International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 2, Issue 11, November 2015

An Integrated IVCCRL Approach for the reduction of Negative Bias Temperature Instability in an AES Core

[1] Anitha Patibandla [2] Dr.B.L.Raju
[1]Associate Professor [2] Principal
[1][2] Department of Electronics & Communication Engineering
[1]MRCET, [2]ACE Engineering College
Hyderabad, India

Abstract:— **Reliability of Circuits is one of the major concerns in VLSI circuits and systems designs. Negative Bias Temperature Instability(NBTI), which has a deteriorating effect on the threshold voltage and the drive current of semiconductor devices, is emerging as a major reliability degradation mechanism [1].An important Reliability issue in the recent times is the Negative bias temperature instability (NBTI) in the MOS circuits in Cryptographic cores. Many works propose hardware implementations of cryptographic primitives with the promise of reduction in area, power dissipation and cost. An integrated IVCCRL approach for the reduction of Negative Bias Temperature Instability in an AES Core using the techniques of Input Vector Control (IVC) and Reversible Logic (RL) is being proposed in this paper. The effect of input vector control investigated. Mini-mum leakage vectors, which lead to minimum circuit performance degradation and maximum leakage reduction rate, are selected and used when the circuit is in the standby mode. Analysis on the potential to save the circuit performance degradation by internal node control techniques during circuit standby mode is discussed. The optimization is done for the AES algorithm using NCL Reversible Gates for low power, low cost and low area. Simulation Results have been analyzed and presented.**

***Keywords*— NCL, Reversible Logic, AES, NBTI**

I. INTRODUCTION

Circuit reliability is one of the major concerns in VLSI circuits and systems. Negative Bias Temperature Instability (NBTI), which has a detrimental effect on the threshold voltage and the drive current of semiconductor devices, is emerging as a major reliability degradation mechanism [1].NBTI occurs when PMOS devices in circuits are heavily stressed under negative gate voltage (i.e., Vgs = −Vdd) at elevated temperature, causing a shift in threshold voltages (for example, Threshold voltage modification due to NBTI can be as much as 50mV [2]), and resulting in degradation of device performance [1]. Bias temperature stress under constant voltage (DC) (i.e., static NBTI) leads to device performance degradation at a very fast rate. Also, under actual AC stress condition [3, 4], when stress is periodically removed, the degradation of device parameters is partially recovered, which leads to a less severe parameter's shifts over long time when compared with that under DC stress condition. The previous work about NBTI primarily focuses on the analysis of the threshold voltage degradation and the impact on the drive current of semiconductor devices [3, 5]. Of late, some analytical models that evaluate NBTI effect with multi-cycle AC stress were proposed to help designers estimate the circuit performance degradation due to NBTI [6, 7] based on these analytical circuit degradation models, some researchers have investigated NBTI aware design methods [8,9]. Kumar et al. [8] studied the impact of NBTI on the read stability of SRAM circuits and proposed a simple bit transition technique to recover from the static noise margin of SRAM cells. Paul et al. [9] presented an NBTI-aware sizing algorithm to ensure the accuracy of nano-scale circuits. Earlier analytical NBTI models for the circuit performance degradation were based on the estimation that the circuit temperature remains constant all the time; However, during circuit operations, the circuit temperature changes tremendously when the circuit mode changes between active and standby state. As NBTI is temperature-dependent, and experiments indicate that at higher temperature, the degradation under stress is faster, but the recovery is slower [4]. It has been proved that the impact due to NBTI under a higher temperature has a large gap compared with that under a lower temperature condition. NBTI not only depends on the temperature, but also depends on the input states of the PMOS devices; meanwhile the leakage current of a gate also relies on the gate input states. One of the most popular leakage

reduction techniques applied in the circuit standby mode is the input vector control method (IVC) [10–14]. Therefore, in this paper, we also investigate the approach of using the IVC technique to simultaneously reduce the leakage and reduce the impact of NBTI. The IVC technique is based on the well-know transistor stacking effect: a CMOS gate's sub threshold and gate oxide leakage current varies dramatically with the input vector applied to the gate [15, 16]. Primarily in an IVC technique, the minimum leakage vector (MLV) is used with the help of standby signals to reduce both sub threshold and gate oxide leakage current when the circuit is at the standby mode. When the MLV is modified, in the circuit standby mode, the internal state of each node in the circuit is set to 0 or 1, such that the circuit standby leakage is minimized. The repeatedly stressed on PMOS transistors in the circuits in the critical paths or near critical paths may have negative impact on the circuit performance due to NBTI.

II. REVERSIBLE LOGIC AND REVERSIBLE GATES PRELIMINARIES

A Boolean function f: $B_n \rightarrow B_n$ is said to be reversible if it is objective. In other words every input vector is uniquely mapped to an output vector. The problem of synthesis is to determine a reversible circuit that realizes a given function f. In this paper, for the purpose of synthesis we consider the gate library consisting of multiple-control Toffoli (MCT) gates. An n-input MCT gate with inputs (x1, x2. . . xn) pass the first (n − 1) inputs unchanged, and complements the last input if all the remaining (n − 1) inputs are at 1. Figure 1 shows an n-input MCT gate. A simple NOT (n = 1) and controlled-NOT or CNOT (n = 2) are special cases of the MCT gate. Any reversible function can be implemented as a cascade of reversible gates, without any fan out or feedback. To estimate the cost of an implementation, several metrics are used, Namely, number of gates, number of equivalent MOS transistors, and number of equivalent basic quantum operations called the quantum cost [1]. There are standard ways of computing the quantum cost from a given gate net list [3]. Some works also try to reduce the number of Garbage Outputs, which are the outputs that are don't cares for all possible input conditions.

III. OVERVIEW OF NCL

NCL uses dual-rail or quad-rail signaling methods to achieve the DI. A pair of dual-rail signals A0 and A1 could be either 10 (i.e., DATA0), 01 (i.e., DATA1), or 00 (i.e., NULL); as 11 is considered invalid. Similarly, the quad-rail signaling method uses four rails instead of two. The possible sets for quad-rail signaling method will be DATA0 (1000), DATA1 (0100), DATA2 (0010), DATA3 (0001), and NULL (0000). NCL uses two states, DATA (i.e., data representation) and NULL (i.e., control representation) to synchronize itself and control the input and output, eliminating the need of a reference clock signal. To indicate the transition between the NULL and DATA states, each NCL combination logic must be bracketed by input and output DI registers, these registers have an input/output acknowledgment signal that changes between 0s and 1s to provide request-for-NULL (i.e.,RFN) and request-for- DATA (i.e.,RFD), respectively. An example is shown in Figure 7.1. These signals are used to initiate a delay insensitive handshaking protocol that handles timing locally.

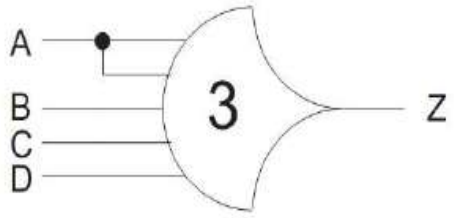

Figure 1:An NCL Gate

Table 1: Truth table of NCL TH23 gate

Z^*	A B C	Z	Z^*	A B C	Z
0	0 0 0	0	1	0 0 0	0
0	0 0 1	0	1	0 0 1	1
0	0 1 0	0	1	0 1 0	1
0	0 1 1	1	1	0 1 1	1
0	1 0 0	0	1	1 0 0	1
0	1 0 1	1	1	1 0 1	1
0	1 1 0	1	1	1 1 0	1
0	1 1 1	1	1	1 1 1	1

IV. NCL AES ALGORITHM AND ITS IMPLEMENTATION

AES algorithm consists of a number of rounds that depend mostly on the key size. For both ciphering and deciphering of AES algorithm, each round consists of

linear operation (i.e., Add Round Key, Shift Rows, and Mix Columns steps) and non-linear operation (i.e., Sub Bytes step). The Sub Bytes step is the first step of AES round. Each byte in the array is dated by an 8-bit substitution box (S-Box), which is derived from the multiplicative inverse over GF. AES S-Box is constructed by combining the inverse function with an inverse affine transformation in order to avoid attacks based on mathematics. The S-Box is the most critical components in the implementation of AES hardware. It consumes majority of power and is also the most vulnerable component in SCAs. The block diagram of multiplicative inversion over GF component where MM modular multiplication is, and XOR is exclusive-or operation.

The hardware implementation of AES S-Box follows the combinational logic circuit architecture, but uses NCL gates Block Diagram of a Combinational S-Box with Encryption and Decryption Data Paths. The affine transformation and inverse affine transformation components follow a series of Boolean equations where I and Q represents the 8-bit input and output, respectively. Both transformations require many XOR gates. The multiplicative inversion in GF follows the procedure shown in Figure part (b). 1) The Map operation converts the 8-bit input into elements of GF (i.e. ah and al); 2) Calculate the square of ah and al. It should be noticed that multiplication in GF is done by multiplying the polynomial ah(x) ah(x) follows a modular reduction; 3) A series of multiplication and XOR operations were implemented to extend the field GF to the field GF.

To implement the conventional S-Box using NCL, the XOR, AND, and MUX operation in dual-rail NCL gates are required. NCL has a total of 27 threshold gates to realize various logic functions. In order to achieve the input-completeness and observability, it is important to choose the correct threshold gates. For example, in the design of a two-to-one multiplexer, according to the K map in and both of them can be mapped to a NCL circuit with a TH24comp gate, a THand0 gate, and a TH22 gate. The finalized NCL MUX logic diagram is shown in Figure. Two TH24comp gates can be used to implement an XOR logic function. A THand0 and a TH22 gate can be used to implement an AND logic function each of the blocks SB, SR, MC, ARK and KeyGen are implemented using reversible logic gates.

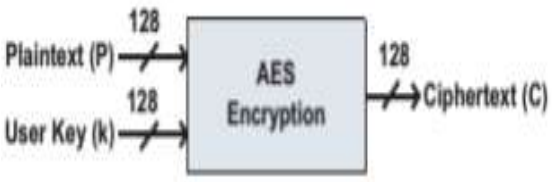

Figure 2: Top level Schematic of AES Encryption

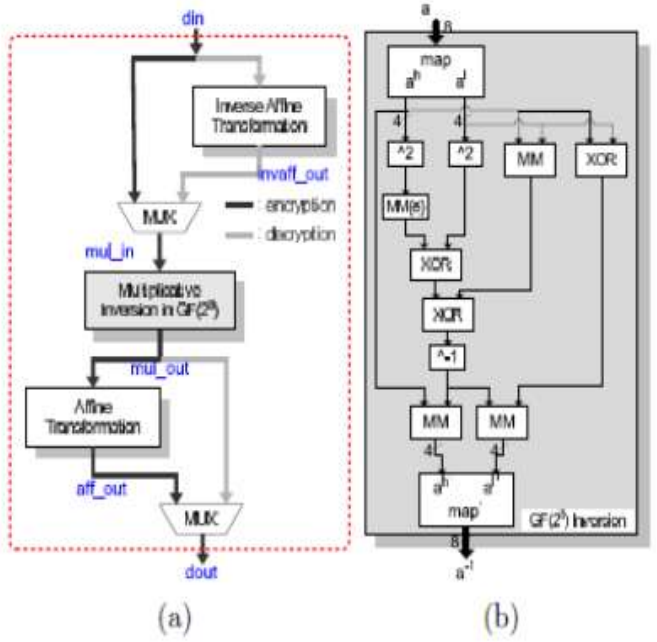

Figure 3:AES design

Table 2 :Affine and Inverse Affine Transformations

Boolean Equations for Affine Transformation and Inverse Affine Transformation Components

$q = aff\_trans(i)$	$q = aff\_trans^{-1}(i)$
$q_0 = (i_0 \oplus i_4) \oplus (i_5 \oplus i_6) \oplus (i_7 \oplus 1)$	$q_0 = i_2 \oplus i_5 \oplus i_7 \oplus 1$
$q_1 = i_1 \oplus i_5 \oplus i_6 \oplus i_7 \oplus i_0 \oplus 1$	$q_1 = i_0 \oplus i_3 \oplus i_6$
$q_2 = i_2 \oplus i_6 \oplus i_7 \oplus i_0 \oplus i_1$	$q_2 = i_1 \oplus i_4 \oplus i_7 \oplus 1$
$q_3 = i_3 \oplus i_7 \oplus i_0 \oplus i_1 \oplus i_2$	$q_3 = i_2 \oplus i_5 \oplus i_0$
$q_4 = i_4 \oplus i_0 \oplus i_1 \oplus i_2 \oplus i_3$	$q_4 = i_1 \oplus i_3 \oplus i_6$
$q_5 = i_1 \oplus i_5 \oplus i_2 \oplus i_3 \oplus i_4 \oplus 1$	$q_5 = i_2 \oplus i_4 \oplus i_7$
$q_6 = i_6 \oplus i_2 \oplus i_3 \oplus i_4 \oplus i_5 \oplus 1$	$q_6 = i_0 \oplus i_3 \oplus i_5 \oplus 1$
$q_7 = i_7 \oplus i_3 \oplus i_4 \oplus i_5 \oplus i_6$	$q_7 = i_1 \oplus i_4 \oplus i_6$

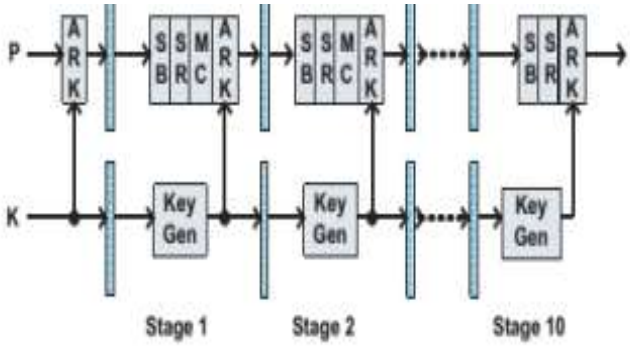

Figure 4: Reversible Pipelined implementation of AES

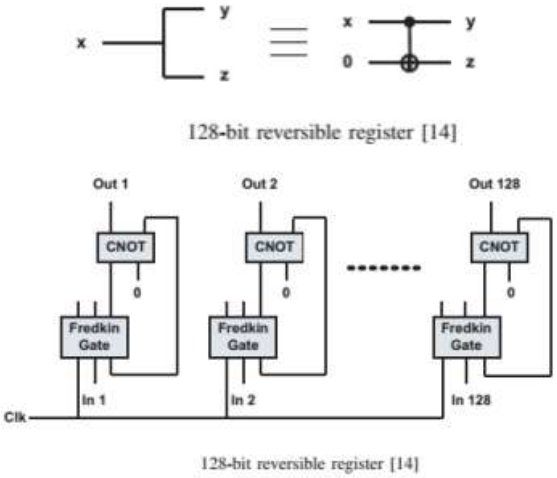

Figure 5: Reversible Register

V. IMPLEMENTATION

There are two basic approaches to mitigating NBTI: 1) reducing the stress on the pMOS transistors and 2) enhancing the recovery process. Stress reduction techniques aim to reduce the aging rate by controlling temperature, whereas recovery enhancement techniques aim to increase the recovery time. The pMOS devices. *Recovery*- A leakage lookup table is created by simulating all the gates in the standard cell library under all possible input patterns. Thus the leakage current Ileakage(v) can be expressed as: Ileakage(v) =XIN Il(v, IN) × Prob(v, IN) (19)where Il(v, IN) and Prob(v, IN) are the leakage current and the probability of gate v under input pattern IN. Determining MLV is proved to be NP-complete; both exact and heuristic approaches have been proposed to search for the MLV [10–12]. In this paper, we first find a set of MLV's using a simple probability based technique; then investigate the effects of different MLV's on the performance degradation due to NBTI; and finally MLV's that simultaneously achieve the minimum circuit performance degradation and the maximum leakage reduction rate are selected. The pseudo-code for our probability-based algorithm to select an MLV set is shown in Fig.3. The probability based algorithm starts by generating N random vectors; and the leakage current of each vector in the MLV set is within a given range of the minimum leakage current in the set. Next, for each primary input, the probability is calculated by the number of 1s out of the total number of vectors. New vectors are produced using the calculated probabilities. The leakage current of each new input vectors are calculated and the MLV set is updated. The probabilities for all primary inputs will converge to either 0 or 1, and it means that there is no probability of generating other vectors. So this is the convergence point of circuit leakage current and the algorithm is halted. Using a circuit logic simulator, the internal state of each edge can be calculated for each MLV. The _d(v) for a given period of time of each gate v is evaluated referring to Eq.(18) in Section 2.3.The timing and area overhead of the IVC technique, which is caused by the flip-flop at the primary inputs of the circuits, can be neglected for a large digital circuit design; however, for large circuits, the internal states can not be well controlled by the primary input vectors, thus the leakage variance due to different input combinations is not very large, and the MLV's may not result in a significant leakage reduction. Because of the same reason, various MLV's may not result in large difference of impact on circuit degradation. Lin et al. [13] pointed out that if the internal node deep in the circuit can be manipulated, greater leakage current reduction can be achieved. If the internal nodes can be controlled to reduce the leakage during the circuit standby mode, they can be also controlled to relieve the NBTI impact. Assuming all the PMOS's in the critical paths and near-critical paths are driven by the supply rail during the circuit standby mode (i.e., all PMOS devices are driven by'1'), the circuit performance degradation will be minimized.4 Simulation results In this section, we present the experimental results on ISCAS85 benchmarks. All ISCAS85 benchmark circuit netlists are synthesized using a commercial synthesis tool and mapped to a 90nm standard cell library. A leakage current lookup table of all the standard cells is generated using HSPICE. The 90nm standard cell library is constructed using the PTM90nm bulk CMOS model.

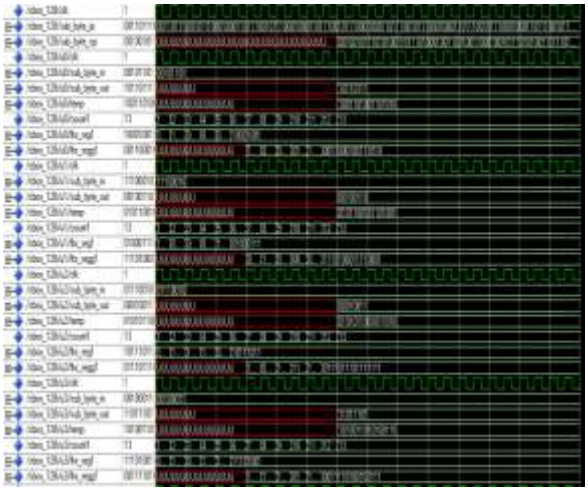

Figure 6: Waveform for the proposed NCL S-Box with input signals

Figure 7: Power waveform of NCL S-Box design.

Temperature: 27°C VDD: 1.8V	Synch S-Box	NCL S-Box
Total Power Dissipation (Watts) - Accusim+Eldo	2.474E-08	1.934E-08
Total Power Dissipation (Watts) - AdvanceMS	2.686E-08	1.961E-08

Simulation Results			
Mode	Input	Output	
		S-Box	NCL S-Box
Encrypt	9	00000001	0101010101010110
	26	10100010	1001100101011001
	106	00000010	0101010101011001
	122	11011010	1001101001101001
	158	00001011	0101010110011010
Decrypt	32	01010100	0110011001100101
	51	01100110	0110100101101001
	156	00011100	0101011010100101
	185	11011011	1010011010011010
	203	01011001	0110011010010110

Figure 8: Power simulation results for synchronous ES S-Box and NCL AES S-Box using Accusim and Advance MS.

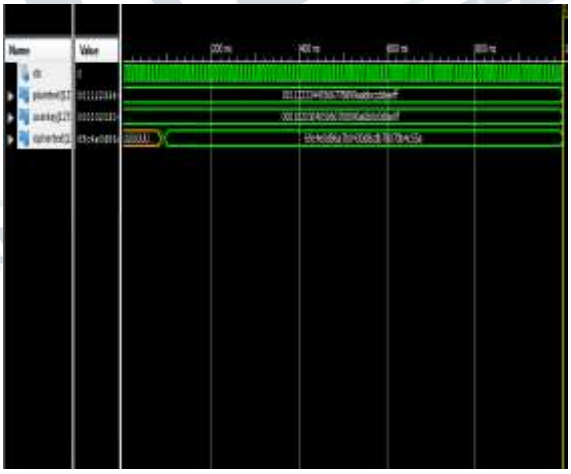

Figure 9: Simulation results for 10 arbitrary samples from conventional synchronous S-Box and the proposed NCL S-Box.

Table 2. NBTI-aware IVC technique

Circuits	Gate number	Nominal delay(ns)	Δdelay (%)	MLV difference (%)
c432	169	2.69	5.06	0.24
c499	204	1.99	5.62	0.17
c880	383	2.29	5.66	0.22
c1355	548	2.39	5.38	0.17
c1908	911	2.46	5.39	0.12
c2670	1279	2.99	5.58	0.20
c3540	1669	3.48	5.39	0.13
c5315	2329	2.94	5.28	0.20
c6288	2447	8.54	6.20	0.09
c7552	3566	2.30	5.27	0.10

Table 3: Delay degradation of ISCAS85 benchmarks under NBTI and potential of internal node control

ISCAS85 Benchmark Circuits	$T_{standby} = 400K$		$T_{standby} = 330K$	
	Max $\Delta delay(\%)$	Potential (%)	Max $\Delta delay(\%)$	Potential (%)
c432	8.41	3.41	5.42	0.565
c499	8.57	3.16	5.81	0.550
c880	8.65	3.16	5.92	0.602
c1355	8.46	3.27	5.60	0.544
c1908	8.44	3.38	5.53	0.602
c2670	8.60	3.15	5.86	0.562
c3540	8.48	3.22	5.66	0.524
c5315	8.46	3.24	5.56	0.499
c6288	8.90	3.06	6.44	0.748
c7552	8.42	3.28	5.51	0.507

VI. CONCLUSION

In this paper, we have proposed an improved temporal NBTI-induced performance degradation model for digital circuits. The power calculation for an AES S-Box have been analyzed. The standby mode temperature and the active and standby time ratio, which have significant effect on circuit performance degradation due to NBTI, are considered in our model for the first time. We study the impact of IVC technique (which leads to maximum leakage reduction during circuit standby mode on circuit performance degradation due to NBTI. The MLV has been calculated. It is further proposed to estimate the impact of NBTI on other encryption cores.

REFERENCES

[1] V. Huard, M. Denais, and C. Parthasarathy, "NBTI degradation:From physical mechanisms to modelling," Microelectronics Reliability, vol. 46, no. 1, pp. 1–23, 2006.

[2] J. Stathis and S. Zafar, "The negative bias temperature instability in MOS devices: A review," Microelectronics Reliability, vol. 46, no.2-4, pp. 270–286, 2006.

[3] G. Chen, M. Li, C. Ang, J. Zheng, and D. Kwong, "Dynamic NBTI of p-MOS transistors and its impact on MOSFET scaling," IEEE Elec. Dev. Lett., vol. 23, no. 12, pp. 734–736, 2002.

[4] S. Mahapatra, P. Bharath Kumar, T. Dalei, D. Sana, and M. Alam,"Mechanism of negative bias temperature instability in CMOS devices:degradation, recovery and impact of nitrogen," in Tech. Dig.Intl. Elec. Dev. Meeting, 2004, pp. 105–108.

[5] S. Mahapatra and M. Alam, "A predictive reliability model for PMOS bias temperature degradation," in Tech. Dig. Intl. Elec. Dev. Meeting, 2002, pp. 505–508.

[6] R. Vattikonda, W. Wang, and Y. Cao, "Modeling and Minimizationof PMOS NBTI Effect for Robust Nanometer Design," in Proc. Of Design Automation Conference, 2006, pp. 1047–1052.

[7] S. V. Kumar, C. H. Kim, and S. S. Sapatnekar, "An Analytical Model for Negative Bias Temperature Instability," in IEEE/ACM Intl. Conf. on Computer-Aided Design, 2006.

[8] S. Kumar, C. Kim, and S. Sapatnekar, "Impact of NBTI on SRAM Read Stability and Design for Reliability," in Intl. Symp. on Quality Electronic Design, 2006, pp. 210–218.

[9] B. Paul, K. Kang, H. Kufluoglu, M. Alam, and K. Roy, "Temporal Performance Degradation under NBTI: Estimation and Design for Improved Reliability of Nanoscale Circuits," in Proc. of Design, Automation and Test in Europe, vol. 1, 2006, pp. 1–6.

[10] A. Abdollahi, F. Fallah, and M. Pedram, "Leakage current reduction in CMOS VLSI circuits by input vector

control," IEEE Trans. On Very Large Scale Integration (VLSI) Systems, vol. 12, no. 2, pp. 140–154, 2004.

[11] F. Gao and J. Hayes, "Exact and heuristic approaches to input vector control for leakage power reduction," in IEEE/ACM Intl. Conf. on Computer Aided Design, 2004, pp. 527–532.

[12] R. Rao, F. Liu, J. Burns, and R. Brown, "A heuristic to determine low leakage sleep state vectors for CMOS combinational circuits," in IEEE/ACM Intl. Conf. on Computer Aided Design, 2003, pp. 689–692.