Implementation of 32nm MD5 Crypto-Processor using Different Topographical Synthesis Techniques and Comparison with 500nm Node

Juan-Jose Jimenez, Andre Borja, Laetitia Silly, Luis-Miguel Procel, Lionel Trojman, Ramiro Taco

Implementation of 32nm MD5 Crypto-Processor using Different Topographical Synthesis Techniques and Comparison with 500nm Node

Juan-José Jimenéz; André Borja; Laetitia Silly; Luis-Miguel Prôcel; Lionel Trojman; Ramiro Taco

***Abstract*— This work focuses on several synthetizations developed in both 32nm and 500nm technologies to evaluate the performance differences of MD5 Crypto-Processor. We decided to conduct a topographical synthesis instead of a non-topographical synthesis as it takes more parameters into account to create a more accurate design. We started by comparing some basic cells like inverters and register banks to understand the main differences between the two technologies. Several approaches were considered at this point to understand how different synthetization parameters affect the chip performance and characteristics. These different approaches were focused on time, power and area, and balanced configurations of synthesis flow. Finally, after comparing the performance given by the different approaches in basic digital structures, the balanced approach was implemented in 32nm and benchmarked with the 500nm implementation. Our conclusions were consistent among the various tests conducted and by downscaling we can expect a 10x increase in the clock frequency, a 100x decrease in power consumption, and around a 300x decrease in the area while using the 32nm technology. As a result, we developed a method to fairly compare complex systems to allow a designer to consider if the benefits justify the costs for a technology change.**

***Keywords*— Topographical Synthesis, 32nm Technology, Synthesis Guide, Integrated Circuit, MD5, Synopsys, Technology Scaling.**

I. Introduction

THIS paper aims to implement a 32nm CMOS technology in an ASIP (Application Specific Instruction Processor) for cryptography applications. To create an IC (Integrated Circuit) of an ASIP, it is necessary to follow a digital design flow that starts with the synthesis process [1]. The synthesis of a digital circuit is the process that ends with the design of a customized netlist for the creation of a circuit. Either for an FPGA-like processor or an ASIP, both start with a physical description of the desired hardware, done in HDL (Hardware Description Language). Via software, a netlist is created from this information, and it serves as a map for how the logical cells shall be connected to satisfy the initial hardware description [2].

In previous work with this methodology, we could implement an MD5 algorithm 500nm technology node (Open-Source) ASIP [3]. this MD5 cryptoprocessor was implemented to test different FSM (Finite State Machine). Thanks to its application of combinational and sequential logic, this cryptoprocessor showcases a common real-life application.

However, the implementation of such ASIP in 32nm is not straightforward. Indeed, the lower technology node library includes a more detailed description of the physics of the MOSFET and therefore this led the designers to a different method for more accurate hardware synthesis.

An alternative is to use a topographical synthesis that includes extra parameters. These ones allow a more accurate design of the netlist and a therefore a more accurate representation of the chip [4-5]. These extra parameters are the physical limitations of individual logic cells and design rules of the technology being implemented.

Topographical synthesis even contemplates the physical distance between individual gates while creating the netlist. Since a common goal on each step of the digital design flow of an IC is to have a more accurate representation of the real hardware to avoid detrimental effects, when possible, topographical synthesis is then a useful tool. In this work, we decided to implement a 32nm ASIP based on our previous design in 500nm [3] but using a topographical perspective with a more comprehensive understanding of the 32nm technology library.

This paper is divided into 3 parts. In the first part, we will analyze some basic building blocks in 32nm technology. This analysis will be done to have a basic understanding of some physical and electrical parameters. We will then analyze an inverter and a registered bank in this technology. As expected in terms of performance the 32nm outrate the 500nm one. As a matter of fact, we obtain a data arrival time of up to 75 times less than its counterpart.

The inverter was chosen since it is the basic building block of any process with combinational logic as the inverter is part of every logic cell. A register bank is chosen

since it has a dependence on a clock signal and will give us an initial idea of how sequential blocks work. The results will be compared to the ones of a 500nm (Open-Source) technology from [6].

Then, the second part will take various approaches to compare the results. We will start with the implementation of the cryptoprocessor in the 32nm technology with a basic test and then with a full optimization topological synthesis test. Then we will take 3 optimization approaches. They will be a time-focused, power and area, and lastly a balanced approach between the two of them [7-8].

Once we find a well-rounded netlist from the different topographical synthesis approaches, in stage three we will compare it to the original 500nm technology to assess the results of technology scaling to find the quantitative differences. All the simulations will be carried out with DC – Compiler from Synopsys. Finally, there will be a discussion of the results of technology scaling, as well as the changes we might expect for different optimizations approaches when creating an IC in a 32nm technology [9].

II. Synthesis in 500nm and 32nm Technologies

As it is expected from a technology scaling process from 500nm to 32nm, several electrical parameters that would be consistent with the reduction in the technology node. The usual improvements that one can expect from a reduction in technology are size and power reduction, as well as a speed increase. The size reduction is evident as smaller technologies have smaller standard cells. The power reduction is usually due to a reduction of the driving voltage required for a high-digital value and by lower driving currents among the different cells. Another effect of this smaller range between the low and high voltages required for the digital values becomes easier and faster. This might allow us to increase clock frequency to values that the older technologies were not able to sustain correctly [9-10].

However, to compare different technologies, we need a custom-specific instruction processor to test among both technologies. To do this, a crypto-processor that implements a reduced version of the MD5 algorithm on an integrated circuit was chosen. As mentioned, this MD5 crypto-processor [3] showcases a common real-life application.

A. MD5 Crypto-Processor

This studied ASIP replicates the MD5 hashing algorithm but instead of using a 512-bit word as an input like in the original algorithm (Fig. 1), we use a 16-bit input but maintains all the different logical functions to encrypt the input into an 8-bit encrypted output. In this specific topology [3], counters in the control module's FSM of the chip were introduced to reduce chip area, and power consumption. The same topology strategy is applied for the 32nm crypto-processor. It is worth, since in our previous work, the MD5 ASIP was implemented in the Open Source library of 500nm from [6]. This ASIP takes an input and with the guidance of the control module and performs several operations and logical functions to perform an individual task. This process has both sequential blocks as well as combinational blocks and requires 139 steps to fully encode a result [3]. Such variety gives us a well-balanced application that will test the different technologies in parameters such as time, frequency, area, among others.

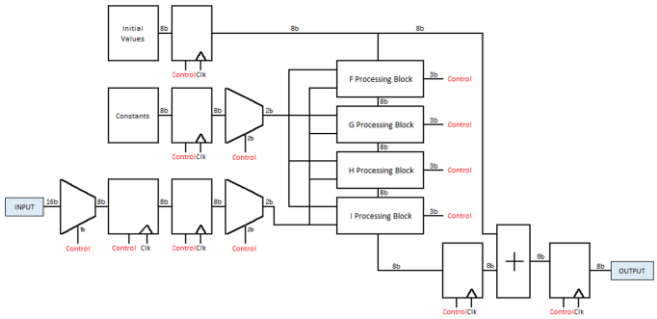

Fig. 1. Combinational Logic Modules with Inputs from the Control Module

B. Different Topographical Synthesis Approaches.

The simulation of several known digital circuits to determine the benefits of topographical synthesis and to observe if the difference in the results of these 32nm technology cells and compare them with their 500nm counterparts.

The crypto processor will be topographically synthesized utilizing RVT (Regular Voltage Threshold) 32nm libraries. However, different approaches will be considered to assess the effect on the final microprocessor [11-12]. We will analyze a time-focused approach, power and area-focused approach, and finally, a balanced one to compare them and find the expected tradeoff between the parameters. Once one approach is chosen, it will finally be compared with the original 500nm technology implementation of the MD5 to quantify all the differences between these two technologies.

III. ASIP Description and Topographical Methodology

In this work, the entire synthesis process was carried out using Synopsys tools, through Design Compiler (DC) tool which account with a topographical synthesis technology (DCT). This tool allows physical constraints to be included during the synthesis process, simulating a more accurate microprocessor.

For the starting tests, an inverter and an 8-bit register bank were first synthesized. This will allow to understand how the 32nm technology behaves for the design. However, the most important analysis will be the different approaches considered with the TCAD. Different parameters will shape up the netlist. These approaches will be defined in the next sub-section.

A. Topographical Synthesis Simulation Techniques

The first analysis was to determine the changes one can achieve with the topographical synthesis in contrast with a regular synthesis. Through Table I, the techniques applied to the different synthesis parameters are mentioned. In the case of the basic synthesis, optimization techniques were not used since many of them are only available in the topographic synthesis. In the second case, all the optimization methods available in DCT were applied, maintaining a balance in minimizing time, area, and power.

The DCT technology analysis was used not only to introduce restrictions but also to establish synthesis constraints based on time, power and area criterion to custom the optimization. Then, three topographic synthesis approaches on the MD5 ASIC to evaluate the behavior and robustness of the 32nm technology for a complex circuit.

TABLE I. TEST CONDITIONS FOR COMMON DIGITAL CIRCUIT TEST

Synthesis Parameter	Basic Test	Full-Optimization Test
Synthesis Technique (Optimization)	Compile	Compile_ultra
Retiming Technique	No	Optimize-registers
Incremental Synthesis (Re-Optimization)	No	Compile_ultra -incremental
Area Recovery	No	Optimize_netlist -area
Topographical	No	Yes

In the first configuration, an aggressive constraint of time was carried out regardless of the area and power criterion. The second approach takes the opposite route by optimizing power and area criterion. Finally, the third case takes a balanced approach between time and power/area. Table II shows the three configurations applied in the study. Lastly, the 32nm optimized version will be compared to the MD5 500nm implementation to contrast their results.

IV. RESULTS

A. *Basic Circuits Technology Comparison*

1) Inverter

The first stage of this work began by testing the simplest digital circuit: the inverter. As mentioned, the tests used two synthesis techniques for each technology. Through the inverter, the basic impact of the technology scaling and the influence of the topographic synthesis against the standard can be determined.

Table III shows the results of the reports generated by the TCAD tools. As a result, differences between synthesis techniques are not very striking alike for the technology nodes. The topographic synthesis presents a 10-15% general improvement in the results with the 500nm technology. With 32nm technology there is no significant difference between synthesis procedures, and it can be attributed to the fact that the inverter is a very simple circuit and lake of optimization possibilities.

TABLE II. SYNTHESIS TECHNIQUES SETUP FOR MD5 OPTIMIZATION.

Synthesis Parameter	Balanced Optimization	Power & Area Optimization	Time Optimization
Synthesis Technique (Optimization)	Compile_ultra	Compile_ultra -gate_clock -no_autoungroup	Compile_ultra -retime
Retiming Technique	Optimize-registers	Optimize-registers	Optimize-registers
Incremental Synthesis (Re-Optimization)	Compile_ultra -incremental	Compile_ultra -incremental	Compile_ultra -incremental
Area Recovery	Optimize_netlist -area	Optimize_netlist -area	-
Topographical	Yes	Yes	Yes

TABLE III. INVERTER REPORTS

Inverter Synthesis Reports				
Technology	**500 nm**		**32 nm**	
Synthesis Technique	**Basic**	**Full**	**Basic**	**Full**
Data Arrival Time [ns]	3.74	3.21	0.05	0.05
Total Power [uW]	724.1	653.6	7.44	7.44
Total Area [um2]	416	416	1.27	1.27

This first stage highlights the advantage of 32nm technology over the 500nm. Indeed, the inverter shows a data arrival time of at most 75 times less than its counterpart. In power consumption there is a considerable reduction of almost 100 times less with the new technology. Finally, the size of the device is the result that presents the greatest difference with an area reduction greater than 325 times with 32nm technology.

2) Register Bank

To increase the complexity, we decided to test an 8-bit register bank. In the tests, the period of the clock signal was varied from 1 to 50 nanoseconds to assess the robustness of the technologies with a fast sequential circuit. Fig. 2 shows the slack as a function of the clock period. For both technologies, it is observed that the topographic synthesis is slightly better. In the case of 32nm, the digital circuit can work using a 1ns clock with a critical slack close to zero (~0.02 ns). However, in the case of 500nm, a minimum clock of 10ns can be used where the slack becomes almost zero (~0.03 ns). This indicates that there is a clear speed limitation with larger technology. In all cases shown in Fig. 2, the slack increases linearly as the clock period increases.

The total power consumption of the device for each technology case (Fig. 3) shows a clear advantage in 32nm technology with a 20-30 times power consumption reduction on slow clocks. At high frequency, the difference becomes exponential. Fig. 4 shows the area occupied by the circuit. As mentioned in the previous case, it is the parameter that shows the greatest advantages for 32nm technology. In this case, a reduction of 150-180 times the area that the same circuit occupies in 500nm is determined. As expected, the area remains constant and is independent of the clock period.

B. *MD5 Synthesis Optimization*

In this second stage, the circuit was subjected to three topographic synthesis configurations with different techniques explained in Table II. In all three approaches, the circuit was able to run with a faster clock than the original. The results are very similar, but the power and area optimization technique has slightly lower results than the other approaches. The results in general are quite good and indicate that despite being a much more complex circuit than the previous ones, the technology allows the implementation with relatively fast clocks. The results of the different approaches taken for topographical synthesis is shown in Table IV.

In all three cases, power consumption tends to grow exponentially for fast clocks as seen in Table IV. This is closely linked to the dynamic power that increases as a function of frequency [12]. Data shows a 5-10% improvement in technique focused on power and area. The other two techniques do not have significant differences from each other. The last parameter that was studied in this stage was the area occupied by the circuit. Table IV shows that for the power and area optimization technique the area is almost 10% greater than the other cases. Regarding the other two techniques, no significant differences are observed until the circuit must work in the region of very fast clocks.

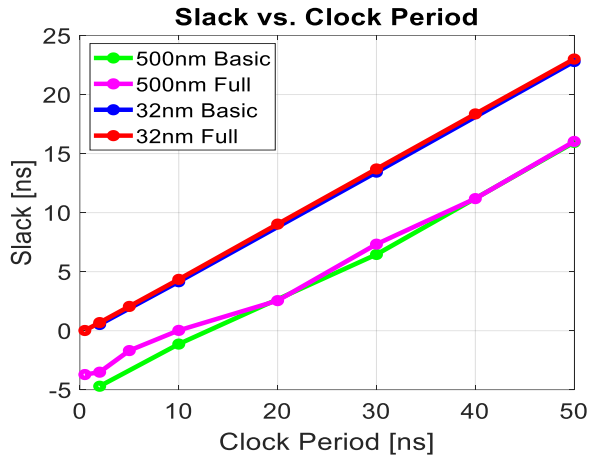

Fig. 2. Slack as a function of Clock Period on an 8-bit register bank.

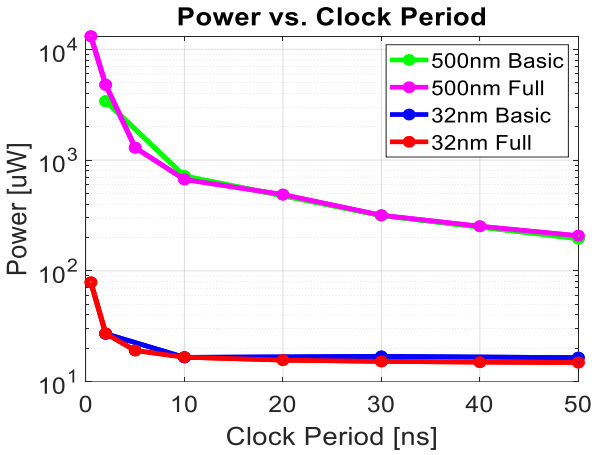

Fig. 3. Power as a function of Clock Period on an 8-bit register bank.

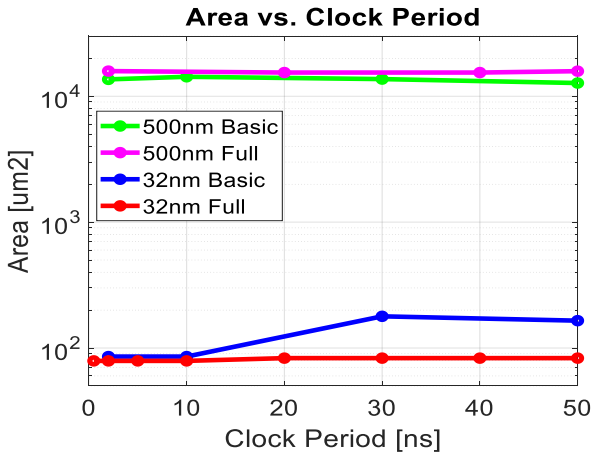

Fig. 4. Area as a function of Clock Period on an 8-bit register bank.

C. *Technology Scaling Impact on MD5*

In this last part, the comparison between the two technologies was studied for the MD5 ASIP. For the 32nm technology, the balanced approached was considered for its well-rounded performance. When analyzing the time results shown in Fig. 5, it is observed that the slack of the device in 32nm is 30-35 times greater than its counterpart in stable regions. Critical slack occurs at 12 and 1 nanoseconds for 500 and 32-nanometer technologies, respectively. This indicates that the device can work with a faster clock by scaling its technology.

Fig. 6 shows the results of the device's power consumption. As expected, the technology scaling generates 20-30 times less consumption. The most important thing about the graph is that the power consumption curve is stable for both technologies. In both cases, the power consumption increases linearly until it reaches the critical slack region is reached where the consumption increases exponentially.

The last analysis corresponds to the area of the device, shown in Fig. 7 In this case, the area reduction is greater than 900 times when scaling the technology. This behavior indicates that for more complex circuits, the technology scaling generates better benefits in the area than if it is applied in simple structures.

TABLE IV. 32NM MD5 REPORTS

Slack [ns]				
Clock Period [ns]	**Clock Frequency**	**Balanced**	**Power & Area**	**Time**
25	**40 MHz**	11.46	11.31	11.46
5	**200 MHz**	2.17	2.09	2.17
1	**1 GHz**	0.00	-0.00	0.00
Total Power [uW]				
25	**40 MHz**	211.68	213.67	211.68
5	**200 MHz**	269.32	263.48	269.32
1	**1 GHz**	683.27	734.71	759.57
Total Cell Area [um2]				
25	**40 MHz**	1744	1941	1744
5	**200 MHz**	1646	1738	1646
1	**1 GHz**	1792	1989	1875

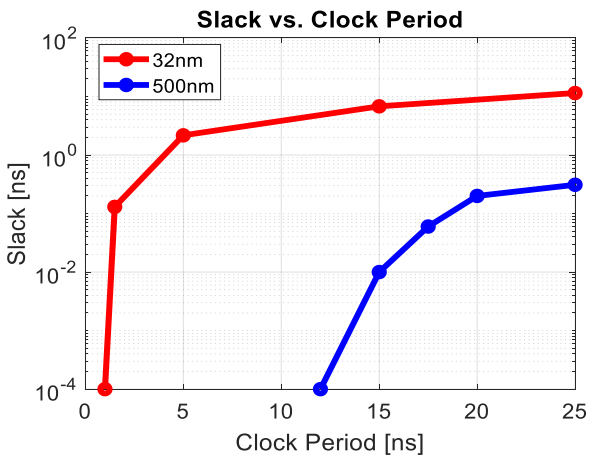

Fig. 5. Slack as a function of Clock Period on MD5 (both technologies).

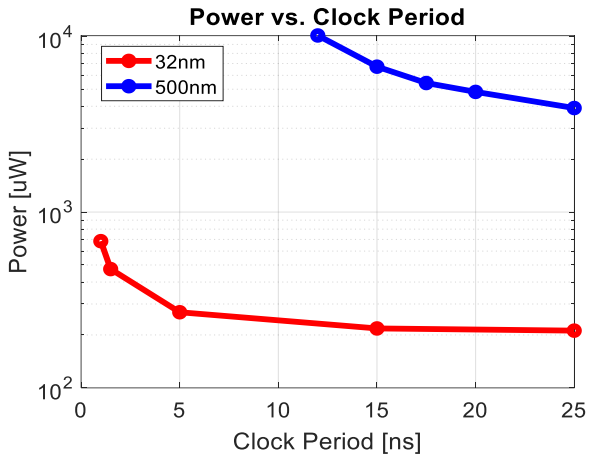

Fig. 6. Power as a function of Clock Period on MD5 (both technologies).

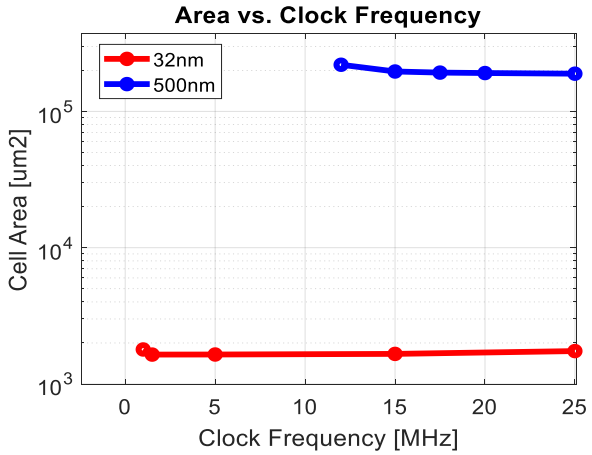

Fig. 7. Area as a function of Clock Period on MD5 (both technologies).

V. Conclusions

Although the use of new technologies might sound like an appealing idea at the design moment of a digital circuit, one should consider if the application for which the microprocessor is being used will take advantage of the benefits of smaller technologies. Perhaps the application does not require the use of smaller technologies, in which case it might be more useful to stay with older technologies as they probably are less expensive than the newer ones. The use of a new technology implies the need to do many tests before guaranteeing that it can be applied in the market. If a digital circuit works correctly and the different performance tests in time, power and area are adequate for a specific technology, this does not mean that the same happens for other technologies. Furthermore, if there is an escalation in technology, this implies that there will be new physical phenomena that must be considered. It is for this reason that this research was carried out with the aim of demonstrating the reliability and effects of technology scaling in different digital circuits.

Topographic synthesis was shown to be a great tool in the simulation of digital circuits since it is a process in which the physical limitations of the technologies are considered. Through this research, the configuration and application of the 32nm library offered by Synopsys for different simple and complex digital circuits were developed, obtaining strong results in all cases that allow us to do a comparison between the two technologies. Regardless of comparing individual cells of a full microprocessor, the data obtained for the technology scaling were similar. For all cases, we can expect around a 10x increase in the clock frequency, a 100x decrease in power consumption, and around a 300x size decrease. Giving us good starting values to consider technology down-scaling profitable.

References

[1] Sung Dae Kim, Jeong Hoo Lee, Chung Jin Hyun and Myung Hoon Sunwoo, "ASIP approach for implementation of H.264/AVC," *Asia and South Pacific Conference on Design Automation, 2006.*, Yokohama, 2006, pp. 7 pp.-, doi: 10.1109/ASPDAC.2006.1594777.

[2] Manoj Kumar Jain, M. Balakrishnan and Anshul Kumar, "Integrated on-chip storage evaluation in ASIP synthesis," *18th International Conference on VLSI Design held jointly with 4th International Conference on Embedded Systems Design*, Kolkata, India, 2005, pp. 274-279, doi: 10.1109/ICVD.2005.112.32nm cmos technology.

[3] J. Jiménez, L. Trojman and L. Procel, "Power and Area Reduction of MD5 based on Crypto-processor Using novel approach of Internal Counters on the Finite State Machine," *2019 IEEE Fourth Ecuador Technical Chapters Meeting (ETCM)*, Guayaquil, Ecuador, 2019, pp. 1-4, doi: 10.1109/ETCM48019.2019.9014878.

[4] H. Elmiligi, A. A. Morgan, M. W. El-Kharashi and F. Gebali, "A Topology-based Design Methodology for Networks-on-Chip Applications," *2007 2nd International Design and Test Workshop*, Cairo, 2007, pp. 61-65, doi: 10.1109/IDT.2007.4437429.

[5] Shenghua Liu *et al.*, "Topological routing to maximize routability for package substrate," *2008 45th ACM/IEEE Design Automation Conference*, Anaheim, CA, 2008, pp. 566-569.

[6] Y. Kuo, L. J. Arana, L. Seva, C. Marchese and L. Tozzi, "Educational design kit for synopsys tools with a set of characterized standard cell library," *2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS)*, Puerto Vallarta, 2018, pp. 1-4, doi: 10.1109/LASCAS.2018.8399907.

[7] Zaifu Zhang, R. Wieler, G. Jonatschick and H. Poskar, "Synthesizing testability features into a design with the Synopsys Test Compiler," *IEEE WESCANEX 95. Communications, Power, and Computing. Conference Proceedings*, Winnipeg, Manitoba, Canada, 1995, pp. 462-467 vol.2, doi: 10.1109/WESCAN.1995.494074.

[8] R. Dean Adams, R. Abbott, Xiaoling Bai, D. Burek and E. MacDonald, "An integrated memory self test and EDA solution," *Records of the 2004 International Workshop on Memory Technology, Design and Testing, 2004.*, San Jose, CA, USA, 2004, pp. 92-95, doi: 10.1109/MTDT.2004.1327990.

[9] J. W. Sleight *et al.*, "Challenges and Opportunities for High Performance 32 nm CMOS Technology," *2006 International Electron Devices Meeting*, San Francisco, CA, 2006, pp. 1-4, doi: 10.1109/IEDM.2006.346881.

[10] G. G. Shahidi, "Evolution of CMOS Technology at 32 nm and Beyond," 2007 IEEE Custom Integrated Circuits Conference, San Jose, CA, 2007, pp. 413-416, doi: 10.1109/CICC.2007.4405764.

[11] G. Stenz, B. M. Riess, B. Rohfleisch and F. M. Johannes, "Performance optimization by interacting netlist transformations and placement," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 19, no. 3, pp. 350-358, March 2000, doi: 10.1109/43.833203.

[12] Weitorg Chuang, "Delay And Area Optimization For Compact Placement By Gate Resizing And Relocation," *IEEE/ACM International Conference on Computer-Aided Design*, San Jose, CA, USA, 1994, pp. 145-148, doi: 10.1109/ICCAD.1994.629757