernstein, D.Blaauw, A.Bryant, L.Chang, K.K.Das, W.Haensch, E.J.Nowak, D.M.Sylvester , "Ultralow-voltage, minimum-energy CMOS", IBM res. & dev., vol.50 NO 4/5, pages 469-490, pages 1778-1786, July/Sept 2006

[6] Benton H. Calhoun, Alice Wang and Anantha Chandrakasan, "Modeling and Sizing for Minimum Energy Operation in sub-threshold Circuits", IEEE Journal of Solid-State Circuits, vol. 40, No.9, Sept. 2005.

[7] Arash Reyhani-Masoleh, "Efficient algorithms and architectures for field multiplication using Gaussian normal basis", IEEE transactions on computer, vol. 55, No. 1, pages 34-47,Jan. 2006.