Utilizing NBTI for Operation Detection of Integrated Circuits

Ambika Prasad Shah(✉), Amirhossein Moshrefi, and Michael Waltl

Institute for Microelectronics, TU Wien, Vienna, Austria
ambika_shah@rediffmail.com, {moshrefi,waltl}@iue.tuwien.ac.at

Abstract. Counterfeiting of integrated circuits (ICs) has become a serious challenge in recent years, as the reuse of devices can affect the reliability and security of electronic systems. This is of particular importance for military, space, and financial applications. Nevertheless, it can be very difficult to detect recycled ICs, especially when they have been used for only a short period of time. To detect the reuse of ICs, we take advantage of the fact that the threshold voltage of single PMOS transistors change over time due to Negative Bias Temperature Instability (NBTI). As a consequence of a pure drift of the threshold voltage towards higher values, the standby leakage current decreases over time. We analyze the change of the standby leakage current of the c17 ISCAS'85 benchmark suite employing the PTM model implemented in HSPICE to estimate the operational time of the chip. Our results clearly demonstrate that the standby leakage current for worst case and minimum stress conditions increases by 20.5% and 10.08% after the stress time of 3 years, respectively. Thus the thorough investigation of the standby leakage current provides a measure for the operational time analysis of ICs.

Keywords: NBTI · Circuit simulation · Standby leakage current · Counterfeit · Recycled chip · Reliability · ISCAS'85 benchmark circuit

1 Introduction

The counterfeiting of Integrated Circuits (ICs) has been increased over the last decades and could not only affect the stable operation of integrated circuits but furthermore cause security leaks of electronic systems. Based on the recent report by the International Chamber of Commerce, the value traded for counterfeit and pirated goods could reach $991 billion by 2022 [1]. One major concern for counterfeiting is its negative impact on innovation, but might also lead to a lowering of employment and economic growth [2]. On the other hand, according to January 2019 report from the World Economic Forum, e-waste is now the

The research leading to this work has received substantial funding from the Take-off program of the Austrian Research Promotion Agency FFG (projects no. 861022 and 867414).

A. Sengupta et al. (Eds.): VDAT 2019, CCIS 1066, pp. 190–201, 2019.
https://doi.org/10.1007/978-981-32-9767-8_17

fastest growing waste in the world. Apparently, only 20% of global e-waste is formally recycled, but this could be significantly increased by reusing of electronic systems [3].

There are various types of counterfeit for electronic systems, for instance the ICs can be recycled, remarked, overproduced, cloned, tampered, etc. [4]. Among these, the recycled and remarked electronic components together cover more than 80% of counterfeit of the individual components [5]. However, counterfeiting of ICs is not straight-forward and might also suffers from the lack of proper test solution to prevent fraudulent of them. Thus a unique way for testing and detection of unwanted recycling of electronics systems has to be created to control the boom of counterfeiting ICs. So far, several detection techniques to identify recycled ICs have been proposed. Zhang et al. [6] proposed a path-delay fingerprinting approach for identifying recovered ICs by calculating the delay of fast aging gates. In [7], Guo et al. have used a SRAM cell which appeared most sensitive to aging mechanisms for the detection of possibly recycled ICs. In common, these two techniques are based on the statistical data analysis and require a pre-analysis of large number of pristine circuits. Zhang et al. [8] proposed a ring oscillator (RO) based light weight on-chip sensor to detect the reuse of ICs. This design contains a reference RO next to the normally used ROs, as the different structures ages with different rates, this can be used to detect counterfeit of electronics. However, although this approach is effective, it requires additional on-chip hardware and hence cannot be used for existing structures which are in use and already circulating in the market.

A new approach could take advantage of the aging of single transistors of the circuits over time. In detail, we use the change in parameters of the ICs due to Negative Bias Temperature Instability (NBTI) of individual transistors to detect possibly recycled ICs. Due to NBTI, the threshold voltage of PMOS transistor drifts over time, and if pure NBTI degradation is considered, the standby leakage current (I_{ddq}) of the transistor decreases at the same time [9,10]. This decrease of I_{ddq} over time can be used as the parameter for detecting the operational time of the IC. So far we estimate the I_{ddq} of the entire chip by performing circuit simulations for a large number of transistors. To demonstrate the proposed methodology, we use c17 circuit from ISCAS'85 benchmark suite [11] and calculate the critical path, which is exposed to the worst case stress conditions, of the circuit, and compare the steady power consumption to the minimum stress case. Finally, we clearly reveal a significant reduction in the steady power consumption of the degraded circuit, which enables to detect the reuse of electronic chips.

2 ISCAS'85 c17 Benchmark Circuit

Figure 1 shows the circuit for c17 from the ISCAS'85 benchmark suite which consists of six NAND gates and is used for further analysis. For the c17 circuit one has to identify the critical path where the most PMOS transistors are stressed during normal operation. For this, the inputs of the single NAND gates are

analyzed next. As we primarily focus on the NBTI for PMOS case, the transistors are stressed when a logical low state is applied at the respective inputs of the NAND blocks. Figure 2 shows the probabilities of getting logic high at each node of the circuit, P_1 through P_{11}, and are computed by applying all possible input pattern combinations to the inputs (I[1]–I[5]) of the circuit. Here P_i is the ratio of the number of 1's on the line i to the total number of input patterns. For this circuit, the total number of combinations are $2^5 = 32$. The signal probabilities for all the inputs are considered to be 0.5 as the probability of primary input being 0 or 1 is assumed to be equal.

The total degradation of the PMOS transistor due to NBTI depends on the input signal probability. The impact of NBTI on the entire c17 circuit depends on the input and output signal probability of each NAND gate, which is again the input probability of a subsequent NAND gate. The output signal probability for a logic '1' input of each NAND gate can be express as [12]

$$P(Y = 1) = 1 - P_{\mathrm{A}} P_{\mathrm{B}}. \tag{1}$$

where P_{A} and P_{B} are the input signal probabilities for being logic '1' at the inputs of the respective NAND gate. Considering Fig. 2, it can be observed that the gates G1 and G2 have the highest probability to be stressed, as one or both inputs see the logic '0' state more frequently than the inputs of other NAND gates. NAND gate G5 has the minimum probability of being stressed during operation. The NAND gates which are stressed mostly during operation are highlighted in red whereas NAND gate which are exhibit only minimum stress is highlighted in green.

For worst case stress patterns and the minimum stress patterns of the twelve PMOS transistors of six NAND gates of the c17 circuit are summarized in Table 1. There are two input patterns for each case, which are used for further analysis of the degradation of the c17 circuit.

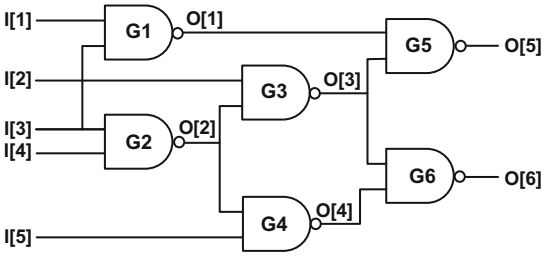

Fig. 1. c17 circuit from ISCAS'85 benchmark suite. G1-G6 are the two input NAND gates. I[1]–I[5] are the circuit inputs, O[1]–O[4] are the intermediate outputs of the single nodes, and O[5]–O[6] are the outputs of the entire circuit.

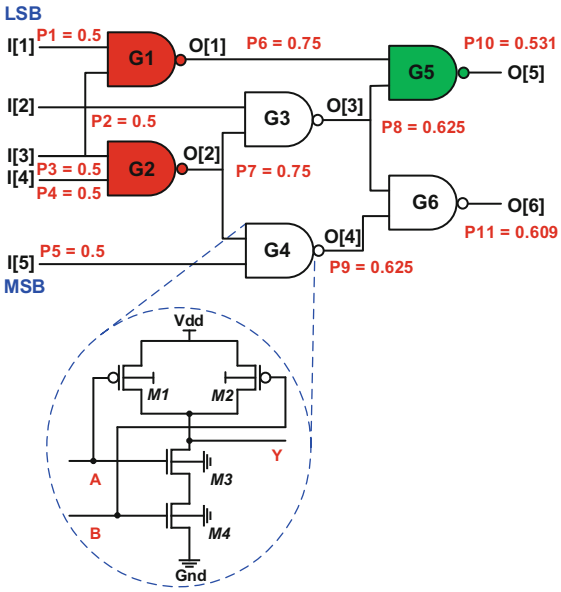

Fig. 2. Input and output signal probabilities for six NAND gates in c17 circuit. It has to be noted, that the PMOS devices are stressed when a logic '0' is applied at the respective inputs. (Color figure online)

Table 1. Stressed PMOS transistors (M_1 and M_2) in all NAND gates of c17 circuit for the four extreme input patterns

NAND gates	Maximum stress		Minimum stress	
	00010	10010	11110	11111
G1	M_1, M_2	M_1, M_2	M_1	–
G2	M_1, M_2	M_1, M_2	–	–
G3	–	–	M_2	M_2
G4	M_2	–	M_1	M_1
G5	M_2	M_2	–	M_1
G6	M_1	M_1, M_2	–	–

2.1 Static Timing Analysis of the c17 Circuit

Static timing analysis (STA) is one of the techniques to verify the timing of a digital design. STA is used at the gate level to derive the faults caused due to cross-talk delay effects [13]. The numbers of cross-talk faults between all possible combinations of inputs in a digital VLSI circuit can be very large and thus impractical to detect for large complex circuits. Therefore static timing analysis is typically used to get a reduced set of cross-talk delay faults [13]. The tree data structure is used to analyze the entire paths in the circuit more

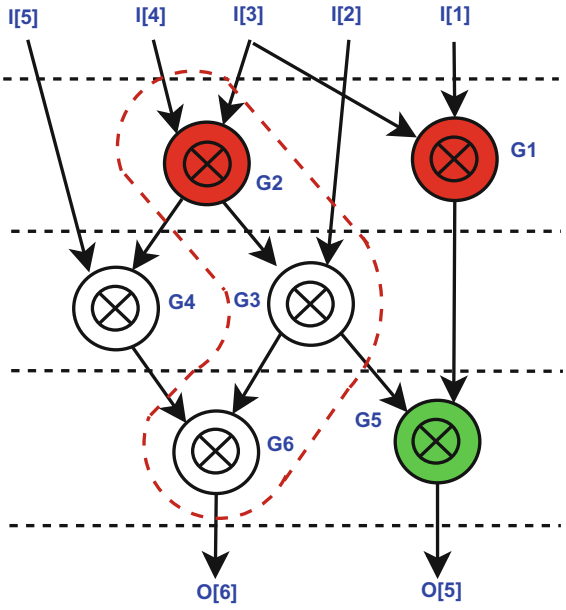

Fig. 3. Dataflow graph (DFG) for critical path of c17 benchmark circuit.

detailed. To calculate the total number of paths in the circuit the depth-first search algorithm is used. A set of critical paths from the total number of paths are detected which exhibit the largest delay of all the paths.

In VLSI design, data-flow graph (DFG) is typically used to represent the circuit netlist. The use of DFG is extended for logic synthesis, design verification, timing analysis, and post-manufacturing testing. DFGs can also be used for timing analysis of the c17 benchmark circuit [14], as shown in Fig. 3. By performing an STA, we note that the path I[4] → G2 → O[2] → G3 → O[3] → G6 → O[6] is the critical timing path for the underlying c17 circuit. The longest paths for the c17 circuit are indicated by the enclosed loop line, as shown in Fig. 3. We used this critical path for calculating the maximum delay of the circuit. Further, out of the two NAND gates, which exhibit the worst case stress conditions G1 and G2, the latter is part of the critical path and thus used for further analysis more closely.

2.2 Steady Leakage Current (I_{ddq}) Model for NAND Gate

Figure 4 shows the two input CMOS NAND gate with inputs A, B and output Y. In addition all the leakage current components present in the circuit for the four possible input bit combinations are also shown we have considered the subthreshold leakage current, the gate leakage and the junction leakage current for further analysis, as these are the major leakage current components [15]. The sum of all the components for each transistor for each particular input

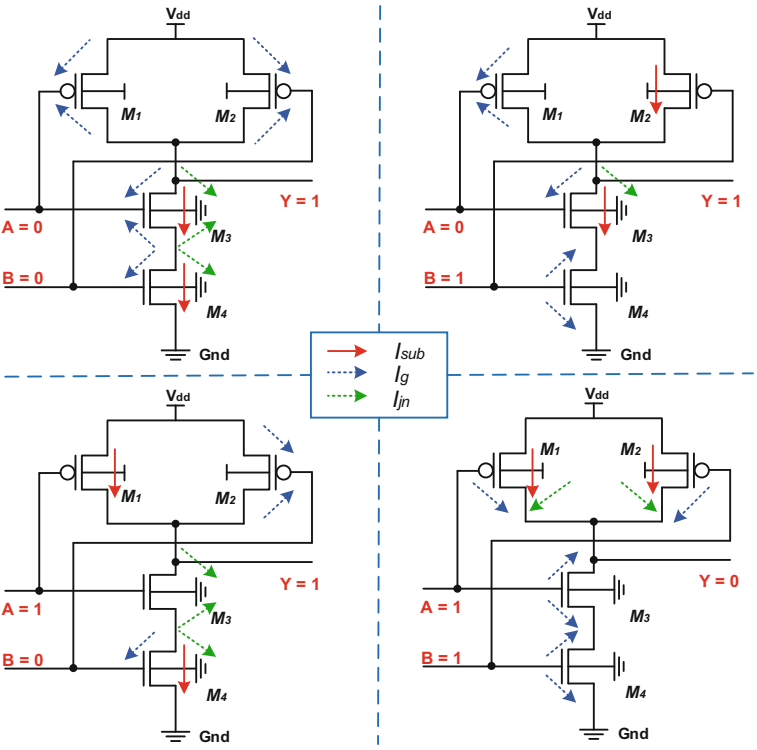

Fig. 4. Standby leakage current (I_{ddq}) model of a two input NAND gate for four different input combinations is shown. The currents I_{sub}, I_{g} and I_{jn} are the subthreshold leakage current, gate leakage current, and junction leakage current, respectively.

combination is considered as the overall standby leakage current, and can be calculated as follows:

Case 1: For $A = B = 0$

$$I_{\mathrm{sub}_{00}} = I_{\mathrm{sub}_{\mathrm{M3}}} + I_{\mathrm{sub}_{\mathrm{M4}}} \tag{2}$$

$$I_{\mathrm{g}_{00}} = \sum_{x=1}^{4} I_{\mathrm{gd}_{\mathrm{M}x}} + \sum_{y=1}^{3} I_{\mathrm{gs}_{\mathrm{M}y}} \tag{3}$$

$$I_{\mathrm{jn}_{00}} = I_{\mathrm{jns}_{\mathrm{M3}}} + I_{\mathrm{jnd}_{\mathrm{M3}}} + I_{\mathrm{jnd}_{\mathrm{M4}}} \tag{4}$$

$$\boldsymbol{I_{\mathrm{ddq}_{00}} = I_{\mathrm{sub}_{00}} + I_{\mathrm{g}_{00}} + I_{\mathrm{jn}_{00}}} \tag{5}$$

Case 2: For $A = 0, B = 1$

$$I_{\mathrm{sub}_{01}} = I_{\mathrm{sub}_{\mathrm{M2}}} + I_{\mathrm{sub}_{\mathrm{M3}}} \tag{6}$$

$$I_{g_{01}} = \sum_{x=1}^{3} I_{gd_{Mx}} + I_{gs_{M1}} + I_{gs_{M3}} \tag{7}$$

$$I_{jn_{01}} = I_{jnd_{M1}} \tag{8}$$

$$\boldsymbol{I_{ddq_{01}} = I_{sub_{01}} + I_{g_{01}} + I_{jn_{01}}} \tag{9}$$

Case 3: For $A = 1, B = 0$

$$I_{sub_{10}} = I_{sub_{M1}} + I_{sub_{M4}} \tag{10}$$

$$I_{g_{10}} = I_{gd_{M2}} + I_{gs_{M2}} + I_{gd_{M4}} \tag{11}$$

$$I_{jn_{10}} = I_{jnd_{M3}} + I_{jns_{M3}} + I_{jnd_{M4}} \tag{12}$$

$$\boldsymbol{I_{ddq_{10}} = I_{sub_{10}} + I_{g_{10}} + I_{jn_{10}}} \tag{13}$$

Case 4: For $A = B = 1$

$$I_{sub_{11}} = I_{sub_{M1}} + I_{sub_{M2}} \tag{14}$$

$$I_{g_{11}} = \sum_{x=1}^{4} I_{gd_{Mx}} + \sum_{y=3}^{4} I_{gs_{My}} \tag{15}$$

$$I_{jn_{11}} = I_{jnd_{M1}} + I_{jnd_{M2}} \tag{16}$$

$$\boldsymbol{I_{ddq_{11}} = I_{sub_{11}} + I_{g_{11}} + I_{jn_{11}}} \tag{17}$$

Table 2 summarizes the different leakage current components present for the different input combinations for the two input NAND gate. The cross (×) represent the absence of any leakage component, a checkmark (✓) represent the presence of subthreshold leakage component, bullet (•) and circle (○) represent the gate and junction leakage components for source and drain side, respectively. Table 3 summarizes the resulting steady leakage current I_{ddq} for the four different input combinations of the two input NAND gate. I^{N}_{sub}, I^{N}_{jn}, I^{N}_{g} and I^{P}_{sub}, I^{P}_{jn}, I^{P}_{g} represents the subthreshold leakage current, the junction leakage current, and the gate leakage current components for the NMOS and PMOS transistors, respectively. Please note, that only the PMOS transitors leakage current are considered to change over time due to NBTI, whereas the NMOS leakage currents are considered stable in our analysis.

2.3 Effect of NBTI on the Steady Leakage Current (I_{ddq})

With the scaling of CMOS technology, variability and reliability issues of single transistors become more and more important for the performance and lifetime of integrated circuit. In this context, NBTI and positive BTI (PBTI) play an important role for NMOS and PMOS devices. However, extensive experimental investigations demonstrated that the effect of NBTI in PMOS is more sizable compared to the PBTI in NMOS case and is thus considered to be the dominant

Table 2. Presence of leakage current components for a NAND gate

Transistor	Leakage components	Input (A, B)			
		00	01	10	11
$M1$	I_{sub}	×	×	✓	✓
	I_{g}	● ○	● ○	×	○
	I_{jn}	×	×	×	○
$M2$	I_{sub}	×	✓	×	✓
	I_{g}	● ○	×	● ○	○
	I_{jn}	×	×	×	○
$M3$	I_{sub}	✓	✓	×	×
	I_{g}	● ○	○	×	● ○
	I_{jn}	● ○	○	● ○	×
$M4$	I_{sub}	✓	×	✓	×
	I_{g}	○	● ○	○	● ○
	I_{jn}	○	×	○	×

Table 3. Standby leakage current (I_{ddq}) model for 2 input NAND gate

A	B	I_{ddq}
0	0	$4I_{\text{g}}^{\text{P}} + 2I_{\text{sub}}^{\text{N}} + 3I_{\text{jn}}^{\text{N}} + 3I_{\text{g}}^{\text{N}}$
0	1	$I_{\text{sub}}^{\text{P}} + 2I_{\text{g}}^{\text{P}} + I_{\text{sub}}^{\text{N}} + I_{\text{jn}}^{\text{N}} + 3I_{\text{g}}^{\text{N}}$
1	0	$I_{\text{sub}}^{\text{P}} + 2I_{\text{g}}^{\text{P}} + I_{\text{sub}}^{\text{N}} + 3I_{\text{jn}}^{\text{N}} + I_{\text{g}}^{\text{N}}$
1	1	$2I_{\text{sub}}^{\text{P}} + 2I_{\text{jn}}^{\text{P}} + 2I_{\text{g}}^{\text{P}} + 4I_{\text{g}}^{\text{N}}$

limiting factor of a device/circuit lifetime [16]. NBTI refers to the stress case for PMOS transistors when a negative bias is applied across at the transistor's gate contact. This negative bias can trigger the creation of so called interface states and oxide defects, which lead to a drift of the threshold voltage, reduction of the sub-threshold slope and to a reduction of the on-current [16]. When the gate stress is released the shift of the threshold voltage accumulated during stress recovers partially, but also permanent degradation of the threshold voltage after each stress cycle is observed. The latter can lead to a significant permanent shift of the threshold voltage of PMOS over time, which can introduce some uncertainty in the device/circuit behavior and thus decrease the device/circuit lifetime. By considering a drift of the threshold voltage only, this behavior can cause a reduction of the standby leakage current of the transistor and hence a reduction of the overall I_{ddq} of the complete chip when the chip is used for a long time [10].

Following up the previous identification of the NAND gates which undergo the worst case stress conditions of the analyzed c17 circuit, we now want to take the change of the threshold voltage during device operation into account. As

discussed, G2 and G5 are the NAND gates which are exhibited to the worst case and minimum stress conditions, respectively. Thus the maximum change in the steady power consumption follows from

$$\Delta I_{\mathrm{ddq}} = \left| I_{\mathrm{ddq}}|_{G_2} - I_{\mathrm{ddq}}|_{G_5} \right|. \tag{18}$$

When chip ages, I_{ddq} from G5 will decrease rapidly, whereas the I_{ddq} from G2 will not change as much. This will unavoidably result in an increase of ΔI_{ddq} which gets larger the longer the chip gets used.

In order to analyze the maximum change of the steady leakage current, the test pattern that selects the PMOS transistors leakage of fast aging gates, i.e. worst stress conditons, is identified (index F). Similarly, we also select a second test pattern that selects the PMOS transistors with the smallest leakage current increase, i.e. slow aging gates (denoted with index S).

The normalized ΔI_{ddq} for all the combinations are finaly used to detect the recycled IC and is calculated to

$$\Delta I = \frac{I_{\mathrm{S}} - I_{\mathrm{F}}}{I_{\mathrm{S}} + I_{\mathrm{F}}}. \tag{19}$$

3 Simulation Results and Discussion

To demonstrate the effectiveness of the proposed approach for detecting recycled ICs, the PTM 32 nm CMOS technology is used [17]. For the analysis of the device stress, the HSPICE MOSRA model has been used [18]. All the simulations are performed at an elevated temperature ($\mathrm{T} = 125\,^{\circ}\mathrm{C}$) for the stress time of three years.

Figure 5 shows the power dissipation of c17 benchmark circuit for input bit combinations leading to either the maximum or the minimum number of PMOS transistors stressed simultaneously. From results it is observed that the c17 has the maximum number of PMOS transistors is stressed for input combinations, '00010' and '10010'. From these bit-combinations the maximum power dissipation is for bit-combination '00010'. Similarly, if we consider the minimum number of PMOS transistor under stress, then the c17 has the minimum power dissipation, which is obtained for the input bit combination '11111'. From the maximum stress input pattern, it is also observed that the NAND gate G2 is always the one with the maximum stress as input I[3] and I[4] are always low for all the considered input bit combinations. Figure 5 furthermore reveals that the c17 circuit has the minimum power dissipation for the input bit-patterns '10010' and '11111' for the maximum and minimum number of stressed PMOS transistors, respectively. Thus these two combinations are considered as the fast aging pattern (T_{F}) case and the slow aging pattern (T_{S}) case.

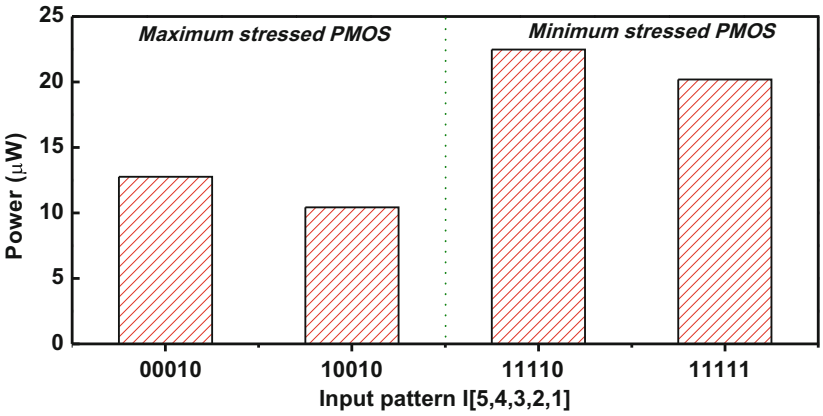

Fig. 5. c17 circuit power dissipation for the input patterns having maximum and minimum number of PMOS are under stress. As can be seen, the steady power consumption tends to decrease for the heavily stressed case.

Figure 6 shows the 5000 Monte Carlo simulations for analyzing the power consumption for different input patterns. As can be seen, the input patterns '00010' and '11110' have the highest deviation for the maximum and the minimum number of stressed PMOS, respectively, whereas the input pattern, '10010' and '11111' have the minimum deviation for the maximum and the minimum number of stressed PMOS, respectively. As we primarily focus on the analysis of the standby leakage current for estimating the lifetime of IC; we will consider the input patterns which exhibit less variation. The input pattern with respect to maximum degradation due to NBTI is '10010' and considered as a first test pattern (T_{F}). Similarly, for the reference input pattern '11111' is considered as the second test pattern (T_{S}), which shows only a small variation in the power consumption and furthermore triggers the c17 circuit path with minimum number of stressed PMOS devices.

Table 4 shows the normalized steady leakage current I_{ddq} based on the selected input patterns for the pristine, as well as stressed c17 circuit. One can observe that I_{F} reveals the higher effect of stress compared to I_{S}. The decrement in both, I_{F} and I_{S}, after three years of stress is 20.5% and 10.08%, respectively. Furthermore it can be observed that the ΔI increases with stress time. The $\Delta I\%$ for fress simulation is 77.88%, and it increases to 80.12% after the stress time of three years. Following from this trend, this cleverly method allows to detect whether the underlying electronic devices is in its virgin, or the device has already been used.

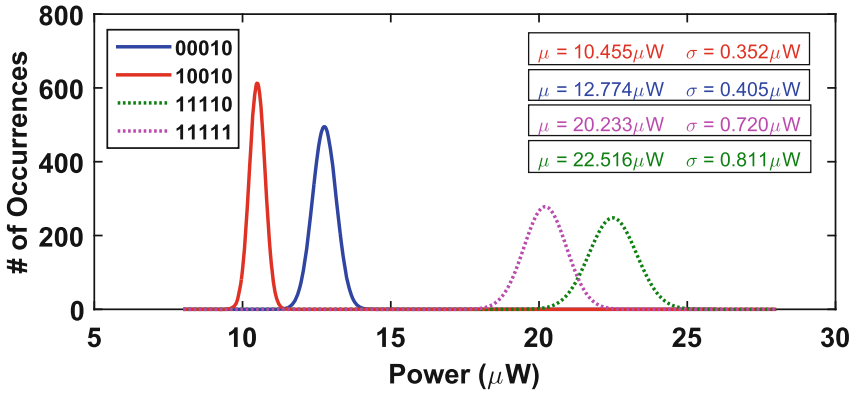

Fig. 6. Monte carlo distribution of c17 circuit power for the input patterns having maximum and minimum number of PMOS are under stress.

Table 4. Normalized I_{ddq} for new and used c17 circuit

Usage Time ↓	I_F (nA)	I_S (nA)	$\Delta I(\%)$
Fresh	1.824	14.67	77.88
1 Year	1.54	13.51	79.58
2 Years	1.49	13.31	79.90
3 Years	1.45	13.19	80.12

4 Conclusion

Counterfeiting of ICs might give rise for instable electronic applications but also might cause severe security leaks. To detect if any electronic circuit is still in its pristine state or has already been used a new approach based on analysis of the circuit's steady power consumption is discussed. Device aging is considered due to NBTI and is applied to the c17 benchmark circuit. For the analysis, the input patters leading to worst case stress conditions and minimum overall device stress are identified. Finally, the comparison of the standby leakage consumption for both cases clearly reveal that a significantly reduced standby power consumption is observed for the used devices compared to the pristine ones. This finally enables to distinguish between pristine and recycled integrated electronics circuits.

References

1. The economic impacts of counterfeiting and piracy. https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf. Accessed 09 Mar 2019
2. Frontier Economics: The economic impacts of counterfeiting and piracy. Frontier Economics, Melbourne (2017)

3. A New Circular Vision for Electronics. http://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf. Accessed 09 Mar 2019
4. Guin, U., DiMase, D., Tehranipoor, M.: Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. J. Electron. Test. **30**(1), 9–23 (2014)
5. Kessler, L.W., Sharpe, T.: Faked parts detection. Printed Circ. Des. Fab **27**(6), 64 (2010)
6. Zhang, X., Xiao, K., Tehranipoor, M.: Path-delay fingerprinting for identification of recovered ICs. In: 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp. 13–18. IEEE (2012)
7. Guo, Z., Rahman, M.T., Tehranipoor, M.M., Forte, D.: A zero-cost approach to detect recycled SoC chips using embedded SRAM. In: 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 191–196. IEEE (2016)
8. Zhang, X., Tehranipoor, M.: Design of on-chip lightweight sensors for effective detection of recycled ICs. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **22**(5), 1016–1029 (2014)
9. Shah, A.P., Yadav, N., Beohar, A., Vishvakarma, S.K.: Process variation and NBTI resilient schmitt trigger for stable and reliable circuits. IEEE Trans. Device Mater. Reliab. **18**(4), 546–554 (2018)
10. Kang, K., Alam, M.A., Roy, K.: Characterization of NBTI induced temporal performance degradation in nano-scale SRAM array using I_{ddq}. In: 2007 IEEE International Test Conference, pp. 1–10. IEEE (2007)
11. ISCAS'85 Benchmark Circuits. http://www.pld.ttu.ee/~maksim/benchmarks/iscas85/. Accessed 9 Apr 2019
12. Ghavami, B., Raji, M., Saremi, K., Pedram, H.: An incremental algorithm for soft error rate estimation of combinational circuits. IEEE Trans. Device Mater. Reliab. **18**(3), 463–473 (2018)
13. Bhuvaneswari, M.C.: Application of Evolutionary Algorithms for Multi-objective Optimization in VLSI and Embedded Systems. Springer, Heidelberg (2014). https://doi.org/10.1007/978-81-322-1958-3
14. Neophytou, S.N., Michael, M.K.: Path representation in circuit netlists using linear-sized ZDDs with optimal variable ordering. J. Electron. Test. **34**(6), 667–683 (2018)
15. Islam, A., Hasan, M.: Leakage characterization of 10T SRAM cell. IEEE Trans. Electron Devices **59**(3), 631–638 (2012)
16. Schroder, D.K.: Negative bias temperature instability: what do we understand? Microelectron. Reliab. **47**(6), 841–852 (2007)
17. Zhao, W., Cao, Y.: Predictive technology model for nano-CMOS design exploration. ACM J. Emerg. Technol. Comput. Syst. (JETC) **3**(1), 1 (2007)
18. Synopsys: HSPICE user guide: Simulation and analysis (2010)