AFRL-RY-WP-TR-2020-0277

POST-MANUFACTURING PROGRAMMABLE CAMOUFLAGED LOGIC

Ken Mai

Carnegie Mellon University

OCTOBER 2020
Final Report

AIR FORCE RESEARCH LABORATORY
SENSORS DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7320
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals.

Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RY-WP-TR-2020-0277 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

BOZADA.CHRISTOPHER.A.1131856993 Digitally signed by BOZADA.CHRISTOPHER.A.1131856993 Date: 2020.10.14 12:09:29 -04'00'

CHRISTOPHER A. BOZADA
Program Manager
Aerospace Components and Subsystems Division

BROOKS.ADAM.L.1270115205 Digitally signed by BROOKS.ADAM.L.1270115205 Date: 2020.10.19 09:50:40 -04'00'

ADAM L. BROOKS, Lt Col, USAF
Deputy
Aerospace Components and Subsystems Division
Sensors Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

*Disseminated copies will show "//Signature//" stamped or typed above the signature.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
October 2020	Final	19 December 2017 – 13 December 2019

4. TITLE AND SUBTITLE
Post-Manufacturing Programmable Camouflaged Logic

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8650-18-1-7814

5c. PROGRAM ELEMENT NUMBER
63760E

6. AUTHOR(S)
Ken Mai

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
Y1Q6

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213-3815

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Sensors Directorate
Wright-Patterson Air Force Base, OH 45433-7320
Air Force Materiel Command
United States Air Force

Defense Advanced
Research Projects Agency
DARPA/MTO
675 North Randolph Street
Arlington, VA 22203

10. SPONSORING/MONITORING AGENCY ACRONYM(S)
AFRL/RYD

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)
AFRL-RY-WP-TR-2020-0277

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This material is based on research sponsored by Air Force Research laboratory (AFRL) and the Defense Advanced Research Agency (DARPA) under agreement number FA8650-18-1-7814. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation herein. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies of endorsements, either expressed or implied, of AFRL and the DARPA or the U.S. Government. Report contains color.

14. ABSTRACT

The Carnegie Mellon University research team has developed a post-manufacturing programmable camouflaged logic topology to protect critical intellectual property (IP) embedded in integrated circuit designs during manufacturing and in-the-field. The basis of the design was a threshold voltage defined (TVD) logic gate topology that uses different threshold voltage transistors, but with identical layouts, to determine the logic gate function.

15. SUBJECT TERMS
camouflaged logic topology, intellectual property, threshold voltage defined logic gate topology

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON (Monitor)
a. REPORT	b. ABSTRACT	c. THIS PAGE			Christopher Bozada
Unclassified	Unclassified	Unclassified	SAR	265	19b. TELEPHONE NUMBER *(Include Area Code)* N/A

Table of Contents

Section **Page**

List of Figures

Figure **Page**

List of Tables

Table **Page**

1 SUMMARY

The Carnegie Mellon University (CMU) research team has developed a post-manufacturing programmable camouflaged logic topology to protect critical intellectual property (IP) embedded in integrated circuit designs during manufacturing and in-the-field. The basis of the design was a threshold voltage defined (TVD) logic gate topology that uses different threshold voltage transistors, but with identical layouts, to determine the logic gate function. The post-manufacturing programmability was achieved by using hot-carrier injection (HCI) intentionally to change the threshold voltages of transistors and in turn alter the functionality of the gates. The technique is fully compatible with standard complementary metal oxide semiconductor (CMOS) logic processes, requiring no special layers, structures, or process steps. The CMU team evaluated the overhead and security of PMP-TVD camouflaging. The average overheads of the implemented benchmark circuits using PMP-TVD gates were 8.3x, 4.7x, and 5.6x for delay, power, and area, respectively. To show the feasibility of PMP-TVD logic, two testchips were taped out in 65nm and 28nm CMOS processes. With the prototype testchips, the CMU team demonstrated that the functionality of the structures built with PMP-TVD gates can be enhanced, erased, or changed in the field using HCI while successfully camouflaging the gate function.

2 INTRODUCTION

Advances in semiconductor technology have made the use of integrated circuits (ICs) nearly ubiquitous. Due to increasing costs and complexity, the semiconductor industry has moved towards the globalization of the manufacturing supply chain. Unfortunately, the globalized supply chain has created security and trust concerns due to the possibility of malicious parties engaging in intellectual property (IP) theft or counterfeiting. Moreover, even if the manufacturing supply chain can be secured, the design details of an IC can be compromised later in the field using reverse engineering techniques.

Researchers have explored various hardware obfuscation methods to prevent the attackers from extracting the details of a design. Although the proposed methods aim to thwart these security threats and secure the design information, they fall short, either only aiming at combating reverse engineering or untrusted fabrication individually, or having large performance, area, power, and manufacturing cost overheads. While methods that employ configurable logic aim to provide security against reverse engineering and untrusted fabrication, in these methods, the storage of configuration data in a secure way is not addressed and is vulnerable. Although camouflaged logic, another hardware obfuscation scheme, does not address untrusted fabrication, the configuration can be embedded in the layout and can be stored securely. Therefore, we aim to improve upon existing camouflaging methods to protect IP embedded in IC designs during manufacturing and in the field.

With the exponential scaling of semiconductor processes over the past decades providing unprecedented integrated circuit (IC) performance and power efficiency at ever shrinking costs, use of integrated circuits in military systems and critical supervisory control and data acquisition (SCADA) infrastructure has become near ubiquitous. As a consequence, these ICs have become a tempting target for adversaries seeking to compromise the security of these systems. Thus, securing the design, manufacture, and deployment of these integrated circuits has become a paramount national security concern. One of the primary goals of these attackers is to gain access to the design details of the integrated circuits, which then enable a myriad of cyber-attack vectors including: theft of critical data or intellectual property; design cloning/counterfeiting possibly with hardware Trojan insertion; and enhancing other hardware/software attacks.

With the globalization of the semiconductor supply chain and off-shoring of advanced lithographic node foundries, the US must find a way to maintain access to cost-effective state-of-the-art IC fabrication facilities while also ensuring the security of critical intellectual property. While the use of specialized technologies (e.g., 3D integrated non-volatile memory) or elaborate fabrication flows (e.g., split manufacturing) may mitigate these problems, the cost and complexity of such solutions render them infeasible for many applications. Thus, we seek to enable the US access to state-of-the-art **untrusted IC fabrication** facilities while also protecting sensitive IP, doing so using only conventional IC logic fabrication process flows. Additionally, adversaries have access to advanced **reverse engineering** technologies capable of complete IC de-processing. Thus, even after manufacturing, a deployed IC may be subject to a reverse engineering attack and have its entire design database and manufacturing technology compromised.

2.1 Technical Approach

Thus, we seek to protect critical intellectual property (IP) embedded in integrated circuit designs during manufacturing and in-the-field. Our techniques enable use of insecure off-shore fabrication facilities for cost effective advanced manufacturing without any additional costly fabrication steps via post-manufacturing programming. Further, our techniques protect deployed ICs against state-of-the-art reverse engineering attacks by concealing the IC design using threshold-defined camouflaged logic.

We propose to use a post-manufacturing programmable camouflaged logic topology to achieve these goals. The basis of the design is a threshold voltage defined (TVD) logic gate topology (Figure 1(left)) that uses different threshold voltage transistors, but with identical layouts, to determine the logic gate function [7]. Every TVD logic gate has the same physical layout and is one-time post-manufacturing programmed with different threshold voltages for different Boolean functions. The post-manufacturing Vt programming is achieved using intentional directed hot-carrier injection (HCI). We have used the same technique previously to set device Vt's to enhance PUF reliability and build a TRNG on a 65nm CMOS testchip [8][9]. Thus, the proposed design technique is fully compatible with standard CMOS logic processes, requiring no special layers, structures, or process steps. At the same time, it achieves both concealment of critical IP from the foundry and high resistance against reverse engineering and semi/non-invasive attacks.

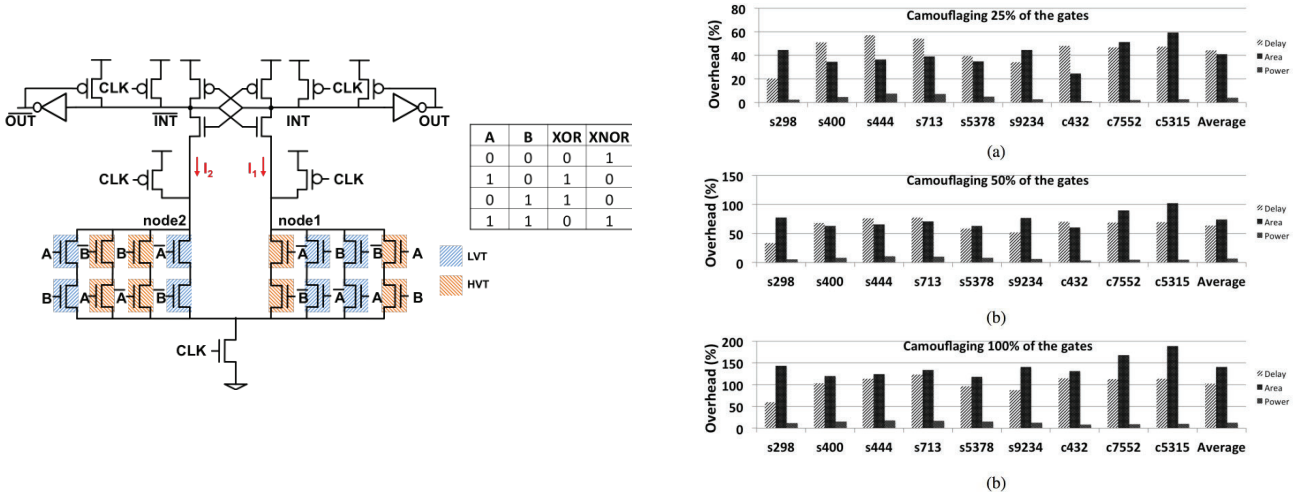


Figure 1: (Left) 2-input TVD-XOR Gate (left) and (Right) Delay, Power, and Area Overhead with Camouflaging Ratios (a) 25% (b) 50% (c) 100% for various ISCAS Benchmarks [7]

Left figure: Transistors with LVT threshold implants are shown in blue, and HVT transistors are shown in orange. Truth table of XOR gate is also shown

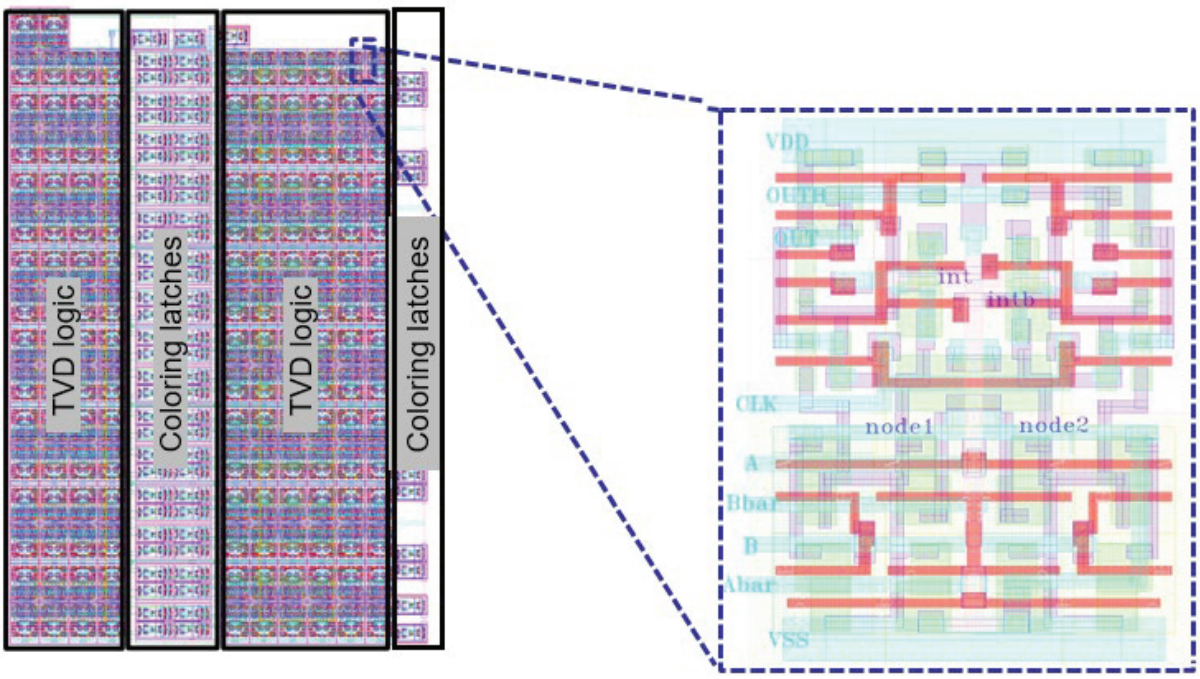


Figure 2: (Left) Sample Layout of an Adder using TVD Logic Gates (note the complete homogeneity of the camouflaged TVD logic gates) and (Right) Layout of a Camouflaged TVD Logic Gate

The proposed post-manufacturing programmed threshold voltage defined (PMP-TVD) design (Figure 3) technique will achieve the following critical design features:

- **Concealment of the logic functionality from the foundry.** The logic gate function is not discernible from any of the IC fabrication mask layers, as the gate topology is generic and devoid of any logic function information. The TVD logic programming is done post-manufacturing in a trusted environment.
- **Fully logic process compatible.** No extra layers or processing steps are needed for the proposed design. We use a wholly conventional CMOS logic process to build the TVD gates and programming infrastructure. We have already demonstrated the post-manufacturing programming technology in a prototype testchip built on a conventional 65nm bulk CMOS logic process with a physical unclonable function design and a true random number generator.
- **High resistance to reverse engineering.** The logic functionality of the post-manufacturing programmable TVD gate is embedded in the threshold voltages of the devices, not the mask patterns. As such, an attacker would need to read out the threshold voltage of an exceedingly high number of transistors on the die to discern the logic function. As this capability has only been demonstrated on single devices with considerable difficulty, we contend that the reading out of thousands or millions of device Vt's on a single die is prohibitively challenging to even an attacker with state-of-the-art reverse engineering capabilities. The low overheads of TVD gates (see below) allows complete replacement of all logic gates with TVD gates, so the resistance to reverse engineering is higher than conventional camouflaged gate proposals that only replace a small number of the gates with camouflaged gates.

- **Self-destruct on tamper.** The logic gates are one-time programmable, one-time erasable. On tamper detection (or any other desired trigger) the programming state of the logic gates can be erased in seconds and cannot be recovered even through invasive reverse engineering.

- **Side-channel attack resistance.** The TVD logic gates are a dynamic differential logic style and thus by nature have strong power analysis resistance. Additional care in the interconnect layout or addition of a discharge phase can enhance this resistance. Further, as the gates are topologically identical and symmetric, the timing behavior of the gates make them resistant to timing attacks.
- **Fast programming time.** By parallelizing the logic gate programming, the hot-carrier injection programming can be done in tens to low hundreds of seconds requiring only a moderately boosted voltage (e.g., 2.5V), which would be available as the I/O voltage or can be generated on-die using a charge pump.
- **High programming reliability and permanence.** Our two previous designs using the HCI programming technique have achieved lab-measured bit error rates near 10^{-9} while withstanding accelerated aging at high temperature and voltage without significant reversal. As modern FLASH memory uses similar technologies (i.e., carrier trapping in nitride trap layers instead of traditional floating gates) for data storage, we contend that the HCI programming technique achieves both high reliability and permanence.
- **Low VLSI overheads.** The exploration of camouflaged TVD logic found modest overheads versus conventional static CMOS in area, power, and delay assuming even complete replacement of all logic gates Figure 1(right). This is in contrast to most camouflaged logic proposals that limit the number of replaced gates and take great pains to choose the optimal gates to replace, as their overheads are so high. Our TVD design has considerably lower overheads and enables *complete* replacement of all logic gates with programmable camouflaged TVD gates.

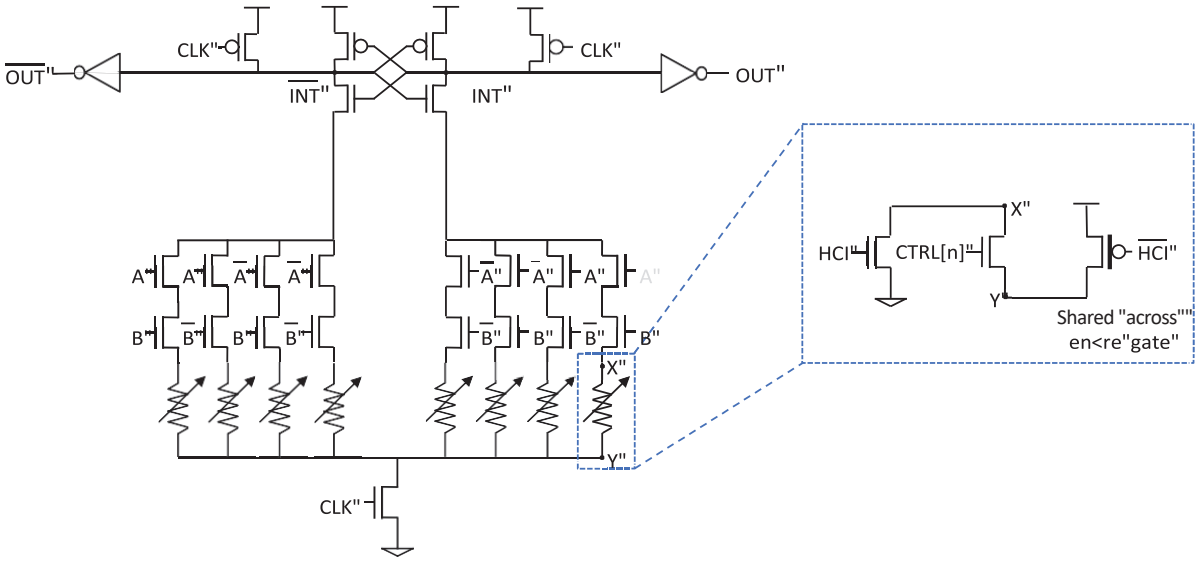


Figure 3: Schematic of proposed Post-manufacturing Programmable Threshold Voltage Defined (PMP-TVD) Logic Gate

Note that the thick oxide HCI PMOS device is shared across the entire logic gate (i.e., only one is needed per logic gate).

As we have previously demonstrated the two technologies (camouflaged TVD logic gates, and HCI Vt programming) separately, we propose to explore how to optimally merge them. The HCI Vt programming was used for a sense amplifier structure in the PUF and TRNG designs, and that StrongARM sense amplifier is identical to the TVD logic gate topology except for the multiple pull-down legs. Thus, we believe that the two technologies are highly compatible. The additional overhead of the additional HCI programming infrastructure and optimization of such is being explored. Another key issue under study is whether an attacker can discern significant design information from the interconnect pattern, without knowledge of the underlying gate logic functions. This is the reverse of the typical split fabrication attack scenario where an attacker has knowledge of the gate logic functions, but not the interconnect patterns. Obfuscation techniques can be applied to decrease the information leakage from the interconnect patterns, and if needed, additional reconfigurability can be added to the interconnect. The interconnect programming can be achieved using the same HCI Vt programming technique used in the TVD logic gates, but the overheads are yet to be determined.

3 TASK RESULTS

3.1 Task 1 – PMP-TVD Circuit Design

PMP-TVD logic gates were designed using commercial CAD tools at the schematic and layout levels (Cadence Composer and Virtuoso). Designs were simulated using a transistor-level simulation tool (Cadence Spectre) and compared against conventional logic gates in area, power, and delay. The CMU team used 65nm and 28nm TSMC process technologies for the simulations and designs. Exemplar designs were developed that were suitable for integration with standard cell synthesis CAD tools (see Task 2) of 2-input and 3-input PMP-TVD logic gates.

The CMU team has shown the circuit details and analysis of the proposed secure camouflaged logic family, post-manufacturing programmed threshold voltage defined logic (PMP-TVD). Further, the CMU team has shown how a PMP-TVD gate operates and explained the design knobs of the structure. Then, the CMU team has evaluated the security of the PMP-TVD gates and shown an overhead analysis compared to standard cell synthesized structures.

With the addition of post-manufacturing programmability on top a TVD gate, PMP-TVD achieved security against untrusted fabrication on top of protection against reverse engineering which is inherited by the TVD topology. In addition, PMP-TVD logic allowed enhancing, erasing, or changing the functionality of the preprogrammed design by applying HCI stress postproduction. Furthermore, reprogrammability gave the designer an advantage of being able to upgrade their design in the field.

Additional details can be found in Appendix A.

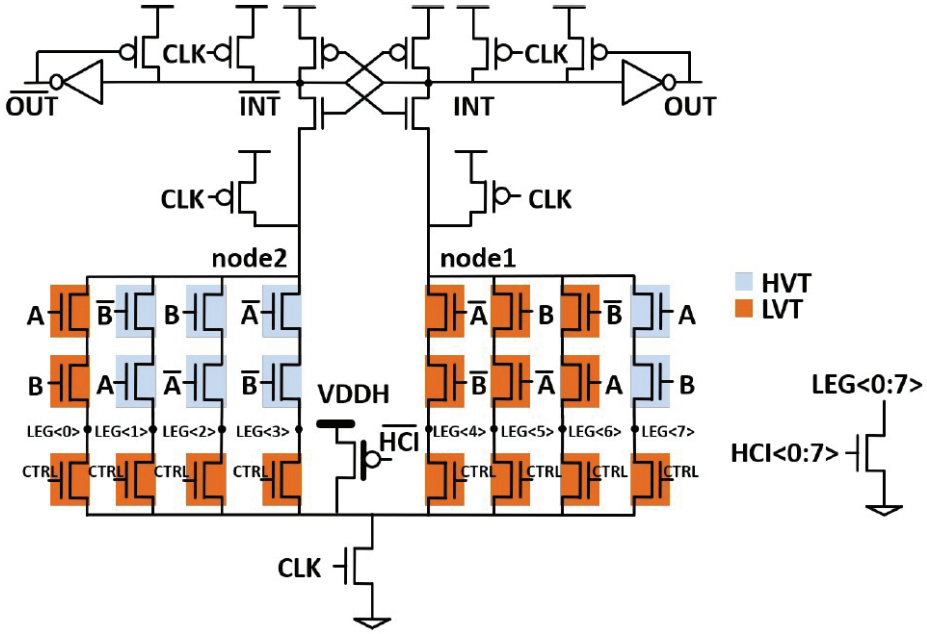


Figure 4: Schematic of a 2-input PMP-TVD Logic Gate Pre-programmed as a NAND Gate

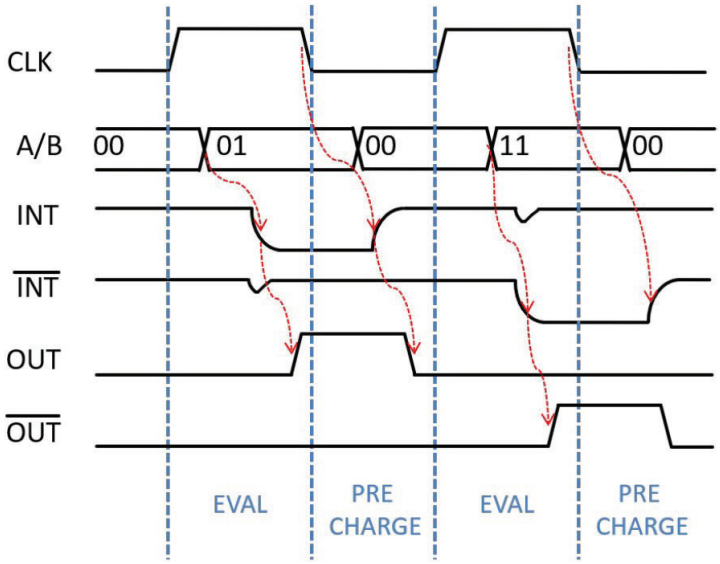


Figure 5: Timing Diagram of a Pre-programmed 2-input PMP-TVD XOR Gate for the Input Transitions of 00 to 01

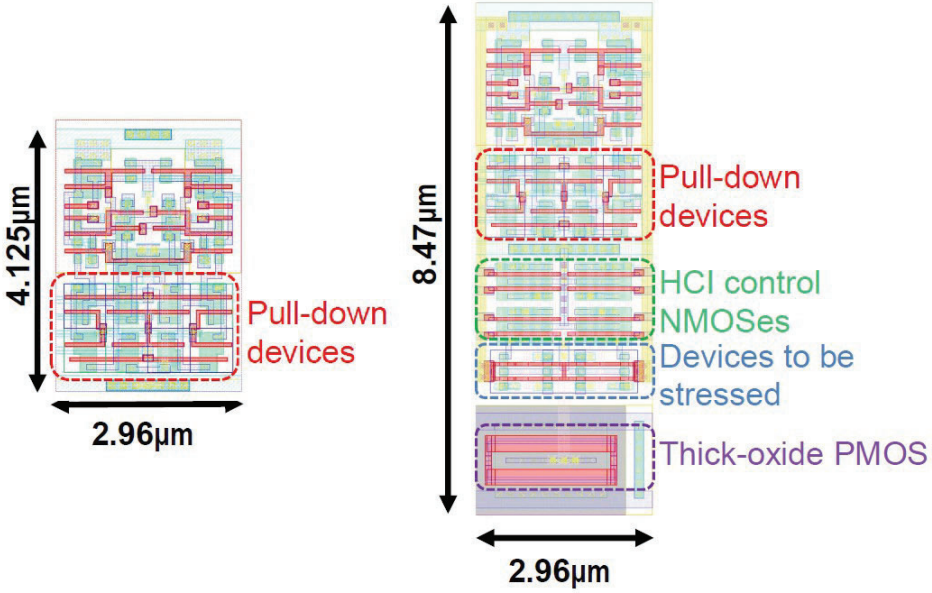


Figure 6: 2-input TVD and PMP-TVD Gate Layout in 65nm Process

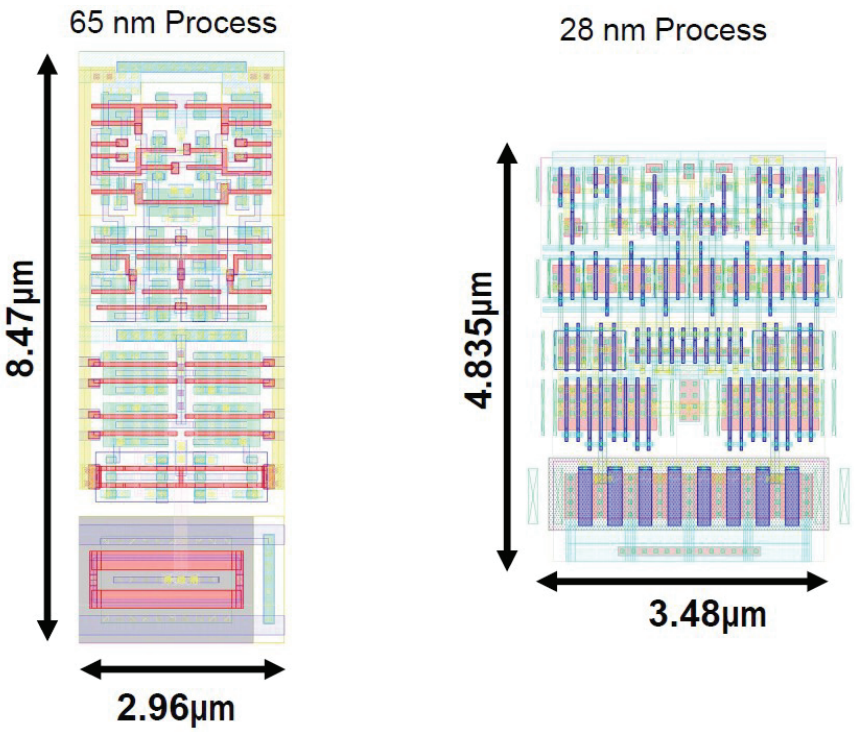


Figure 7: 2-input PMP-TVD Gate Layout Comparison between 65nm and 28nm Process

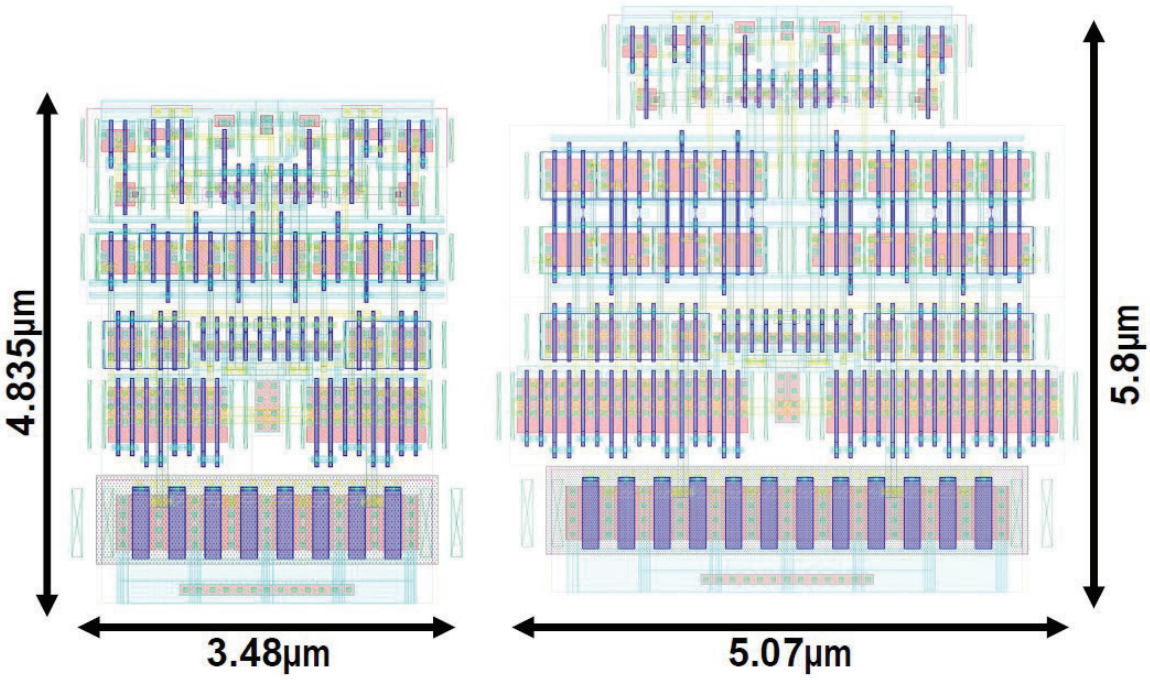


Figure 8: 2-input and 3-input PMP-TVD Gate Layout in 28nm Process

3.2 Task 2 – Standard Cell Synthesis CAD Tool Integration

The CMU team integrated the PMP-TVD logic gates designed in Task 1 with Synopsys Design Compiler. The tool flow was used on ISCAS-85 benchmark circuits, and AES-128 encryption accelerator, and adder RTL designs. The characterization files for the 2-input and 3-input PMP-TVD gates needed to use them as standard cells for Verilog HDL synthesis were generated. The modification of a synthesis CAD tool to use PMP-TVD standard cell gates were completed allowing for the successful synthesis and place-and-route of ISCAS-85 benchmark designs using PMP-TVD gates as standard cells with Synopsys Design Compiler.

Additional results for ISCAS-85 circuits and AES-128 can be found in Appendix A.

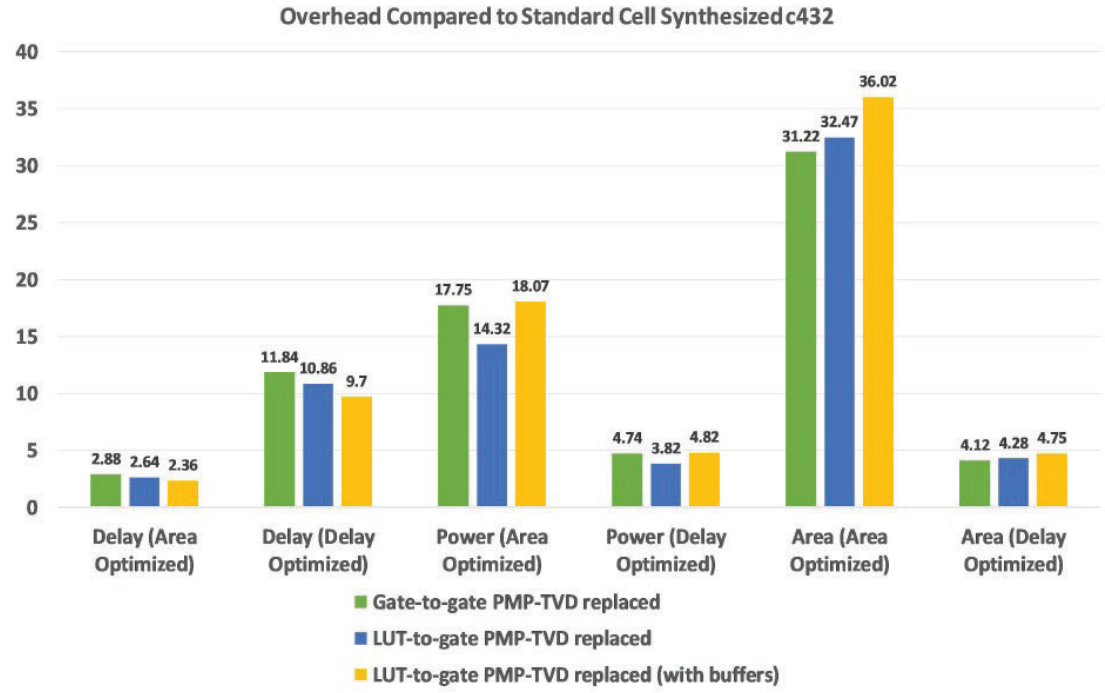


Figure 9: Overhead Results of Gate-to-Gate PMP-TVD replaced (green), LUT-to-Gate PMP-TVD replaced (blue), and LUT-to-Gate PMP-TVD replaced with buffers (yellow) compared to Area Optimized Standard Cell Synthesized and Delay Optimized Standard Cell Synthesized are shown for the Benchmark c432

Table 1. Overhead of Place and Route Step for Standard Cell Synthesized Structures

Designs	Number of Gates	Delay	Power	Area
c432				
Area Optimized	1.01x	1.29x	1.51x	1.09x
Delay Optimized	1.08x	1.66x	1.39x	1.04x
c1908				
Area Optimized	2.48x	1.39x	1.35x	1.66x
Delay Optimized	1.12x	1.74x	1.23x	1.1x
c3540				
Area Optimized	1.00x	1.28x	1.46x	1.02x
Delay Optimized	1.06x	1.78x	1.82x	1.06x
c7552				
Area Optimized	1.00x	1.38x	1.24x	1.02x
Delay Optimized	1.20x	1.91x	1.49x	1.08x

3.3 Task 3 – Testchip Design and Fabrication

The CMU team designed and implemented testchips using the PMP-TVD circuits on 65nm and 28nm TSMC process technologies. The CMU team utilized the Synopsys Design Compiler based CAD tool flow developed in Task 2 to synthesize the designs.

The two prototype testchips consisted of structures built by using TVD and PMP-TVD gates, and HCI characterization array. We used several different 4-bit and 16-bit structures to benchmark the characteristics of the TVD and PMP-TVD logic families. We evaluated power consumption, performance, and area of the structures. We ran multiple tests with multiple different variables to present certain data points in the characterization of HCI. In addition, we explored programming and erasing functionality in PMP-TVD gates using HCI.

We demonstrated that structures can be built using TVD and PMP-TVD logic families with resistance against reverse engineering and untrusted fabrication. Although TVD structures have fixed functionalities, the PMP-TVD structures can be programmed, erased and/or reprogrammed with different functionalities in the field. In addition, using the HCI characterization gathered by the silicon results, we can trade-off between the programming time and the area, performance, and power consumption of the gates.

Additional details can be found in Appendix A.

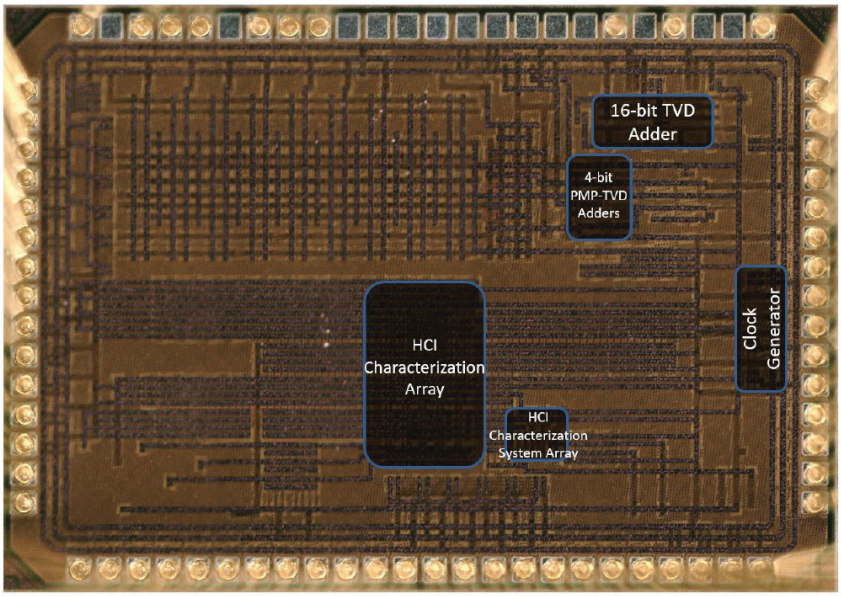


Figure 10: Die Shot of the 65nm Prototype Testchip
16-bit TVD adder, 4-bit PMP-TVD adder and 4-bit PMP- TVD blank structures, HCI characterization array, and HCI characterization system array are highlighted

Table 2. Technology and Features of 65nm Testchip

Technology	65nm CMOS with 9-metal layers	
FO4 in TTLH	35ps	
Supply Voltage	1.0V	
Chip Area	$2.04mm^2$ (1.2mm x 1.7mm)	
Number of I/O Pads	78	
Area of the Structures	**Core**	**Including Test Structures**
16-bit TVD Adder	$2875.12\mu m^2$	$28840\mu m^2$
4-bit PMP-TVD Adder	$941.85\mu m^2$	$8640\mu m^2$
HCI Characterization Array	$40000\mu m^2$	$64000\mu m^2$
HCI Characterization System	$2914\mu m^2$	$5694\mu m^2$

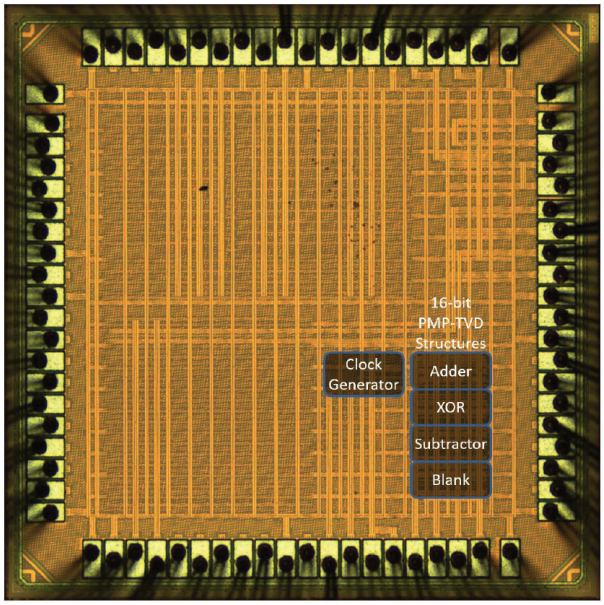


Figure 11: Die Shot of the 28nm Prototype Testchip
16-bit TVD adder, subtractor, XOR, and blank structures are highlighted.

Table 3. Technology and Features of 28nm Testchip

Technology	28nm CMOS with 9-metal layers
FO4 in TTLH	22.3ps
Supply Voltage	0.9V
Chip Area	1.327mm^2 (1.152mm x 1.152mm)
Number of I/O Pads	80
Core Area of the 16-bit PMP-TVD Structure	2183.26μm^2 (30.92μm x 70.61μm)
Area of the 16-bit PMP-TVD Structure Including Test Structures	6897.15μm^2 (58.5μm x 117.9μm)

3.4 Task 4 – Testchip VLSI and Security Evaluation

The CMU team evaluated the 65nm and 28nm testchips (Task 3) on VLSI and security metrics. The testchips were evaluated on both VLSI overheads compared to conventional standard cell designs and security metrics. The security metrics were multi-faceted required multiple different tests. The testchips demonstrated full logical functionality of all blocks at or near the simulation predicted performance and power.

The testchips are packaged in a ceramic PGA package and tested on a custom PCB shown in Figure B.1. The level shifters reduce the 5V signals supplied by the Ni-DAQ to the voltage level that the testchip pads require. The different voltage domains are supplied by the BNC connectors from the Agilent power supplies. The operating clock frequency of the testchip is divided by 4096 times and supplied out using the SMA connector and fed to an Agilent 548559A digital sampling oscilloscope. For the communication between the PC and the PCB, a Ni-DAQ 6259 board is used. The Ni-DAQ board is connected to PCB using the highlighted I/O port in the

figure. The test software is written in C, and the test input vector generation, test output data processing, and test automation are done in Python. The temperature stress tests are done in a TestEquity 107 Benchtop Temperature Chamber.

Additional details can be found in Appendix A.

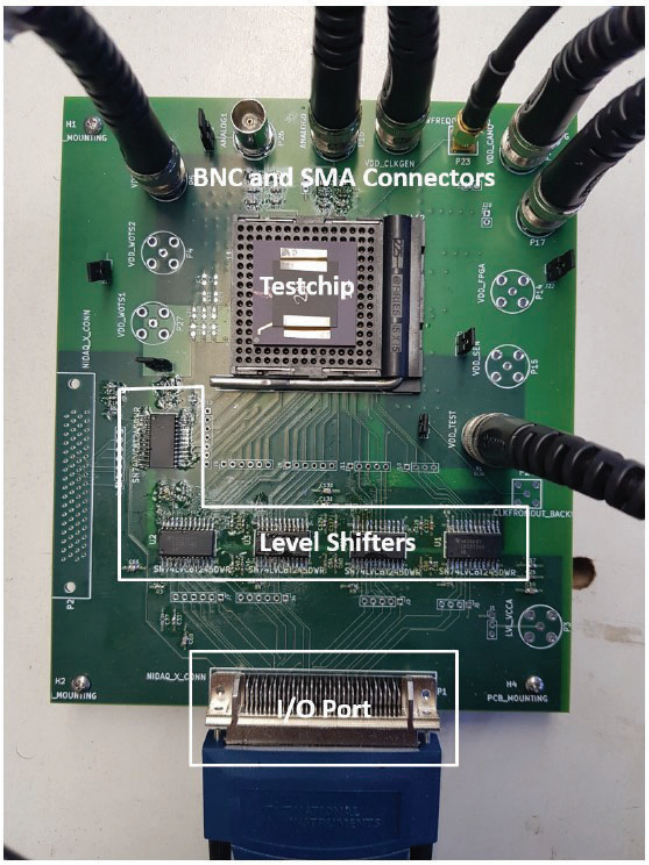


Figure 12: Test PCB for 28nm Testchip

Table 4. 65nm Testchip Results for TVD and PMP-TVD Structures

	4-bit PMP-TVD				16-bit TVD
	Preprogrammed	**Reverse Stressed**	**Boost Stressed**	**Blank**	**Adder**
Area	$0.007mm^2$ (Core: $0.001mm^2$)				$0.029mm^2$ (Core: $0.003mm^2$)
Frequency at 1V	3.2GHz	2.9GHz	3.7GHz	3.6GHz	1.0GHz
Power at 1V	1.14mW	0.96mW	1.09mW	1.09mW	3.22mW
Leakage at 1V	0.15mW	0.14mW	0.14mW	0.14mW	0.26mW

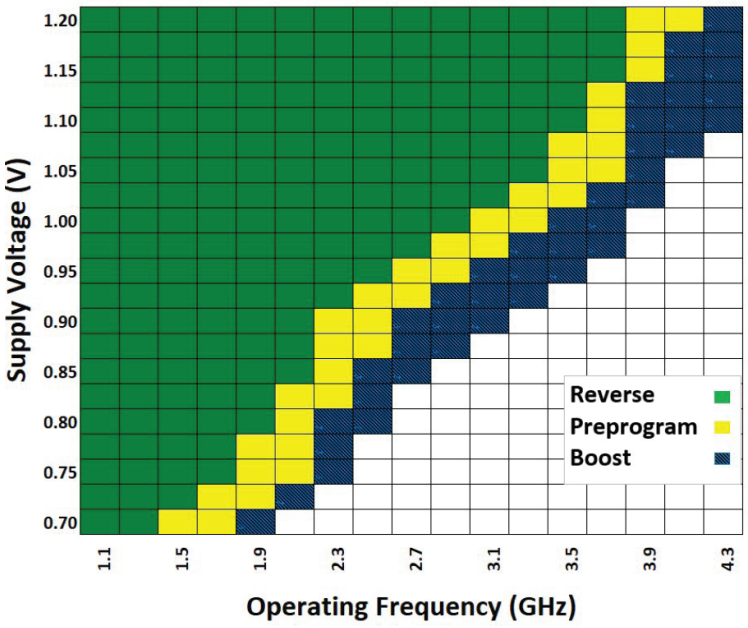


Figure 13: Shmoo Plot at Room Temperature for the 4-bit PMP-TVD preprogrammed Adder

Preprogrammed baseline (yellow), 60 seconds of reverse stress (green), and 60 seconds of boost stress (blue)

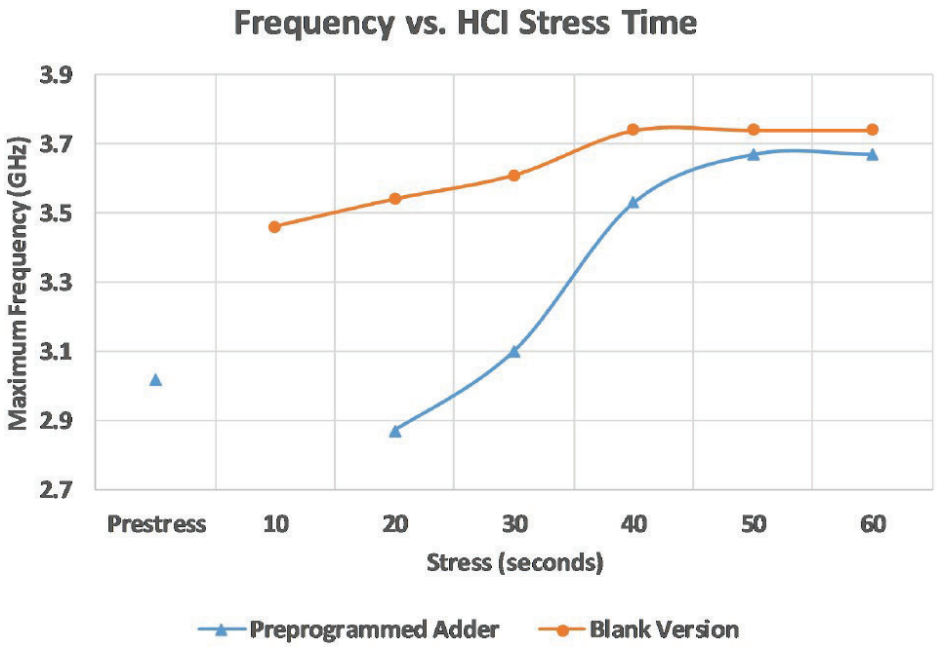


Figure 14: Frequency vs. HCI Stress Time Plot of 4-bit blank PMP-TVD Adder at 1V and Room Temperature (orange)

Also, blue line shows stress time needed to reverse preprogrammed PMP-TVD adder (20 seconds) and subsequent boosting of the reverse function

Table 5. 28nm Testchip Results for PMP-TVD Structures

	16-bit PMP-TVD Preprogrammed			16-bit PMP-TVD Blank
	Adder	Subtractor	XOR	Programmed into Adder
Area	6897.15 μm^2 (Core: 2183.26 μm^2)			
Frequency at 0.9V	790MHz	819MHz	869MHz	731MHz
Power at 0.9V	1.9mW	1.87mW	1.77mW	1.9mW
Leakage at 0.9V	0.067mW	0.0677mW	0.0669mW	0.0762mW

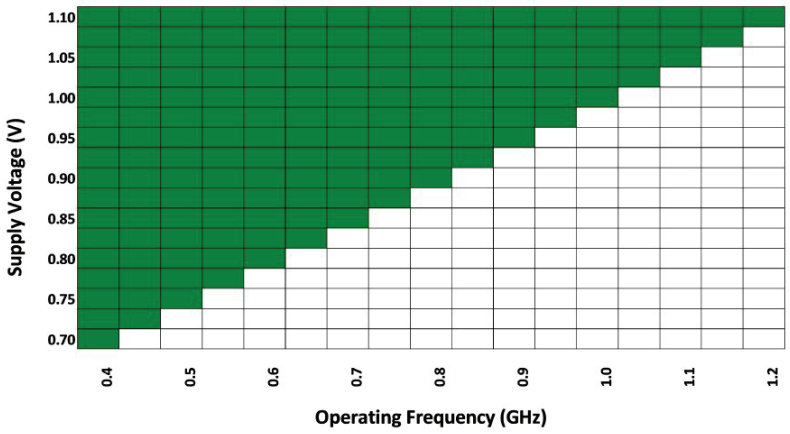


Figure 15: Shmoo Plot at Room Temperature for the 16-bit PMP-TVD preprogrammed Adder

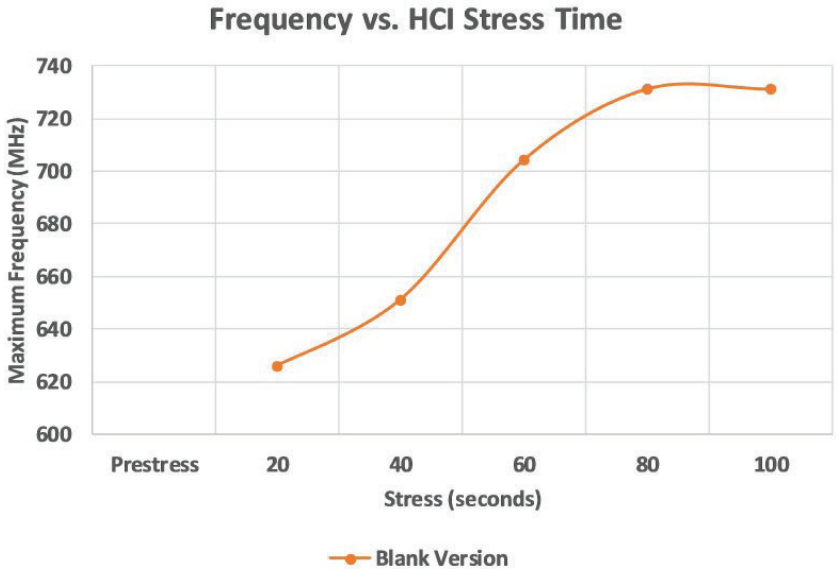


Figure 16: Frequency vs. HCI Stress Time Plot of 16-bit blank PMP-TVD Adder at 0.9V and Room Temperature

HCI stress for an adder functionality is applied at 3V at room temperature in 20 seconds intervals.

4 CONCLUSIONS

We proposed post-manufacturing programmed threshold voltage defined (PMP-TVD) logic. PMP-TVD is a secure camouflaging method that can remove the critical design information from the design database by introducing a reprogrammability feature. PMP-TVD is a logic gate topology that uses different threshold voltage transistors, but with identical layouts, to determine the logic gate function. The camouflaging technique does not rely on limited delayering and imaging resolution, does not require any additional process steps or masks, and is fully compatible with modern CMOS process technology. It has a reprogrammability feature that uses HCI phenomenon to set the functionality, change the functionality, or remove the functionality post-production. To evaluate the overhead of PMP-TVD structures, we have 100% camouflaged a subset of ISCAS85 benchmark circuits with PMP-TVD, and compared them against standard cell synthesized versions. For camouflaging, we have compared two different methods. In the first method, we replaced all the gates with their PMP-TVD equivalents, and in the second method we created a functionally identical circuit with LUTs and used PMP-TVD gates instead of LUTs. Last, we showed the differences between the methods for delay, power, and area overheads. In addition to the secure camouflaging methods, we also proposed a structure to characterize HCI, which is used in PMP-TVD structures.

Silicon results from our prototype testchips prove the feasibility and applicability of TVD and PMP-TVD camouflaging. We showed the viability of camouflaging using PMP-TVD gates in 65nm and 28nm CMOS processes. In addition, we gathered HCI characterization data in the 65nm CMOS process. Moreover, we explored HCI phenomenon to reprogram and erase PMP-TVD gate functionalities. Despite the overhead in area, power, and performance, we showed that there are significant security benefits of PMP-TVD camouflaging compared to existing countermeasures. Therefore, PMP-TVD is a very promising secure camouflaging method that can provide both concealment of critical IP from the foundry and high resistance against reverse engineering.

Although PMP-TVD gates incur delay, power, and area overheads, the structures they replace are only a small percentage of an IC. Therefore, the effective overheads incurred by these security methods are smaller overall. Using CMOS logic process compatible methods, such as PMP-TVD, which provides strong security with configurability and erase on tamper features, may prove to be a cost-effective solution for protecting secure IP against reverse engineering and untrusted fabrication.

5 REFERENCES

[1] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu and L. Pileggi, "Building trusted ICs using split fabrication," Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on, Arlington, VA, 2014, pp. 1-6.

[2] K. Bennett. Newegg selling fake Intel CPUs. [Online]. Available: http://www.hardocp.com/article/2010/03/05/newegg selling fake intel cpus

[3] U. S. A. S. Committee. Inquiry into counterfeit electronic parts in the Department of Defense supply chain.

[4] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging," in *CCS*, 2013.

[5] Chipworks. Intel's 22-nm Tri-gate Transistors Exposed. [Online]. Available: http://www.chipworks.com/blog/technologyblog/2012/04/23/intels-22-nm-trigate-transistors-exposed/.

[6] TAEUS. [Online]. Available: http://www.taeus.com/taeus- services/ ip- litigation-services/reverse- engineering/

[7] B. Erbagci, C. Erbagci, N.E.C. Akkaya, and K. Mai "A Secure Camouflaged Threshold Voltage Defined Logic Family," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* 2016.

[8] M. Bhargava and K. Mai, "A high reliability PUF using hot carrier injection based response reinforcement," *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2013.

[9] M. Bhargava, K. Sheikh, K. Mai, "Robust true random number generator using hot-carrier injection balanced metastable sense amplifiers," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* 2015.

[10] M. C. Hansen, H. Yalcin, and J. P. Hayes, "Unveiling the ISCAS-85 Benchmarks: A Case Study in Reverse Engineering," *Design Test of Computers*, 1999.

[11] J. Peng et al., "A Novel Embedded OTP NVM Using Standard Foundry CMOS Logic Technology," 2006 21st IEEE Non-Volatile Semiconductor Memory Workshop, Monterey, CA, 2006, pp. 24-26.

6 LIST OF APPENDICES

Appendix A: PhD Thesis on PMP-TVD Logic

Etkin Akkaya's PhD thesis thoroughly covers PMP-TVD logic design, the 65nm and 28nm testchips, and associated VLSI and security testing.

Appendix B: PhD Thesis Defense Slides on PMP-TVD Logic

Thesis defense slides from the above.

Appendix C: ISSCC 2018 Paper

Citation: N. E. C. Akkaya, B. Erbagci and K. Mai, "A secure camouflaged logic family using post-manufacturing programming with a 3.6GHz adder prototype in 65nm CMOS at 1V nominal VDD," *2018 IEEE International Solid-State Circuits Conference (ISSCC),* San Francisco, CA, 2018, pp. 128-130.

Appendix D: ISSCC 2018 Paper Slides

Presentation slides from the above.

Appendix E: ESSCIRC 2019 Paper

Citation: B. Erbagci, N. E. C. Akkaya, C. Erbagci and K. Mai, "An Inherently Secure FPGA using PUF Hardware-Entanglement and Side-Channel Resistant Logic in 65nm Bulk CMOS," *ESSCIRC 2019 - IEEE 45th European Solid-State Circuits Conference (ESSCIRC),* Cracow, Poland, 2019, pp. 65-68.

Appendix F: ESSCIRC 2019 Paper Slides

Presentation slides from the above.

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

ACRONYM	DESCRIPTION
AES	Advanced Encryption Standard
CMOS	Complementary Metal Oxide Semiconductor
ESSCIRC	European Solid-State Circuits Conference
HCI	Hot Carrier Injection
HVT	High Vt
IC	Integrated Circuit
IP	Intellectual Property
ISCAS	International Symposium on Circuits and Systems
ISSCC	International Solid-State Circuits Conference
LUT	Look-Up Table
LVT	Low Vt
NAND	Not AND (Boolean function)
NI-DAQ	National Instruments Data Acquisition
PMP-TVD	Post-Manufacturing Programmable Threshold Voltage Defined
SCADA	Supervisory control and data acquisition
SVT	Standard Vt
TRNG	True Random Number Generator
TSMC	Taiwan Semiconductor Corporation
TVD	Threshold Voltage Defined
VLSI	Very Large Scale Integration
VT/Vt	Transistor threshold voltage
XOR	Exclusive OR (Boolean function)

A Secure Camouflaged Logic Family for Untrusted Fabrication and Reverse Engineering

Submitted in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

in

Electrical and Computer Engineering

NAIL ETKIN CAN AKKAYA

B.S., ELECTRICAL AND ELECTRONICS ENGINEERING, BILKENT UNIVERSITY

M.S., ELECTRICAL AND COMPUTER ENGINEERING, CARNEGIE MELLON UNIVERSITY

CARNEGIE MELLON UNIVERSITY

PITTSBURGH, PA

DECEMBER, 2019

Abstract

Advances in semiconductor technology have made the use of integrated circuits (IC) nearly ubiquitous. Due to increasing costs and complexity, the semiconductor industry has moved towards the globalization of the manufacturing supply chain. Unfortunately, the globalized supply chain has created security and trust concerns due to the possibility of malicious parties engaging in intellectual property (IP) theft or counterfeiting. Moreover, even if the manufacturing supply chain can be secured, the design details of an IC can be compromised later in the field using reverse engineering techniques.

Researchers have explored various hardware obfuscation methods to prevent the attackers from extracting the details of a design. Although the proposed methods aim to thwart these security threats and secure the design information, they fall short, either only aiming at combating reverse engineering or untrusted fabrication individually, or having large performance, area, power, and manufacturing cost overheads. While methods that employ configurable logic aim to provide security against reverse engineering and untrusted fabrication, in these methods, the storage of configuration data in a secure way is not addressed and is vulnerable. Although camouflaged logic, another hardware obfuscation scheme, does not address untrusted fabrication, the configuration can be embedded in the layout and can be stored securely. Therefore, we aim to improve upon existing camouflaging methods to protect IP embedded in IC designs during manufacturing and in the field.

We present a secure camouflaged logic family for untrusted fabrication and reverse engineering. Our topology, post-manufacturing programmable threshold voltage defined (PMP-TVD) logic, protects deployed ICs against state-of-the-art reverse engineering attacks and untrusted fabrication by concealing the functionality using threshold voltage defined (TVD) camouflaged logic and having configurability post-

production. The TVD design is a logic gate topology that uses transistors with different threshold voltages, but with identical layouts, to determine the logic gate function and hide the functionality from reverse engineering attacks. The post-manufacturing programmability is achieved by using hot-carrier injection (HCI) intentionally to change the threshold voltages of transistors and in turn alter the functionality of the gates. The proposed technique is fully compatible with standard CMOS logic processes, requiring no special layers, structures, or process steps. In this work, we evaluate the overhead and security of PMP-TVD camouflaging. For the overhead analysis, a subset of ISCAS85 benchmark circuits are synthesized with standard cells and PMP-TVD gates in a 28nm CMOS process. The average overheads of the implemented benchmark circuits using PMP-TVD gates are 8.3x, 4.7x, and 5.6x for delay, power, and area, respectively. To show the feasibility of PMP-TVD logic, two testchips are taped out in 65nm and 28nm CMOS processes. With the prototype testchips, we demonstrate that the functionality of the structures built with PMP-TVD gates can be enhanced, erased, or changed in the field using HCI while successfully camouflaging the gate function. PMP-TVD logic family is a promising secure camouflaging method that can be used to thwart reverse engineering and mitigate the threat of untrusted fabrication.

Acknowledgments

I would like to thank my advisor and committee chair, Prof. Ken Mai, for his guidance and support. Throughout my CMU journey, his guidance and enthusiasm made my experience more valuable. I am grateful to him for providing me this opportunity.

I am also very grateful to Prof. Shawn Blanton, Prof. James Hoe, and Dr. Mudit Bhargava for serving on my defense committee. Their time and valuable feedback made this thesis more comprehensive and possible. I also acknowledge the funding from DARPA and Air Force Research Laboratory that supported this work (Funding source award number: FA86501817814).

During my years at CMU, I had the privilege of working and collaborating with many wonderful people. I would like to thank the wonderful and smart people in our research group. Thank you so much, Dr. Burak Erbagci, Dr. Cagla Cakir, Dr. Mark McCartney, Prashanth Mohan, Onur Kibar, and Oguz Atli.

I would like to especially thank Burak Erbagci for countless hours of chats, discussions, tapeouts, and midnight snacks. Since the beginning of my CMU journey, he taught me many things, be it Pittsburgh-related or PhD-related. I am extremely lucky to have him as a friend.

I have been lucky to have great friends during my time at CMU. I would like to thank Yunus Emre Kesim, as he was my gym buddy, discussion buddy, and midnight coffee buddy. I will always remember the time I have spent with him.

I would like to express my gratitude to my dear friends, Duygu Altintas and Alex Corn. Countless of times they fed me with endless BBQs, supplied me bottomless Tequila Sunrises, and let me spend endless time with their pets, Mushroom, Tusk, Freya, Dandy, Fat Pumpkin, Gray Pumpkin, and Gadget. I am extremely grateful to them for letting me stay at their house during the last two months of my time in

Pittsburgh.

I would like to thank my Counter Strike Global Offensive clan, ⓉhiccⓉ, for helping me maintain a balanced life. I shared so many great memories and spent time with my clan members almost every night. They helped me relieve stress during my most stressful times, and I am grateful for that.

I would like to express my deepest gratitude to my other half, Bilgesu Aslan. I have been fortunate to be with her. She gave me the energy to complete my work, always encouraged me, kept me motivated, and relieved my stress. I sincerely thank her.

Last and foremost, I am grateful for my family and their support. My parents, Bergüzar and Şerafettin, and my brother Deniz, gave their full support and provided me with everything. Their uninterrupted support, love, encouragement, and interest made this work possible. I am fortunate to be a part of this family. I would like to thank my extended family as well. I am proud to be from my hometown, Yozgat, and I humbly dedicate this work to Yozgat.

Contents

List of Figures

List of Tables

“Yozgat’a.”

Chapter 1

Introduction

1.1 Motivation

The exponential scaling of semiconductor processes over the past decades providing unprecedented integrated circuit (IC) performance and power efficiency at ever shrinking costs has made use of integrated circuits in critical infrastructure nearly ubiquitous. As a consequence, these ICs have become a tempting target for adversaries seeking to compromise the security of these systems. Thus, securing the design, manufacture, and deployment of these integrated circuits has become a paramount security concern. One of the primary goals of these attackers is to gain access to the design details of the integrated circuits, which then enable myriad cyber-attack vectors including theft of critical data or intellectual property, design cloning/counterfeiting possibly with hardware Trojan insertion, and enhancing other hardware/software attacks.

With the globalization of the semiconductor supply chain and off-shoring of advanced lithographic node foundries, a new method must be found to maintain access to cost-effective state-of-the-art IC fabrication facilities while also ensuring the security of critical intellectual property. While the use of specialized technologies (e.g., 3D integrated non-volatile memory) or elaborate

fabrication flows (e.g., split manufacturing) could mitigate these problems, the cost and complexity of such solutions render them infeasible for many applications. Therefore, we seek to enable access to state-of-the-art untrusted IC fabrication facilities while also protecting sensitive IP, doing so using only conventional IC logic fabrication process flows. Additionally, adversaries have access to advanced reverse engineering technologies capable of complete IC de-processing. Even after manufacturing, a deployed IC may be subject to a reverse engineering attack, compromising its entire design database and manufacturing technology.

1.2 Supply Chain Threats

In recent years, the globalization of the semiconductor manufacturing supply chain has increased the ease with which adversaries can gain access to critical IC details. A modern IC design flow often includes third party standard cell libraries, IP blocks, and CAD tools, as well as outsourced design, manufacturing, testing, and packaging.

Under these circumstances, a chip designer have to transfer the complete IC layout database, often along with other critical design details (e.g., netlist, test vectors), to the manufacturer. Manufacturers are providing more and more design services to their customers, and are often responsible for completing the final design steps (e.g., standard cell and RAM macro block insertion, coverage fill, DRC check, integration with other designs). As the manufacturer is more involved, the designer must send an increasing amount of design information so that proper verification can be performed.

In the past, secure fabrication facilities were used to fabricate ICs with sensitive IP, but with the continued off-shoring of fabrication facilities, this model is not sustainable. Split fabrication has been proposed as a solution [3], but release of even part of the design to the insecure facility may lead to security compromise; the front end of line (FEOL) facility may place restrictions on

which layer to split the fabrication leading to additional information leakage; and there will be an increased cost and complexity to the entire fabrication process. On the design side, researchers have proposed keyed logic and finite-state machines (FSM), but those designs have been shown to be vulnerable to reverse engineering and may have significant overheads. Finally, the keyed logic concept can be taken to the limit leading to fully programmable designs such as FPGAs. While these designs do not release critical IP to the fabrication facilities, they typically suffer an order-of-magnitude or more decrease in efficiency from ASIC solutions.

1.3 Reverse Engineering Threats

Even when the manufacturing supply chain is be secured, the design details of an IC can still be compromised in the field. Myriad of security vulnerabilities can be exposed via the reverse engineering of the ICs contained in electronics systems. The goal of IC reverse engineering is to uncover the functionality and internal structure (e.g., gate netlist, circuit schematic, layout, manufacturing process details) of the chip via techniques such as depackaging/de-layering, high-resolution imaging, probing, and side-channel examination. With this knowledge, an attacker can [4][5][6][7][8]:

- More efficiently mount various attacks (e.g., fault injection, side- channel),
- Clone/counterfeit the design possibly with hardware Trojans inserted,
- and discover trade secrets (e.g., proprietary algorithms, hard-coded keys and instruction sequences).

Reverse engineering capabilities have advanced to the point where a chip designed even with the most advanced technologies can be imaged and reverse engineered by large corporate entities or adversarial nation states with advanced semiconductor capabilities. A number of commercial entities such as ChipWorks [9] and TAEUS [10] offer IC reverse engineering services

and routinely reverse engineer chips in the most advanced process nodes.

1.4 Secure Camouflaged Logic Family

In this thesis, we aim to protect critical intellectual property (IP) embedded in integrated circuit designs during manufacturing and in the field. We propose to use a post-manufacturing programmable camouflaged logic topology to achieve these goals. The basis of the design is a Threshold Voltage Defined (TVD) logic gate topology that uses transistors with different threshold voltage levels, but with identical layouts, to determine the logic gate function [11]. Every TVD logic gate has the same physical layout and is one-time post-manufacturing programmed with different threshold voltages for different Boolean functions. The post-manufacturing threshold voltage programming is achieved using intentional directed hot-carrier injection (HCI). We have used the same technique previously to set device threshold voltages to enhance physical unclonable function (PUF) reliability and to build a true random number generator (TRNG) on a 65nm CMOS testchip [12] [13]. The proposed design technique, post-manufacturing programmed threshold voltage defined logic (PMP-TVD) [14], is fully compatible with standard CMOS logic processes, requiring no special layers, structures, or process steps. At the same time it achieves both concealment of critical IP from the foundry and high resistance against reverse engineering and semi/non-invasive attacks.

Our goal is to show that our techniques enable use of insecure off-shore fabrication facilities for cost effective advanced manufacturing without any additional costly fabrication steps via post-manufacturing programming, and protect deployed ICs against state-of-the-art reverse engineering attacks by concealing the IC design. To show this, we have implemented PMP-TVD in multiple prototype testchips, one in a 65nm and the other in a 28nm CMOS process. In these prototype testchips, we have analyzed the functionality of the PMP-TVD designs before and after HCI stress. In addition, we have explored the permanence of HCI after the stress is applied.

Moreover, we have demonstrated that by applying HCI stress, a preprogrammed design's functionality can be altered, erased, or enhanced in the field, or a blank structure can be programmed post-production. We have also explored the reprogrammability of PMP-TVD structures by reversing the effects of HCI stress with a built-in functionality.

1.5 Dissertation Organization

In Chapter 2, we provide background information on reverse engineering and untrusted fabrication countermeasures. We review some example countermeasures and discuss their shortcomings and overheads. Later, we discuss threshold voltage based countermeasures and analyze the proposed methods in literature.

In Chapter 3, we introduce our secure camouflaging method, threshold voltage defined logic (TVD), for reverse engineering. We explain the details of the design and the operation of the logic family. We discuss the methodology to implement different types of logic gates using the proposed method. Last, we explain the key properties of the logic family.

In Chapter 4, we introduce our secure camouflaged logic family that employs a novel structure with post-manufacturing programmability feature against untrusted fabrication and reverse engineering scenarios. The proposed method, Post-Manufacturing Programmed Threshold Voltage Defined (PMP-TVD) logic, specifically addresses camouflaging and obfuscation of the IP by manipulating the IC physical design. We explain the operation of the PMP-TVD logic family and introduce the method to achieve post-manufacturing programmability. We analyze the design knobs to compare trade offs between performance, area, power, and programming time. Then we discuss the security aspect of the PMP-TVD logic. For analyzing the overhead of PMP-TVD logic, we have synthesized a subset of ISCAS85 benchmarks using PMP-TVD gates and standard cells. We explore two methods for the synthesis. In the first method, we replace every gate

in the benchmark with their PMP-TVD equivalent. In the second method, we generate the look-up-table (LUT) representation of the functionality, and use PMP-TVD gates as LUTs. Then, we compare these PMP-TVD based structures against their standard cell synthesized counterparts and present the overhead values for delay, power, and area.

In Chapter 5, we present the implementation of PMP-TVD structures in 65nm and 28nm CMOS processes. We describe the details of the testchips and explain our testing methodology. Then, we present the measurement results of the implemented structures and show the results of HCI reprogrammability exploration.

In Chapter 6, we summarize the work, draw conclusions, and present future research directions.

Chapter 2

Background

There is a significant body of work in both techniques for reverse engineering of ICs and various countermeasures for protecting IC intellectual property (IP) [15]. Researchers have proposed transforms on the register transfer level hardware description language to make reverse engineering more challenging [16][17]. As these synthesized designs often have significant white-space, researchers also proposed adding unused dummy gates and interconnects [18]. However, these efficiency of these countermeasures depends on the abilities of the attackers. These countermeasures are in an arms race against reverse engineering tools which offer significant capabilities to de-scramble obfuscated designs [9][19][20][21][22][23][24][11].

Adding gates with some form of reconfigurability has been also offered as a way to conceal design intent from reverse engineers. These methods with reconfigurability typically require some form of memory elements to store the configuration in working designs in the field [25][26][27]. Thus, even if the basic design database does not contain the design information, the deployed systems do in their configuration memory elements, and therefore are mostly vulnerable to reverse engineering [11].

There have been proposals for camouflaged gates using dummy contacts or look-alike gates

to hide the functionality of the structures [25][28]. However, security of these camouflaged structures limited by the capabilities of the attacker. To overcome these issues, threshold voltage based camouflaging techniques are proposed [11]. These designs seek the same goals, but using different methods for the design intent concealment.

In this chapter, we review some example camouflaged methods proposed by researchers and discuss their advantages and issues. To overcome the issues they present, we propose using threshold voltage based countermeasures. We explain the benefits of the methodology, and analyze example countermeasures that are based on this methodology.

2.1 Reverse Engineering and Untrusted Fabrication Countermeasures

2.1.1 Look-alike Gates

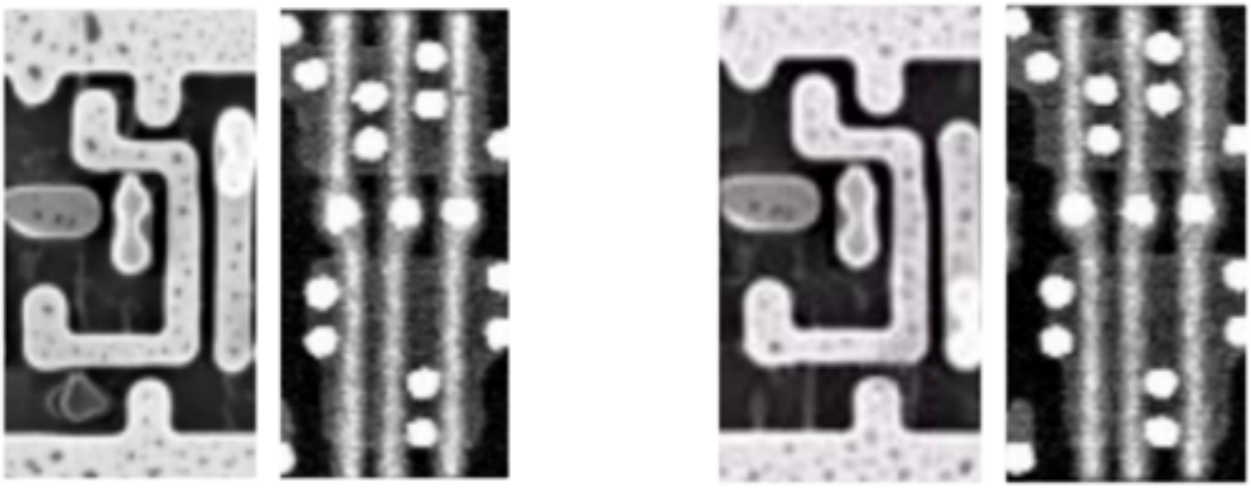


Figure 2.1: SEM images of a regular AND2 (left) and AND2 look-alike gate (right), which functions as OR. Dummy metallization is used to create look-alike gate layouts [28].

To combat reverse engineering, researchers have proposed a number of countermeasures including gate camouflaging wherein an attacker cannot discern the functionality of a particular

logic gate based solely on its observable physical characteristics. One proposed camouflaging technique from SypherMedia [28] uses look-alike gates. In this method of gate camouflaging, similar layouts for certain gate types are used to obfuscate the functionality of the gate. With small or minuscule overheads, some logic functionalities can be laid out to look similar to each other. Figure 2.1 shows an AND2 gate (left) and an AND2 look-alike gate (right) with an OR2 functionality. The metal layers and contacts in the figure are placed in such a way that both of the gates' layouts look very similar. However, only a limited number of gates can be made look similar to each other, which limits the camouflaging efficiency. Another issue is that the minor differences in both of the gates (such as the locations of the contacts, extra diffusion or metal) could make the gates discernible.

2.1.2 Camouflaging Using Dummy Contacts

Another proposed camouflaging technique uses a mix of dummy and real vias/contacts to obscure the gate function [25]. In this camouflaging method, dummy vias/contacts are not fully formed and do not make an electrical connection between layers. However, these dummy connections may possibly be mistaken for real vias/contacts during delayering. The proposed design shown in Figure 2.2 uses a gate that can form a NAND, NOR, or XOR gate with identical layouts except for the placement of real and dummy vias. If the top view of the gate is analyzed, all the contact locations and metal layers will be same for these three types of gates. However, a cross section image of the gate shows us the contacts, which might reveal that the dummy contacts are discernible from the real ones. Moreover, these gates are made with special structures requiring special layers, DRC waivers, and other low-level process manipulations. In this camouflaging method, only a small subset of logic functions can be camouflaged due to their high overheads in area, delay, and power consumption.

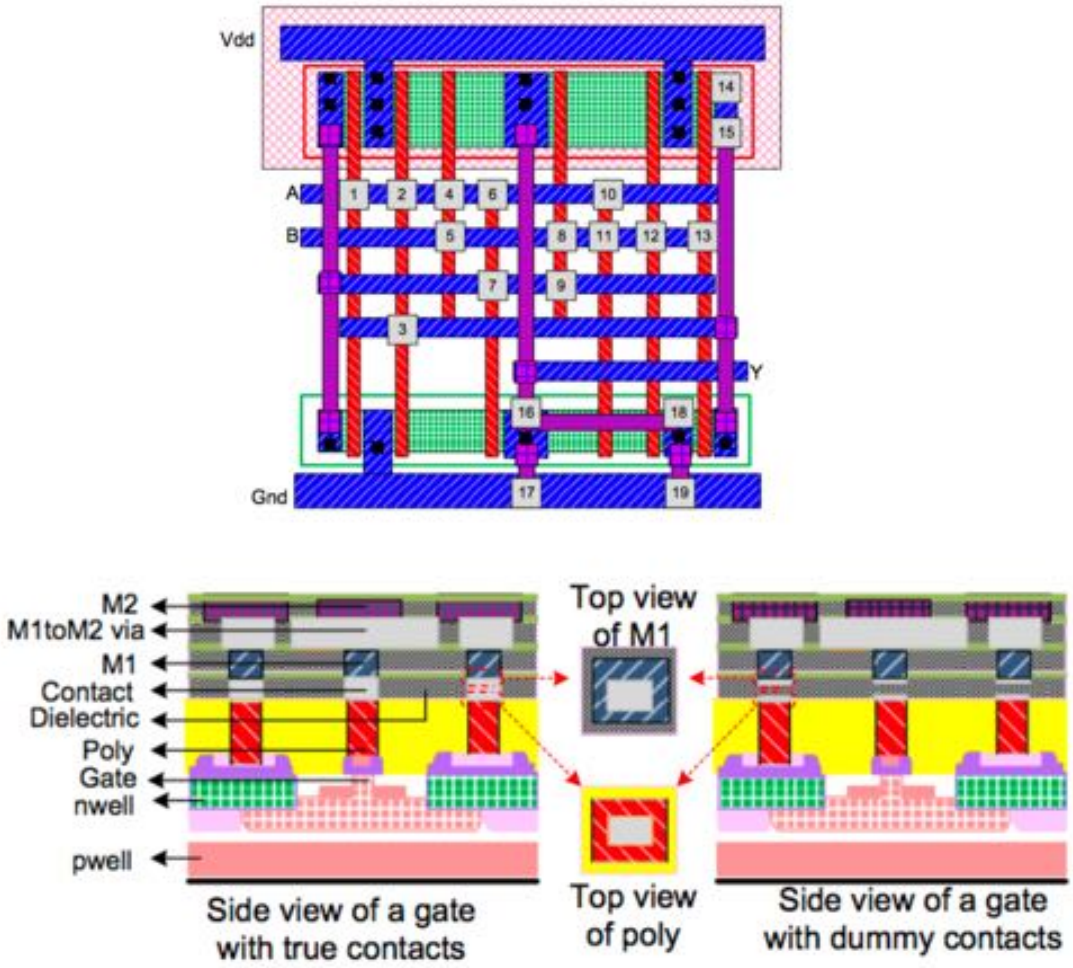


Figure 2.2: The layout image (top) of the camouflaged gate structure proposed by Rajendran et al. and cross section of real and dummy contacts (bottom) [25].

2.1.3 Issues with Current Camouflaging Methods

Although camouflaged gates can make reverse engineering more challenging for the attackers, there are a number of issues with the existing camouflaged gate structures. First, the security of these proposed techniques rely on the limited ability of the attacker to distinguish between real and dummy structures. However, the delayering and imaging capabilities of state-of-the-art reverse engineering are advanced enough to not be fooled by such structures [9]. Further, dummy via/contact fabrication is caught in a dual-sided constraint between reliability and security. If the

dummy structure has a large separation between layers, then the reliability is good, but it is more easily distinguished as a dummy. Conversely a small separation is harder to distinguish, but is more likely to be shorted due to manufacturing variation and therefore leads to a faulty IC. Additionally, the compatibility of building dummy vias/contacts in a modern process is still questionable, as in such processes, the vias/contacts are formed in the same manufacturing step as the interconnect wires themselves. It is unclear how such a partially connected via/contact could be formed without additional special process steps and masks, increasing the cost and complexity of implementing the countermeasure.

Moreover, the dummy gates suffer from area, power, and delay overheads (up to 4x, 5.5x, and 1.8x, respectively) [25][11]. Finally, the designs can be equipped with anti-tamper countermeasures in an attempt to prevent reverse engineering, but these are typically not sufficient to prevent a well-funded technologically sophisticated attacker such as a large corporation or adversarial nation state from performing the reverse engineering successfully.

2.1.4 Threshold Voltage Based Countermeasures

To overcome the issues discussed in the previous section, the transistor threshold voltage can be used as a means of determining the gate function and thereby camouflaging the gate type. In today's processes, multiple transistor threshold voltage levels are offered. Most general threshold voltage levels offered are transistors with *low threshold voltage (LVT)*, *standard threshold voltage (SVT)*, and *high threshold voltage (HVT)*.

LVT devices require a smaller V_{GS} bias compared to SVT devices to turn on, and HVT devices require a higher V_{GS} bias (Figure 2.3). This means that for the same amount of V_{GS} bias, an LVT gate will pass more current compared to a HVT gate, and therefore performance of gates with LVT devices will be higher at the same bias level. Same sized LVT and HVT transistors are identical except for their threshold voltage mask layers. These devices differ only in number of

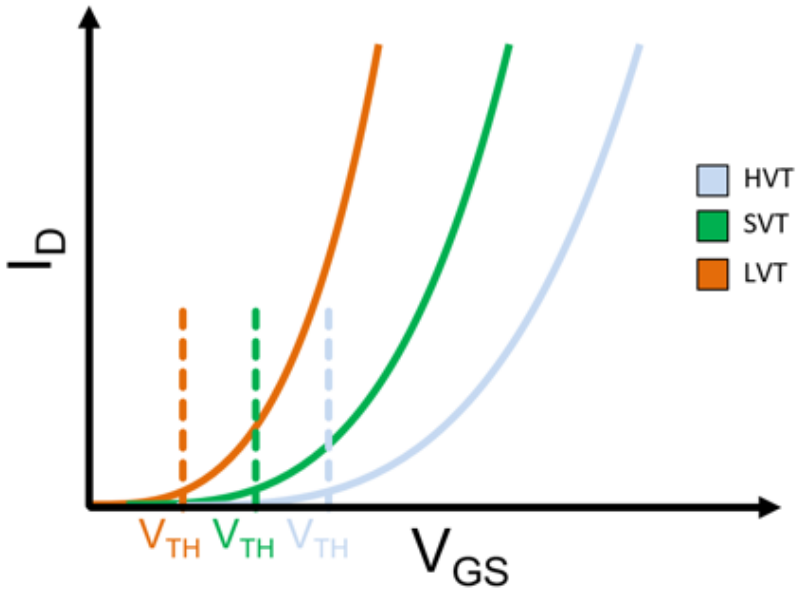


Figure 2.3: $V_{GS} - I_D$ graph of multiple threshold voltage levels, *low threshold voltage (LVT)*, *standard threshold voltage (SVT)*, and *high threshold voltage (HVT)*.

ions implanted in the channel, which is extremely difficult for a reverse engineer to determine, especially on a mass scale. By using different threshold voltage transistors, threshold voltage based solutions can be implemented as a countermeasure against reverse engineering.

While the transistor threshold voltages are not directly discernible from delayering and imaging the IC, there are various methods for measuring the channel doping in literature. Among these are spreading resistance profiling, secondary ion mass spectrometry, scanning capacitance microscopy, kelvin force probing microscopy, and electron holography [29][30][31][32][33]. However, these techniques have limitations in both spatial resolution and accuracy that make them unsuitable for large-scale reverse engineering of a modern IC [34][35][36][37][11]. In a structure with thousands of camouflaged gates, an attacker would need to probe out the threshold voltage of a larger number of devices, potentially in the tens of thousand or millions, in order to de-camouflage the IC. Even if the available techniques could provide the needed resolution of accuracy, the sheer number of devices that would need to be probed would present an additional barrier to the attacker [11].

In the threshold voltage based solutions, the primary requirement is to amplify the threshold voltage difference of the transistors to achieve logic levels for a desired functionality. This amplification can be done in a single-ended or differential manner. Some example single-ended amplification solutions are threshold voltage defined switches [38] and threshold-dependent camouflaged cells [39].

Threshold Voltage Defined Switches

In the threshold voltage defined switch method, HVT and LVT devices are used as switches. The transistors are biased at the mid-point between the nominal NMOS and PMOS threshold voltage levels, so that when the bias is applied a HVT gate does not conduct whereas a LVT gate does (Figure 2.4) [38].

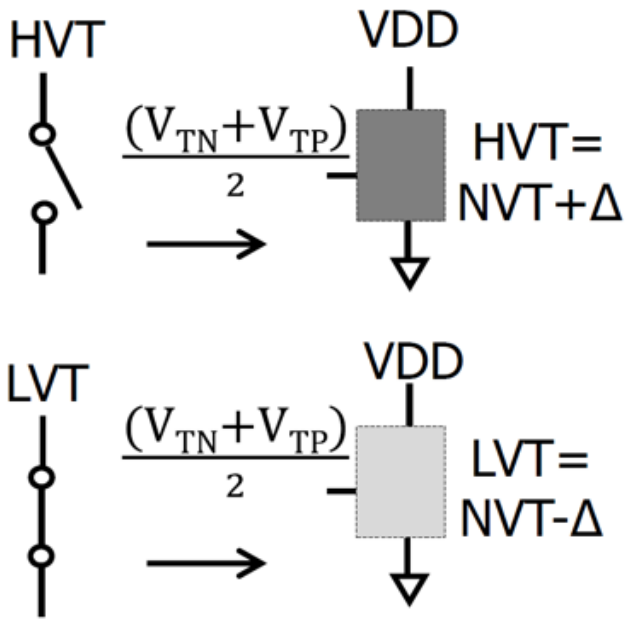


Figure 2.4: Threshold programmable switches in threshold voltage defined switches [38]. With a bias at the mid-point between the nominal NMOS and PMOS threshold voltage levels, a LVT gate conducts whereas a HVT gate does not.

Using the implemented switches, camouflaged gates with NAND, AND, NOR, OR, XOR, and XNOR functionalities can be built. The implemented functionality depends on the threshold

voltage of the switch. However, due to supporting many camouflaged functionalities, the overhead of the camouflaged gate is high. Therefore, to reduce overheads a smaller camouflaged gate that can only realize NAND, NOR, and OR functionalities is also proposed.

For a NAND functionality, the reported overheads compared to a standard NAND gate for area, delay, and power are 12.63x, 2.2x, and 16.89x, respectively [38]. In addition to larger overheads, this design approach depends on a large I_{ON}/I_{OFF} current ratio between LVT and HVT devices where they are biased at a mid-point of their threshold voltage values. Since the devices are not fully turned on or turned off, compared to standard cells, the camouflaged cell will perform slower, and the power consumption will be higher. Moreover, the generation of the mid-point bias voltage requires a resistance ladder. On top of all these issues, the method uses single-ended amplification. Any small variation and/or noise will be amplified, and since there is not any common node to remove the effects of variation and noise, the robustness of the gate will be affected. Shift in the bias voltage will affect the performance and the power consumption of the gate, or even worse, the gate will not operate correctly at all.

Threshold-Dependent Camouflaged Cells

Another method which was proposed by Collantes et al. use pass gates to implement threshold-dependent camouflaged cells [39]. Their implementation (Figure 2.5) can only realize AND or OR functionality depending on the pass gates either being LVT or HVT. According to the 22nm Predictive Technology Models (PTM) that the gates are implemented on, node X swings between 0.2V and 0.4V where the nominal VDD of the process is 1V. Effectively, at node X, 0.2V is logic-0 and 0.4V is logic-1. To fix the logic levels to normal logic levels, skewed inverters with degraded noise margins at the output are used.

However, just like the threshold voltage defined switches, threshold-dependent camouflaged cells suffer are vulnerable to variation and noise due to single-ended amplification. Furthermore,

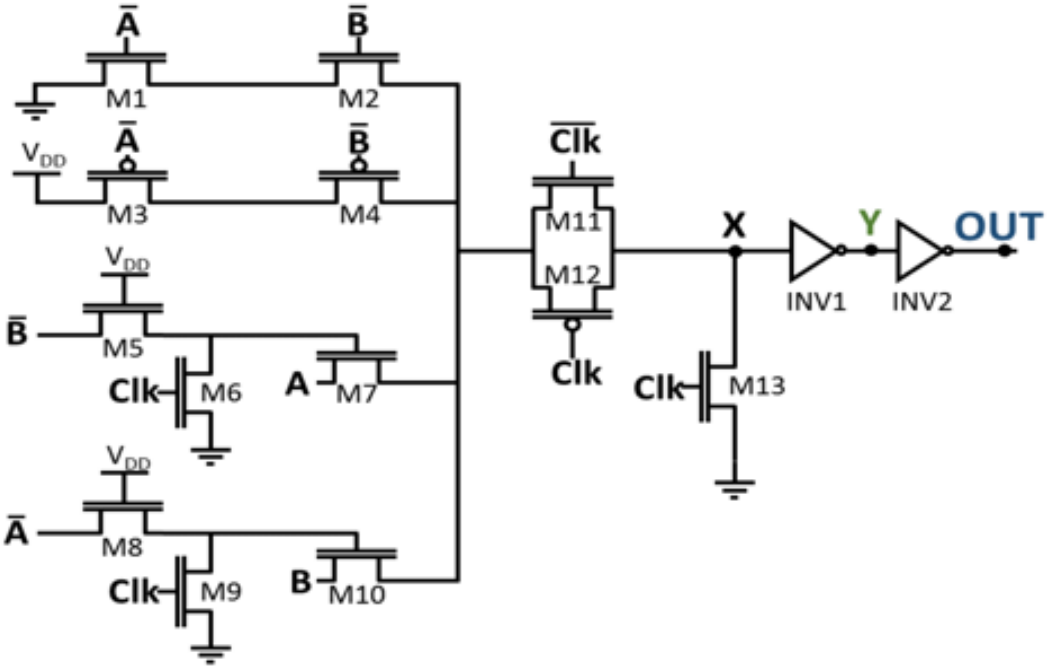


Figure 2.5: Threshold-Dependent camouflaged cell schematic that can function as an AND or OR [39].

the skewed inverters at the output have small noise margins which makes them also sensitive against variations and noise.

Since the current technology nodes have small threshold voltage difference between device types, these single-ended solutions are highly sensitive against process/voltage/temperature (PVT) variations and noise. Hence, we can use differential amplification techniques that employ sense amplifiers where the small difference in the threshold voltage difference is amplified to logic levels. The differential designs will be more robust against the PVT variations and noise compared to single-ended solutions.

2.2 Summary

In the introduction, we provided motivation and context for the thesis. In this chapter, we pave the way to countermeasures for reverse engineering. First, we discuss some proposed coun-

termeasures to prevent reverse engineering. Then, we explain the disadvantages of the current solutions and discussed that the threshold voltage based solutions can overcome the disadvantages. Finally, we reviewed some example threshold voltage based solutions and analyzed their advantages and disadvantages.

Chapter 3

Threshold Voltage Defined (TVD) Logic

So far, the camouflaging solutions against reverse engineering threats rely on the limitations of the attacker. Therefore, threshold voltage based countermeasures are proposed. The previous chapter discusses threshold voltage based solutions with single-ended amplification with reduced reliability. In such cases, differential amplification techniques that use sense amplifiers by amplifying the small difference in the threshold voltage difference to logic levels can be employed. The differential designs will be more robust against the PVT variations and noise compared to single-ended solutions.

In this chapter, we introduce our method of threshold voltage based solution against reverse engineering. Threshold voltage defined (TVD) logic design is a gate camouflaging technique that does not rely on limited delayering and imaging resolution for security. The design is based on a sense amplifier, which has differential amplification, therefore the design is more robust against PVT variations and noise compared to the single-ended threshold voltage based solutions discussed in the previous chapter. Furthermore, TVD does not require any additional process steps or masks unlike dummy via based camouflaging gates and is fully compatible with modern CMOS process technology.

3.1 TVD Logic Basic Operation

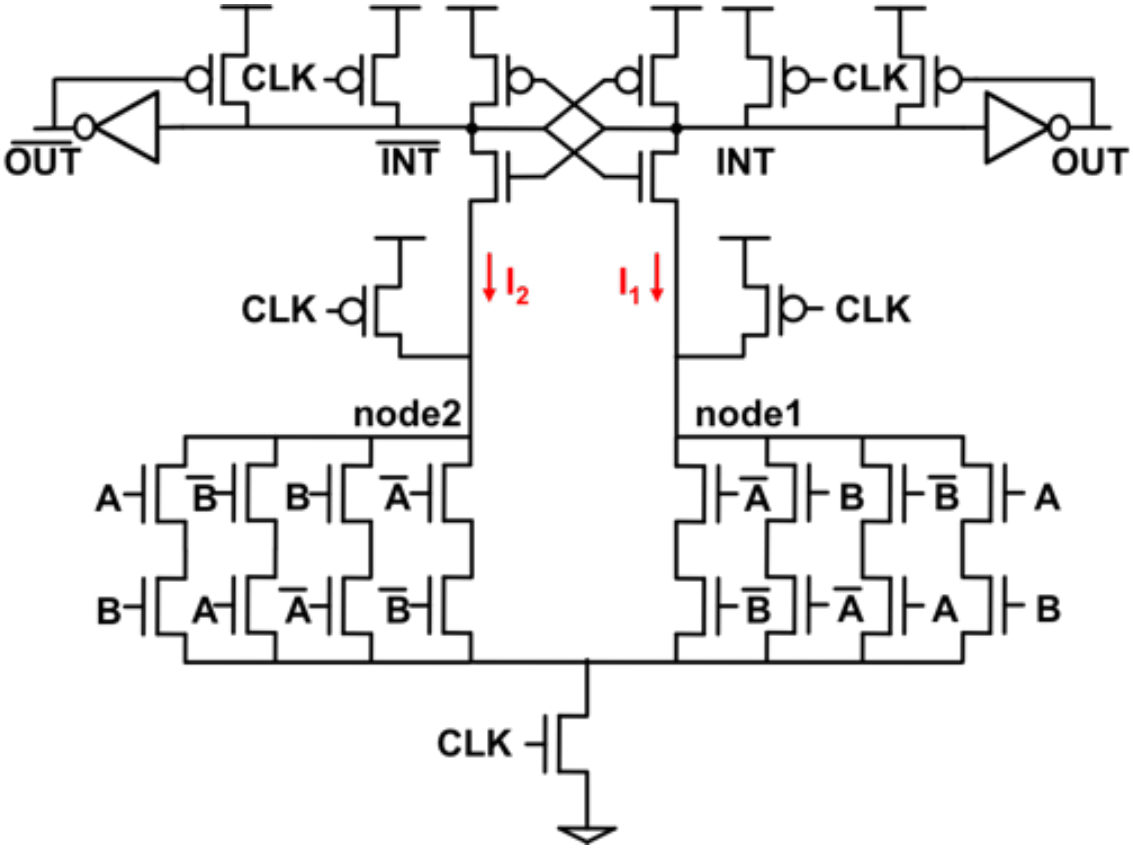


Figure 3.1: A generic 2-input TVD logic gate schematic. Different Boolean functions can be realized by using different threshold implants for transistors in differential pull-down networks (PDNs). Half keepers (on both *INT* and $\overline{INT}$) and the PMOS precharge transistors (on both *node1* and *node2*) are also added to improve gate robustness [11].

The TVD logic gate is based on sense amplifier based logic (SABL) [40] which uses a *StrongArm flip-flop* (SAFF) topology but replaces the input differential pair with a differential pull-down network (PDN) determined by the desired logic function.

A generic 2-input TVD logic gate schematic is shown in Figure 3.1. TVD is a precharged differential structure with an embedded cross-coupled inverter positive feedback amplifier at the top, and a replaced pull-down network at the bottom. Both right and left branches in the pull-down network (i.e. *node1*, *node2*) of a 2-input TVD logic gate consist of four parallel strings. Each branch is stacked with two NMOS transistors, each couple for every input combination

(A/B as $0/0, 0/1, 1/0, 1/1$).

TVD logic is a differential dynamic logic with two phases, precharge and evaluate. In the precharge phase, *CLK* signal is low, and thus the internal nodes *node1*, *node2*, INT, and $\overline{INT}$ are precharged to VDD. Since the internal nodes are precharged, the output nodes OUT and $\overline{OUT}$ are pulled down to VSS. Therefore, all the input pairs of the TVD gate are low. When *CLK* signal goes high, the evaluate phase starts. At this point, the gate waits for valid signals for both of its outputs. A valid signal is defined as $A/\overline{A}$ and $B/\overline{B}$ being *0/1* or *1/0*. When the inputs are valid, a branch from the left and a branch from the right side will have two conducting NMOSes. Being connected to the same inputs, the relative strength of these activated branches determines the output value of the gate. Then, the current difference is amplified by the cross-coupled inverters. Eventually, one of the branches continues to have a path to VSS, while the other path does not, causing the cross-coupled inverter to flip in the appropriate direction. After one of the internal nodes, INT or $\overline{INT}$ is pulled down to VSS, the output inverter next to it pulls the appropriate output node to VDD. After the gate fires and the current difference is amplified to a full logic level, no static current flows. Having a valid output concludes the evaluate phase of the gate.

In the TVD logic gate design, both branches conduct, but asymmetrically such that one will be drawing more current than the other (Figure 3.1), which then determines the value of the output. Therefore, a logic function can be programmed into the gate by determining the current difference between the branches that have the same input combinations. The current difference is introduced by using different threshold implants (i.e. *low threshold voltage* (LVT), *standard threshold voltage* (SVT), and *high threshold voltage* (HVT)) for transistors in differential pull-down networks. An LVT transistor can pull more current compared to a HVT transistor under same gate biasing. Since the inputs for transistors in both left and right branches are identical, different threshold implants are used to create a current difference (ΔI) between those branches (>0 or <0). Stronger strings consist of LVT transistors, while the weaker ones consist of HVT

transistors. Therefore, a string of LVT transistors will pull more current than that of HVT transistors, and the gate will fire accordingly.

For example, if $I_1 > I_2$ according to some input combination, then the INT is pulled down to VSS, while $\overline{INT}$ stays at VDD. Hence, OUT rises to VDD and $\overline{OUT}$ remains at VSS. Therefore, for a certain input combination, if output is required as $OUT/\overline{OUT}= 1/0$, then the current difference should be set as $I_1 > I_2$. To achieve this, for that input combination, the NMOS devices on the right branch should be LVT devices and the ones on the left branch should be HVT devices.

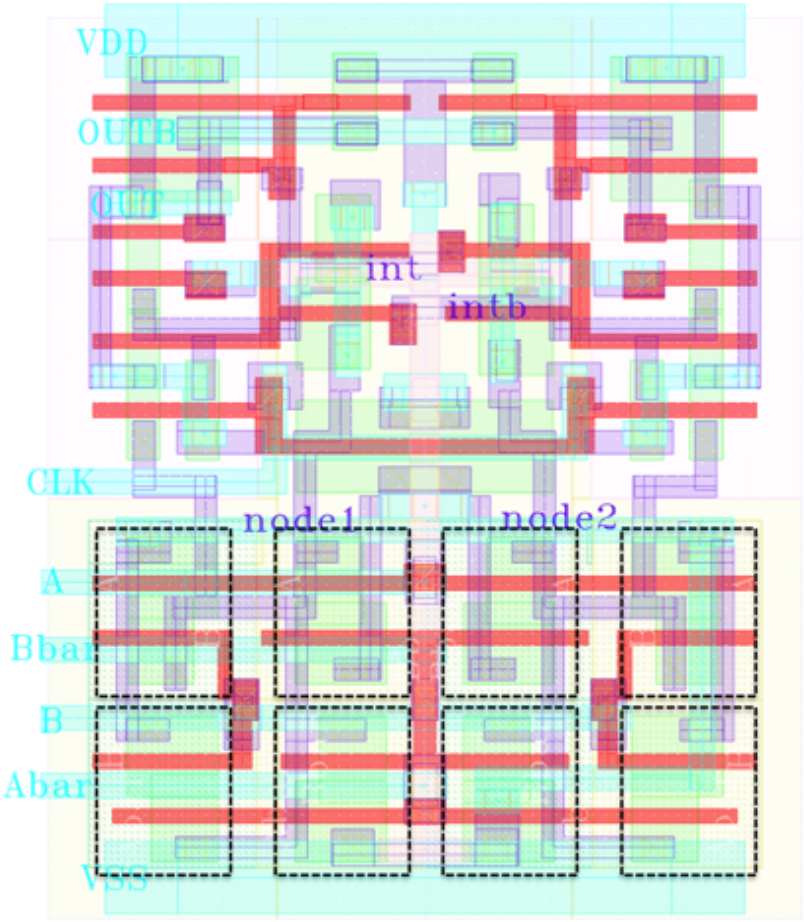


Figure 3.2: A generic 2-input TVD logic gate layout. Different gate types are realized by one time mask programming of the transistors in differential pull-down networks (PDNs) with LVT or HVT implants. All 8 strings with 2-stacked NMOS transistors that need to be programmed are highlighted with dashed lines [11].

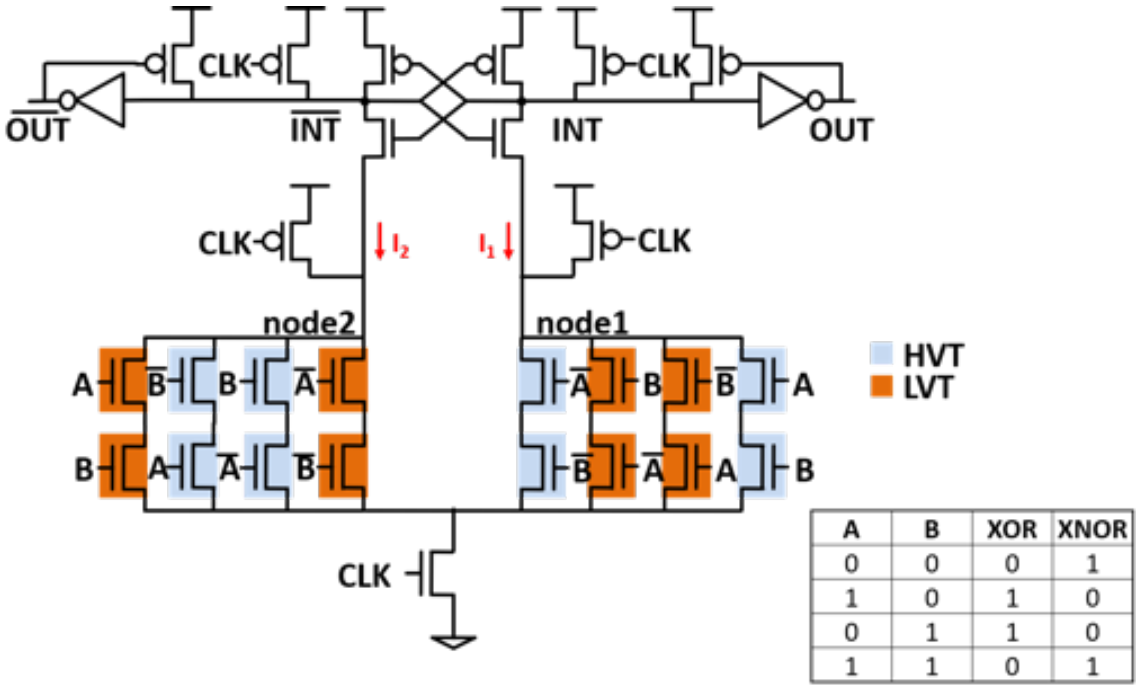
The layout of a generic 2-input TVD logic gate is shown in Figure 3.2. The cross-coupled inverters, precharge PMOSes, and the output inverters are located at the top half of the layout. At the bottom half of the layout, the highlighted parts show each of the stacked NMOS pairs that takes the input combinations. By assigning HVT or LVT threshold implants, the logic functionality of the gate can be programmed to any function desired. The pull-down network, NMOSes of the cross-coupled inverters, and the PMOS of the output inverters are in the critical path of the gate. Therefore, these devices should be sized properly to achieve a good performance while maintaining a small area and power overhead compared to standard cell counterparts.

For the example 2-input TVD gate, there are four possible input combinations ($2^2 = 4$). Each possible input combination can have 2 outcomes, either 0 or 1. Therefore, the total possible functionality that a 2-input TVD gate can take is $2^{(2^2)} = 16$. If we generalize this formula, for an n-input TVD gate, the total possible functionalities that the gate can have is $2^{(2^n)}$.

3.1.1 Example: A 2-input TVD XOR Gate

A 2-input TVD XOR gate and its truth table is shown in Figure 3.3. In an XOR gate, the output will be logic-1 when the inputs are different, and logic-0 otherwise. Therefore, in a 2-input TVD XOR gate, the stacked transistors that are connected to the inputs $A - \overline{B}$ and $\overline{A} - B$ on the side of *node1* are LVT devices. On the other hand, the stacked transistors that are connected to the inputs $A - B$ and $\overline{A} - \overline{B}$ have HVT implants on the side of *node1*. Asymmetrically, the devices on the *node2* side are the exact opposite devices compared to *node1* side (i.e, HVT devices on one side are LVT devices on the other and vice versa)(Figure 3.3).

The transistors are sized such that the NMOS stack have minimal delay overhead while not increasing the input capacitance and internal node capacitance excessively. The precharge devices are sized the minimum device size allowed. The cross-coupled inverters are skewed inverters favoring the NMOS devices due to the NMOS stack and increased internal capacitance at



A	B	XOR	XNOR
0	0	0	1
1	0	1	0
0	1	1	0
1	1	0	1

Figure 3.3: 2-input TVD XOR gate. Transistors with LVT threshold implants are shown in orange, and HVT transistors are shown in blue. Truth table of XOR gate is also shown [11].

node1 and *node2*. Finally, the output inverters are also skewed inverters, but favoring the PMOS devices, since at the beginning of evaluate phase, the output nodes are pulled down to VSS and when the gate evaluates, one of the output nodes is pulled up to VDD.

Figure 3.4 shows the timing diagram for a 2-input TVD-XOR gate for two operating cycles where the inputs A/B transitions from $0/0$ to $0/1$, and from $0/0$ to $1/1$. In the precharge phase, *CLK* is low, thus, *INT* and $\overline{INT}$ are precharged to VDD. When *CLK* goes high, the gate starts its evaluate phase. For the input combination $A/B = 0/1$ ($\overline{A}/\overline{B} = 1/0$), more current flows through *node1* branch ($I_1 > I_2$) because of the LVT transistors in the stack. Therefore, *INT* goes low rapidly, while $\overline{INT}$ makes a small dip and then remains high. Since, *INT* is pulled down to VSS, *OUT* goes high, and $\overline{OUT}$ remains low. On the other hand, for input combination $A/B = 1/1$ ($\overline{A}/\overline{B} = 0/0$), this time more current flows through *node2* branch ($I_2 > I_1$) and $\overline{INT}$ goes low rapidly, as *INT* makes a small dip and remains high. Since, $\overline{INT}$ is pulled down to VSS, $\overline{OUT}$ goes high, and *OUT* remains low. After each evaluate phase, during the precharge

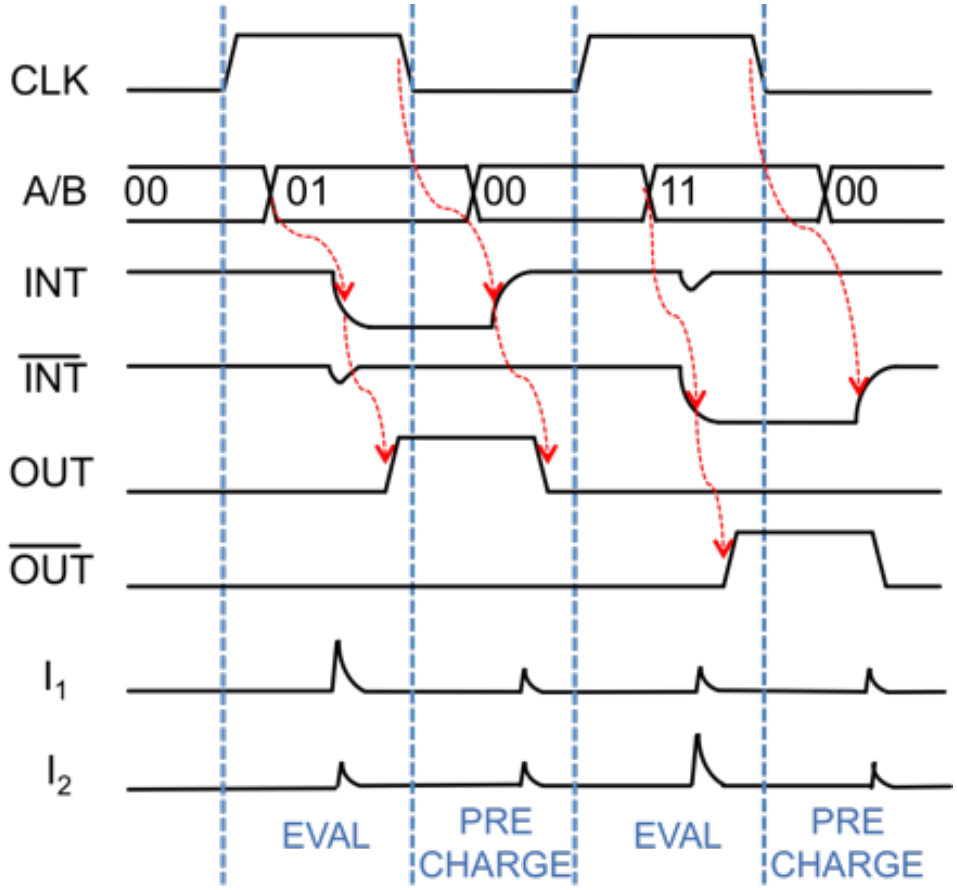


Figure 3.4: Timing diagram of a 2-input TVD XOR gate for the input transitions of 00 to 01 and 00 to 11 [11].

phases, internal nodes *INT* and $\overline{INT}$ are charged to VDD. This effectively pulls output nodes *OUT* and $\overline{OUT}$ down to VSS. Since the inputs to the gate are the outputs of other TVD gates, the inputs $A/\overline{A}$ and $B/\overline{B}$ become $0/0$ as well.

3.2 Other TVD Logic Gates

Although one time mask programming of a 2-input TVD-XOR gate is described in detail, in a 2-input TVD gate, any 2-input Boolean function can be realized by using the same method. For instance, the programming of 2-input TVD-AND and TVD-OR gates are shown in Figure 3.5 and Figure 3.6, respectively.

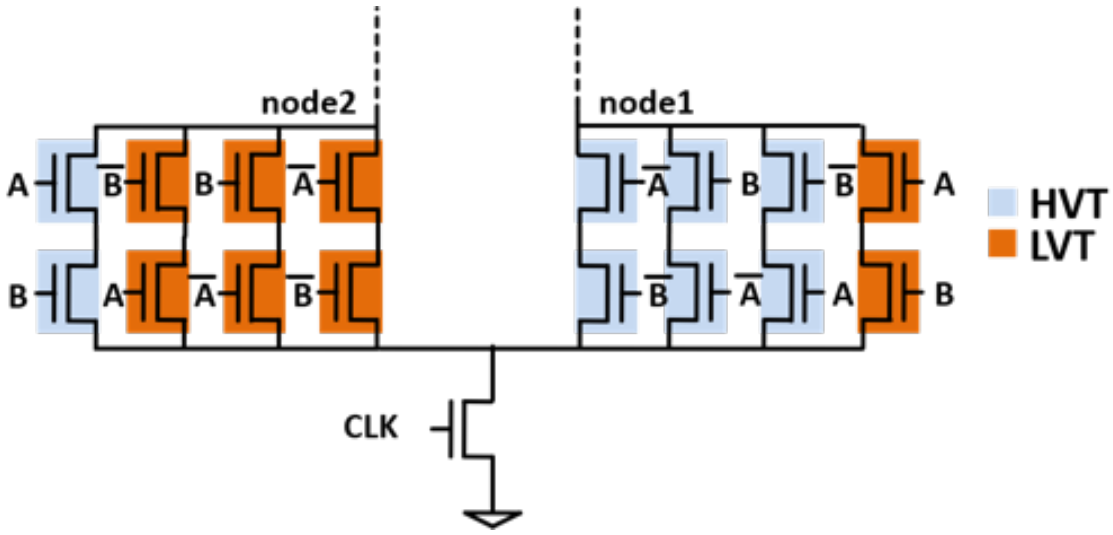


Figure 3.5: 2-input TVD-AND gate. Only the transistors in differential PDNs, which need to be programmed, are shown. Transistors with LVT threshold implants are shown in orange and HVT transistors are shown in blue [11].

TVD logic concept can be extended to n-input gates where $n>2$. However, the number of parallel strings (k) increases exponentially as the number of inputs increases (i.e. $k = 2^n$). Moreover, the number of transistors in pull-down stack (i.e. n) is going to increase as well. Because of the exponential increase of the number of parallel strings and the linear increase in stack height, the gate speed will be degraded. The area and power consumption will increase as well.

Additionally, a single-ended version of the TVD logic can be implemented. The single-ended version of a 2-input TVD-XOR gate is shown in Figure 3.7. The pull-down network on *node2* branch can be replaced by a single reference string with always-on SVT transistors. Depending on the threshold implants used in the actual pull-down network, ΔI will be either > 0 or < 0, hence the gate will fire accordingly. However, because the SVT string is always conducting, the inputs must be valid when *CLK* goes high. Therefore, delayed clock between every TVD logic stage should be used for single-ended TVD logic. Alternatively, a *completion detection signal* similar to [41] from the previous gate can be used to initiate evaluation in the following stage. Note that this is only a requirement for *single-ended* TVD logic. Differential TVD logic

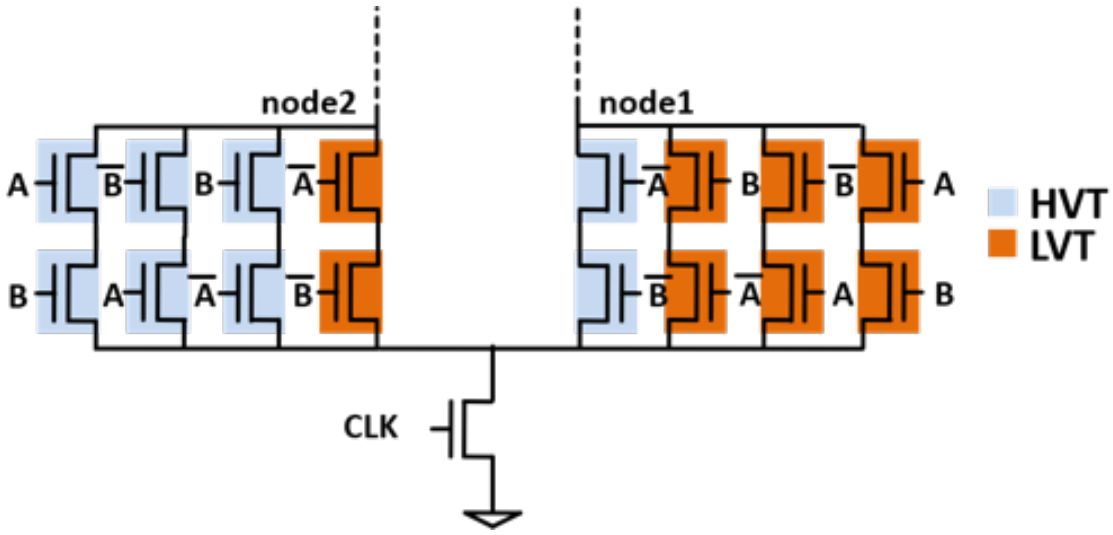


Figure 3.6: 2-input TVD-OR gate. Only the transistors in differential PDNs, which need to be programmed, are shown. Transistors with LVT threshold implants are shown in orange and HVT transistors are shown in blue [11].

as previously described can operate and be chained same as the conventional domino logic and does not require any special clocking.

3.3 TVD Logic Properties

The proposed TVD logic is a differential dynamic logic that can securely camouflage the functionality of a gate. It has two phases, evaluate and precharge. Due to its symmetric design, it has additional security advantages in addition to being a camouflaging method.

Delay

All TVD logic gates have similar delays regardless of the functions they implement. Since it is a dynamic logic with precharged internal nodes, all the input transitions will have similar delays as well. The delay overheads for TVD gates depends on the functionality they implement. Although all of them have similar delays, a 2-input TVD NAND gate will have a higher delay overhead than a 2-input TVD XOR gate compared to static CMOS standard cells.

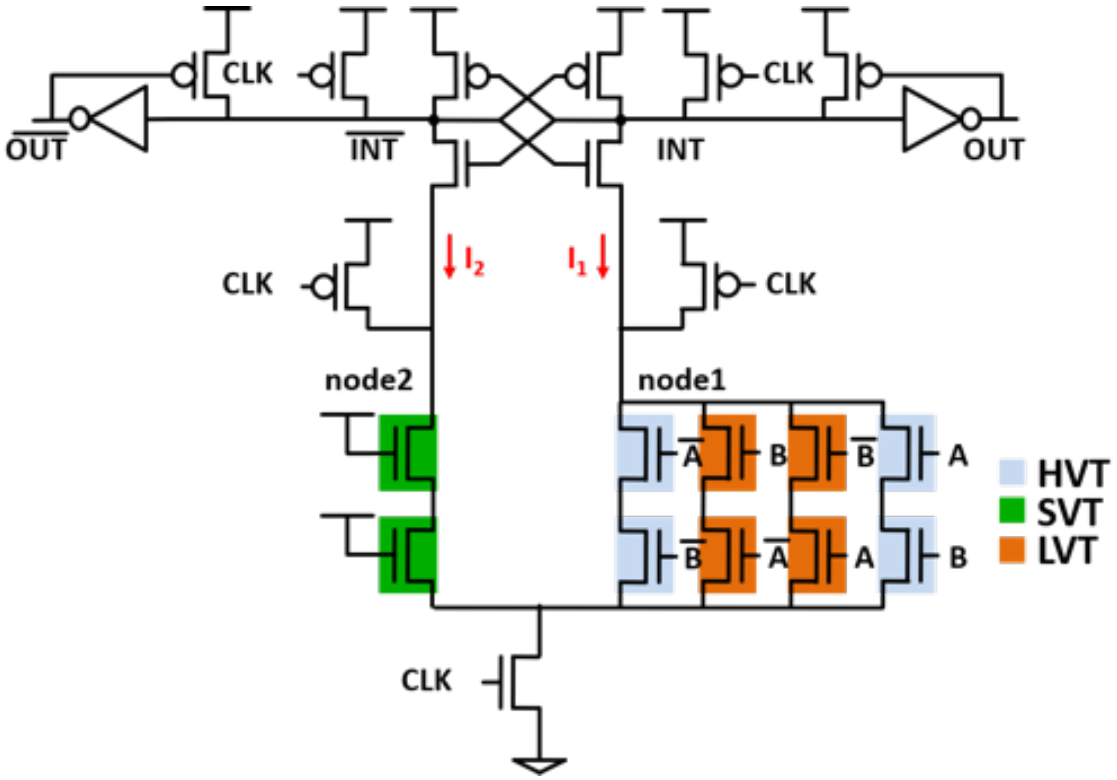


Figure 3.7: Single-ended 2-input TVD-XOR gate. Transistors with LVT, SVT, and HVT threshold implants are shown in orange, green, and blue, respectively [11].

Area

All TVD logic gates with same number of inputs have the exact same area regardless of the functions they implement. The only difference between each different gate is the threshold implants they have to implement different functionalities. Similar to the delay of TVD gates, their area overheads will depend on the functions they have as well. A 2-input TVD NAND gate's area overhead will be higher than a 2-input TVD XOR gate compared to their static CMOS standard cell counterparts.

Power

All TVD logic gates have similar power consumption regardless of the function they implement and regardless of the input transition they observe. Each evaluate cycle, one of the input nodes is discharged and one output node is charged. During precharge phase, the discharged internal

node is charged back, and the charged output node is discharged. Due to its symmetric design, the power consumption at every cycle will be similar. And again, the power overheads will be similar to delay and area overheads, where it will depend on the functionality that the gate realizes.

Simplified TVD Logic

The area, delay, and power overheads for TVD logic can be decreased by limiting the possible Boolean functions supported. For instance, for both TVD AND and TVD OR logic gates, the stacked transistors that are connected to the inputs $A - B$ will have LVT and HVT threshold implants, while the ones that are connected to the inputs $\overline{A} - \overline{B}$will have HVT and LVT threshold implants for branches *node1* and *node2*, respectively. Hence, one string from each branch can be removed safely for a generic TVD logic gate that can support only AND and OR functions. This results in a simpler camouflaged gate structure with lower overheads.

Process Variation, Robustness, and Reliability

The operation of TVD logic is based on one time mask programming of the transistors in differential PDNs. Similarly, the Boolean functionality of the gate also depends on the threshold voltages of those transistors. Differential amplification structure reduces the effects of variations in the threshold voltage. As a result the robustness and the reliability of the structure can be ensured with decreased variation effects and careful sizing.

Reverse Engineering

All TVD logic gates have the same template layout. The functionality of each gate is defined by using different threshold implant masks (either LVT or HVT) for the transistors in the corresponding branches. Therefore, TVD logic gates have the exact same layout, footprint, and input/output/internal connections, making them virtually indistinguishable. The only way for

an attacker to identify a TVD gate in a design, then, becomes probing the threshold voltage for every transistor in the pull-down network or to functionally test the gate, making the reverse engineering extremely challenging.

Power Analysis and Timing Analysis

The differential nature of TVD logic also reduces side-channel leakage against power analysis attacks [42], which exploit the data dependent power consumption in the hardware. The differences in delays for different gate types and input combinations can also be exploited by an attacker [43]. However, the maximum deviation in delays per gate type and input combination are minimal in the TVD logic.

Although TVD logic gates have delay, power and area overheads over the static CMOS standard cells, limiting the number of gates in a design camouflaged can further reduce the overhead. Researchers have proposed various selection algorithms for camouflaging a design to keep the overhead at a reasonable level, while ensuring the security against reverse engineering attacks [25]. The use of TVD logic gates is orthogonal to those lines of research, as TVD logic is simply another style of camouflaged gates that those algorithms could be used with.

3.4 Summary

In this chapter, we proposed Threshold Voltage Defined (TVD) logic as a gate camouflaging technique. The proposed technique does not rely on limited delayering and imaging resolution for security, does not require any additional process steps or masks, is fully compatible with modern CMOS process technologies, and has low area, power, and delay overheads. TVD logic gate topologies use different threshold voltage transistors, but with identical layouts, to determine the logic gate function. Every TVD logic gate has the same physical layout and is one time mask programmed with different threshold implants for different Boolean functions. In summary,

TVD logic is a feasible countermeasure against reverse engineering where TVD also removes the the problems of other threshold voltage based countermeasures that implement single-ended amplification due to its differential amplification structure.

Chapter 4

Post-Manufacturing Programmed Threshold Voltage Defined (PMP-TVD) Logic

TVD logic gate topology removes the reliance on the limitations of the attacker by having different threshold implants. However, to manufacture a chip, this design information needs to be sent to the foundry. Although TVD protects the design against reverse engineering threats, it is still vulnerable against supply chain threats in untrusted fabrication scenarios. To address this issue, we introduce a Post-Manufacturing Programmed Threshold Voltage Defined (PMP-TVD) logic, against IC reverse engineering and untrusted fabrication. The basis of the design is a TVD logic gate topology that solely uses transistors with different threshold voltages in the pull-down networks to determine the logic function of a gate [11]. As in TVD gates, PMP-TVD gates with same number of inputs have identical physical layouts. Furthermore, PMP-TVD gates can be post-manufacturing programmed with different threshold voltages for different Boolean functions using intentional directed hot-carrier injection (HCI). Post-manufacturing programmability feature of PMP-TVD gates provides the protection against untrusted fabrication, because the

critical design information supplied to the foundry can be later changed in the field.

In the following, we explain the concept of programmable TVD logic. We explain HCI physical phenomenon that is used for post-manufacturing programming in PMP-TVD gates. Then, we introduce our proposed design, PMP-TVD. We explain operation of an example PMP-TVD gate both under normal operation and after HCI programming. We analyze the design knobs of the PMP-TVD gates. Furthermore, we talk about the characterization of HCI. We introduce binary aging elements (BAE) that we used for characterization in our testchips, and we present additional use cases for the BAEs. We evaluate the security of PMP-TVD gates and compare them against other proposed methods. Finally, we analyze the overhead of the structures built with PMP-TVD gates compared to structures built with standard cells.

4.1 Programmable Threshold Voltage Defined Gate

TVD logic provides security against reverse engineering, however, the logic function cannot be altered post-production. During manufacturing, the design information needs to be sent to the foundry and the design can be compromised in the supply chain, for example due to untrusted fabrication, obviating the need for later reverse engineering. To combat untrusted fabrication, the critical design information needs to be removed from the design database. This removal can be done by sending a blank or preprogrammed functionality that can be altered post-production. After manufacturing, the chip can be programmed with the desired functionality or even reprogrammed with a different functionality. A further security feature could be the ability to erase the functionality in the field, for example if an attacker's tamper attempt is detected.

By adding a programmable structure at the bottom of the pull-down network, the logic function can be concealed from an untrusted foundry. The structure of a 2-input PMP-TVD gate that is based on a preprogrammed 2-input NAND TVD gate is shown in Figure 4.1. For the

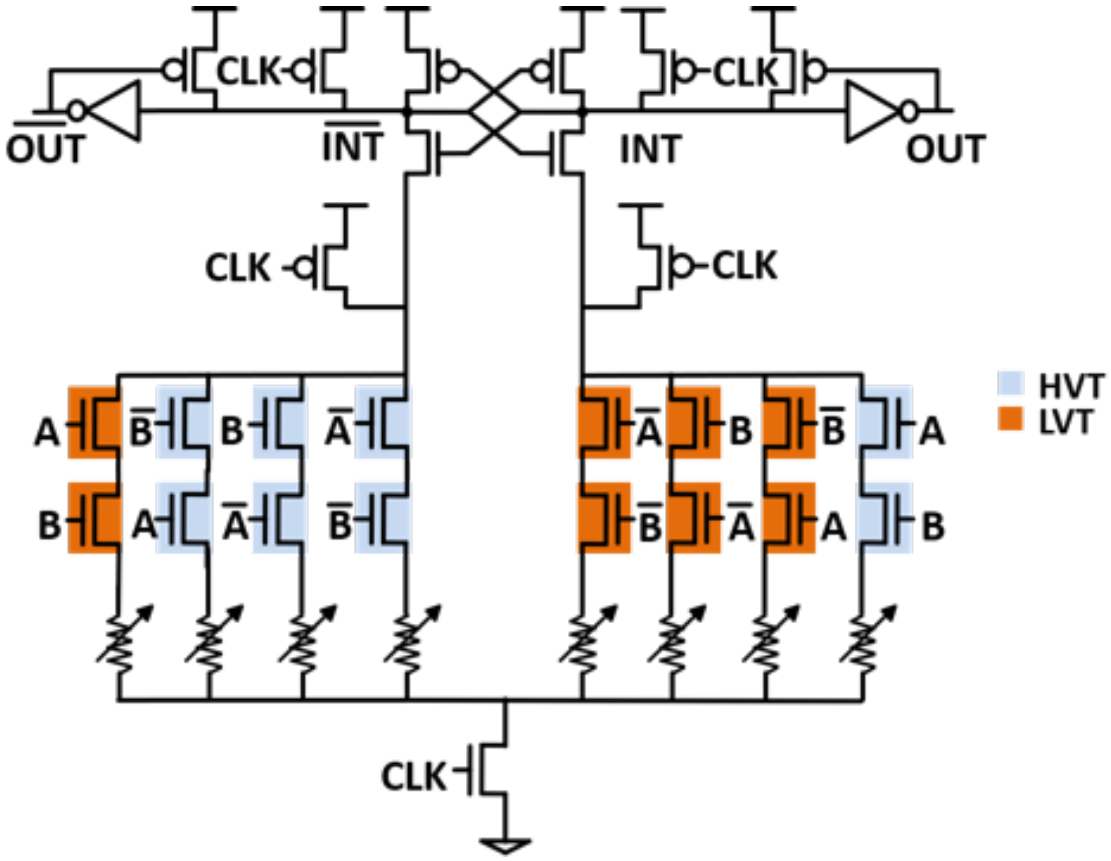


Figure 4.1: Structure of a 2-input Post-Manufacturing Programmable Threshold Voltage Defined (PMP-TVD) logic gate based on a preprogrammed NAND TVD gate. The additional programmable structure at the bottom of the pull-down network gives the ability to alter the functionality post-manufacturing.

programmable structure, low threshold voltage NMOS devices are used. Using hot-carrier injection (HCI), we can set the functionality, change the functionality, or remove the functionality post-manufacturing. For manufacture-time testability, the gates can be preprogrammed with a logic function, and later reprogrammed in the field. In addition, the gates can be manufactured as blank (i.e., without any pre-set logic function).

4.1.1 Hot-Carrier Injection (HCI)

HCI, which is used for in the field programming of the PMP-TVD gates, is a phenomenon by which the threshold voltage of a transistor may be permanently altered post-manufacturing when high energy carriers become trapped in the gate oxide [12][44]. Normally, HCI is an undesired

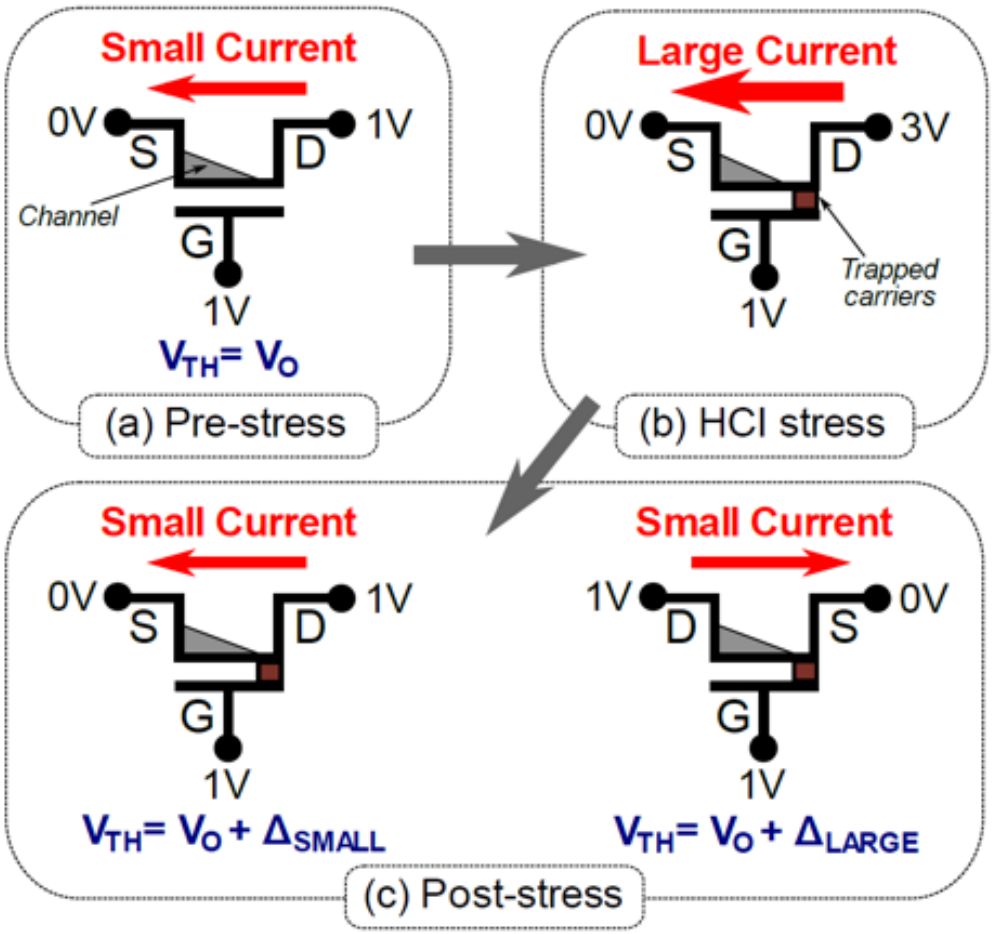


Figure 4.2: (a) Pre-stress NMOS transistor with normal biasing. (b) NMOS transistor under HCI stress conditions. A high V_{DS} generates a large current resulting in some hot electrons getting injected deep into the gate oxide (shown as the brown square). (c) After HCI stress, when the NMOS transistor is biased for normal operation, it sees an increased threshold voltage (Vt). The increase is significant ($> 100mV$) when current is in the opposite direction as during the stress conditions. The increase in Vt, however, is small when current flows is the same direction as during the stress conditions [12][44].

effect where the increase in threshold voltage due to HCI makes the transistors slower, which in turn may affect the reliability of the structures. However, in our proposed PMP-TVD gates, we are using this physical phenomenon in our favor to control the threshold voltage increase in the desired devices.

In Figure 4.2, an overview of HCI phenomenon for an NMOS device is given. In Figure 4.2(a), the NMOS device is under normal bias by applying the nominal VDD over drain-to-source (V_{DS}) and gate-to-source (V_{GS}) of the device. Initially, the device's threshold voltage is assumed

as V_O. With increasing V_{DS} bias, the current passing through the channel increases. As a result of increasing V_{DS} bias, internal electric fields increase and the velocity saturation occurs. With increasing electric fields, the kinetic energy and velocity of the electrons increase, in turn the collisions of electrons increase. These high energy electrons are referred as ”hot carriers”, which can be injected deep into the gate oxide (Figure 4.2(b)). Due to hot carriers trapped in the gate oxide, the transistor requires a higher V_{GS} bias to turn on the device, effectively increasing their threshold voltage. Post-stress, under nominal V_{DS} bias, the device behaves differently depending on the direction of the V_{DS} bias (Figure 4.2(c)). For both of the directions, the device has a post-stress threshold voltage larger than V_O. When the device is biased such that the trapped carriers are closer to the source of the device, the post-stress threshold voltage is much larger than the case where the device is biased such that the trapped carriers are closer to the drain of the device. Since the trapped carriers are deep into the gate oxide, most of this effect is permanent and most of the threshold voltage increase is kept [44].

4.2 PMP-TVD Logic Basic Operation

Figures 4.3, and 4.4 show schematic and layout (in a 28nm CMOS process) of a PMP-TVD NAND gate which is a precharged differential structure with an embedded cross-coupled inverter positive feedback amplifier similar to that used in Sense Amplifier Based Logic (SABL) [40] and Threshold Voltage Defined (TVD) logic [11]. The design of a PMP-TVD gate is explained in detail later in Section 4.3.

The operation of a PMP-TVD gate is similar to a TVD gate. For a 2-input gate, the inputs (A, $\overline{A}$, B, and $\overline{B}$) select one branch on each of the left and right sides of the gate. Depending on the threshold implants on the branches, one side pulls more current compared to the other. Then, this current difference is amplified by the cross-coupled inverters and the amplifier structure locks to one of the output states ($1/0$ or $0/1$).

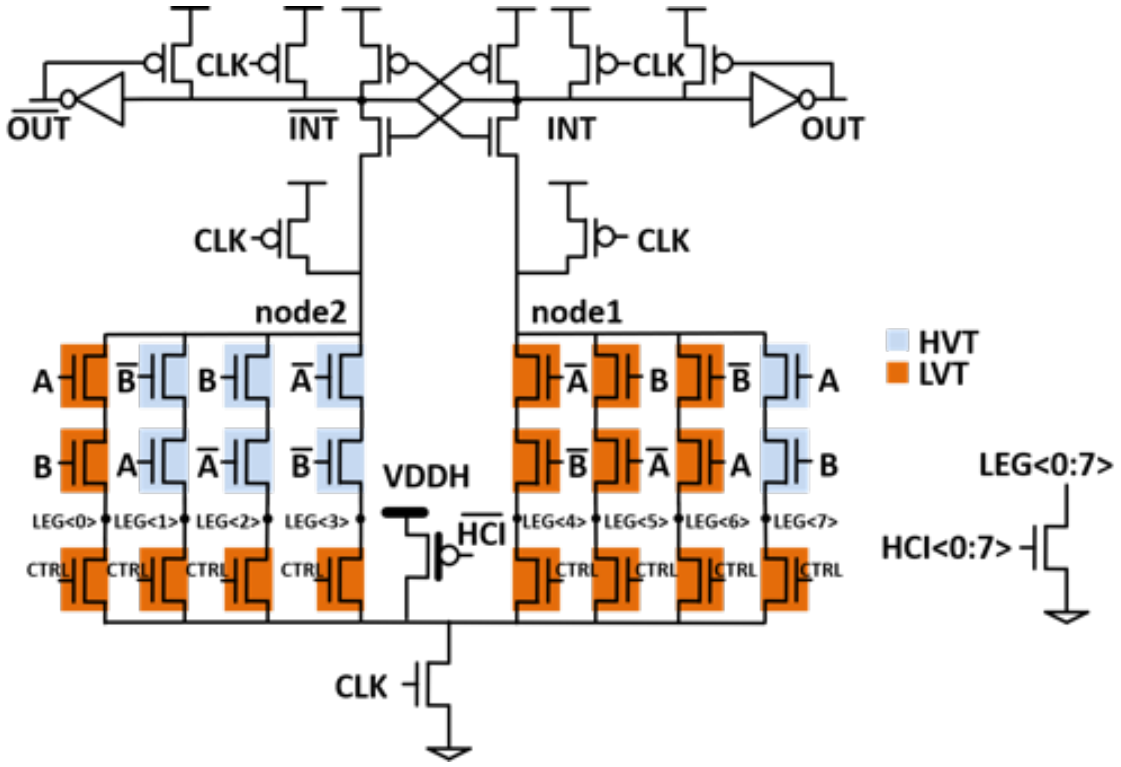


Figure 4.3: Schematic of a 2-input Post-Manufacturing Programmable Threshold Voltage Defined (PMP-TVD) logic gate preprogrammed as a NAND [14]. The stress NMOSes used to program, boost, reverse, or erase the logic function are marked in the blue dashed lines.

Since PMP-TVD gates are TVD based, they can have preprogrammed functionalities after production. However, unlike TVD gates, these functionalities does not have to be one-timed. In PMP-TVD, a logic function can be post-manufacturing programmed into the gates via intentional directed HCI on the final device in the three NMOS stack leg. Therefore, PMP-TVD gates can be also manufactured as ”blank” (i.e., with no manufactured logic function, nominally balanced like a traditional sense amplifier). The preprogrammed gates use a mixture of HVT and LVT devices in the pull-down network to set the logic function and allow for simpler post-manufacturing testing, similar to TVD. Blank gates use all LVT devices in the pull-down network and they must be post-manufacturing HCI programmed before use.

PMP-TVD logic has also two phases, evaluate and precharge, but also it has three mode of operations, HCI stress programming, HCI stress erasing, and normal operation. During HCI

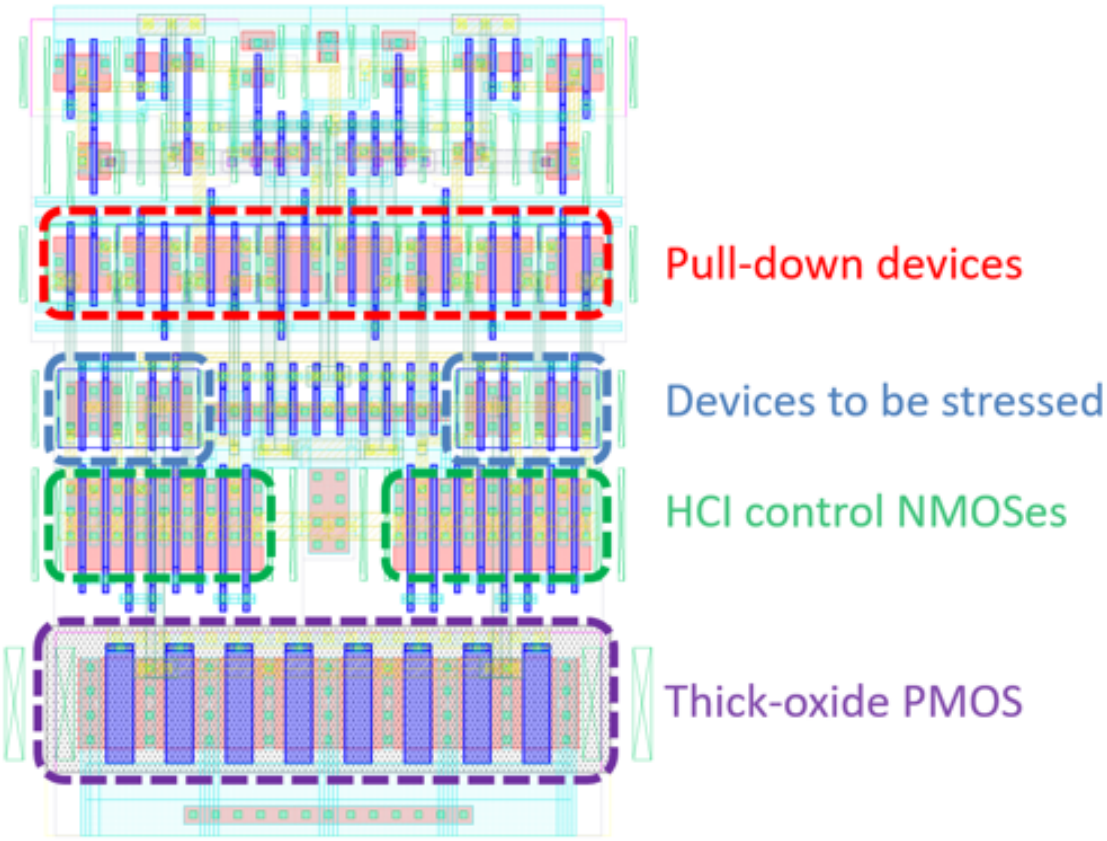


Figure 4.4: Layout of a 2-input Post-Manufacturing Programmable Threshold Voltage Defined (PMP-TVD) logic gate preprogrammed as a NAND in a 28nm CMOS process.The pull-down devices are marked in red dashed lines. The stress NMOSes used to program, boost, reverse, or erase the logic function, HCI control NMOSes, and thick-oxide PMOS are marked in the blue, green, and purple dashed lines, respectively.

programming, all gates are put in reset mode where the *CLK* signal is low, so that all of the gates are in precharge mode and all the differential outputs of the gates are logic-0, turning off all the input pull-down NMOSes. The NMOS devices that are going to be stressed are turned on by controlling the gate signal, *CTRL*. The devices that are going to be stressed need a path to ground, therefore for the desired devices, their bottom stress NMOSes are turned on which are accessed via HCI<0:7> signals. And finally, the center thick-oxide PMOS is turned on ($\overline{\text{HCI}}$=0). To start the HCI stress, the boosted *VDDH* is applied. The selected stress NMOS devices see the HCI stress current and voltage in the opposite direction of the normal operation current flow. This results in maximizing the threshold voltage increase of those NMOSes as discussed in Section

4.1.1. After the desired HCI stress duration has passed, boosted *VDDH* signal is lowered and the HCI stress is completed.

During normal operation, the HCI stress related devices except the stressed NMOSes are turned off. HCI<0:7> signals are set as logic-0 and $\overline{\text{HCI}}$ is set as *VDDH*. The *CTRL* signal is set as same as the nominal VDD. The normal operation of a PMP-TVD gate is similar to TVD gate. During the precharge phase, *CLK* signal is low. This turns on all the precharge devices and the internal nodes are precharged to VDD, and in turn the output nodes are pulled down to VSS. During the evaluate phase, the *CLK* signal goes high. When valid inputs arrive, depending on the functionality the gate evaluates and one of the internal nodes is pulled down to VSS and one of the output nodes is pulled up to VDD.

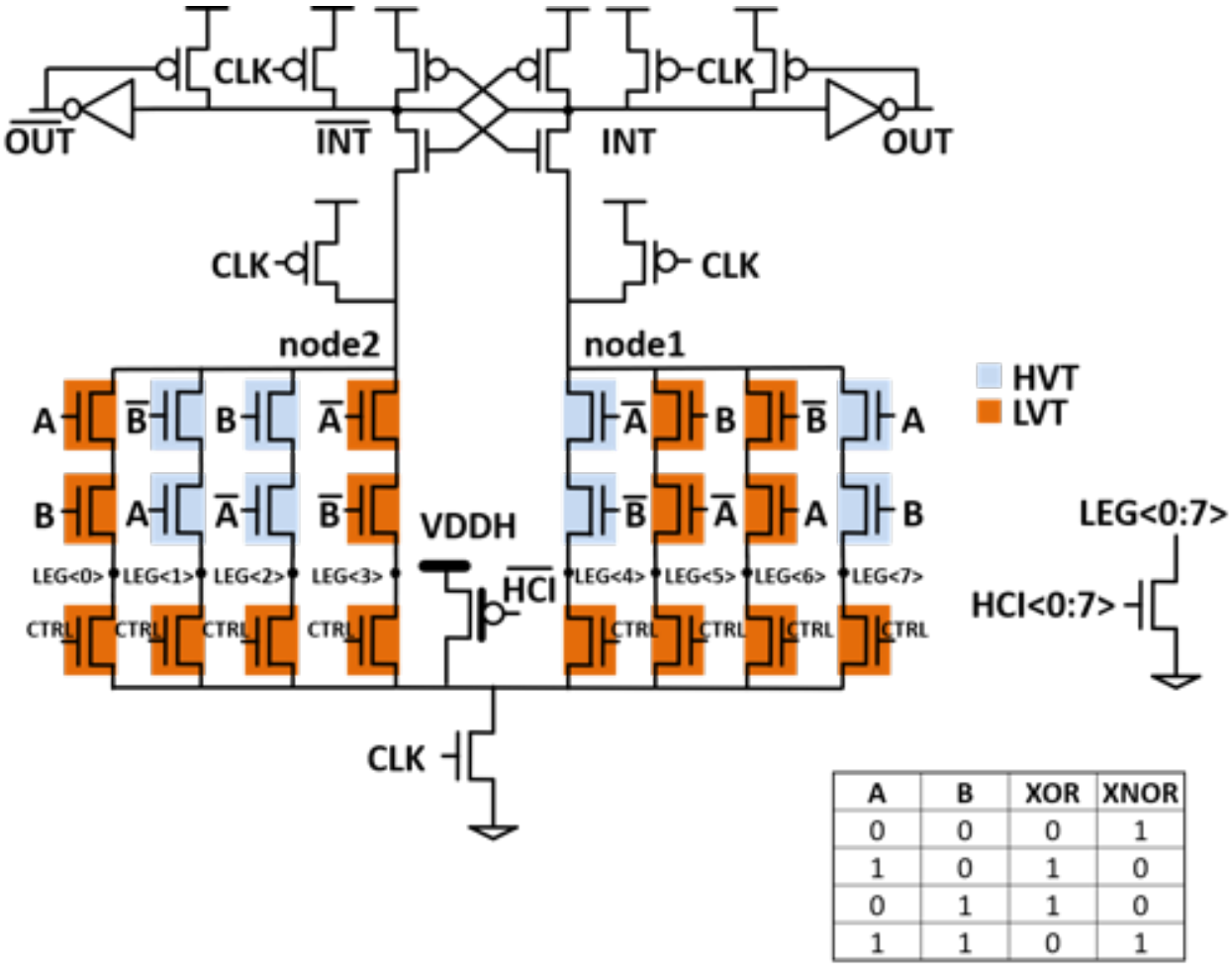
Unlike TVD, since PMP-TVD has programmable devices in them, the output value does not just depend on the preprogrammed devices in the pull-down network but also depends on the stressed NMOSes threshold voltage levels. After HCI stress, the stressed NMOSes will pull less current than their unstressed counterparts on the opposite side. This situation has the following possible effects. If a stressed NMOS is under HVT devices, this means that the current strength of that branch is even more weakened compared to the counterpart branch. Since the counterpart branch will have all LVT devices and an unstressed LVT NMOS, the performance of the gate for that input combination is enhanced. On the other hand, if a stressed NMOS is under LVT devices, the current strength of that branch will start to reduce and after some point, the other branch with HVT devices and an unstressed LVT NMOS will have a higher current pull. This means, for that input combination, the output value will be flipped after the HCI stress, hence the functionality of the gate is changed. Thus, using the HCI stress, a a blank gate can be programmed, a preprogrammed gate can be over-written (different logic function programmed in) or boosted for higher performance (reinforce preprogrammed function), or a gate function can be replaced (e.g., for an erase on tamper detection security feature).

In addition to changing the functionality of a gate by programming a different functionality, if the effects of HCI stress is removed, another functionality can be programmed in [45][46][47]. There have been studies trying to reverse the effects of HCI by trying to remove the trapped charges from the gate oxide. To achieve this, we can apply a zero or negative V_{GS} bias over the stressed NMOS while applying the high HCI voltage over the V_{DS}. According to Khan et al., this requires a higher HCI stress voltage, however even with the same HCI stress voltage some of the trapped charges can be removed [46][47]. To remove the trapped charges, all the devices are set just like HCI programming, except the *CTRL* signal is set as VSS (if the design and technology allows, a bias lower than VSS is preferred). Then the HCI stress is applied for a certain amount of time. After the HCI erasing, the gates should be back in their original programming, however due to some remaining trapped charges, the performance of the gate is expected to have a small decrease.

4.2.1 Example: A 2-input PMP-TVD XOR Gate and HCI Programming

A preprogrammed 2-input PMP-TVD XOR gate and its truth table is shown in Figure 4.5. Similar to the 2-input TVD XOR gate shown in the previous chapter, the pull-down network is preprogrammed with LVT and HVT threshold implants so that the output will be logic-1 when the inputs are different, and logic-0 otherwise. The additional NMOSes on the pull-down network does not affect the functionality of the gate pre-stress. The timing diagram of the 2-input PMP-TVD XOR gate is shown in Figure 4.6. In the figure, two operation cycles are shown. Each cycle has two phases, precharge and evaluate. In the diagram, the inputs transitions from $0/0$ to $0/1$, and from $0/0$ to $1/1$ are shown for A/B.

In the precharge phase *CLK* is low, thus, *INT* and $\overline{INT}$ are precharged to VDD. When *CLK* goes high, the gate starts its evaluate phase. For the input combination $A/B = 0/1$ ($\overline{A}/\overline{B} = 1/0$), more current flows through *node1* branch because of the LVT transistors in the stack. Therefore,



A	B	XOR	XNOR
0	0	0	1
1	0	1	0
0	1	1	0
1	1	0	1

Figure 4.5: 2-input preprogrammed PMP-TVD XOR gate. Transistors with LVT threshold implants are shown in orange, and HVT transistors are shown in blue. Truth table of XOR gate is also shown.

INT goes low rapidly, while $\overline{INT}$ makes a small dip and then remains high. Since, *INT* is pulled down to VSS, *OUT* goes high, and $\overline{OUT}$ remains low. On the other hand, for input combination $A/B = 1/1$ ($\overline{A}/\overline{B} = 0/0$), this time more current flows through *node2* branch and $\overline{INT}$ goes low rapidly, as *INT* makes a small dip and remains high. Since, $\overline{INT}$ is pulled down to VSS, $\overline{OUT}$ goes high, and *OUT* remains low. After each evaluate phase, during the precharge phases, internal nodes *INT* and $\overline{INT}$ are charged to VDD. This effectively pulls output nodes *OUT* and $\overline{OUT}$ down to VSS. Since the inputs to the gate are the outputs of other TVD gates, the inputs $A/\overline{A}$ and $B/\overline{B}$ are $0/0$ as well.

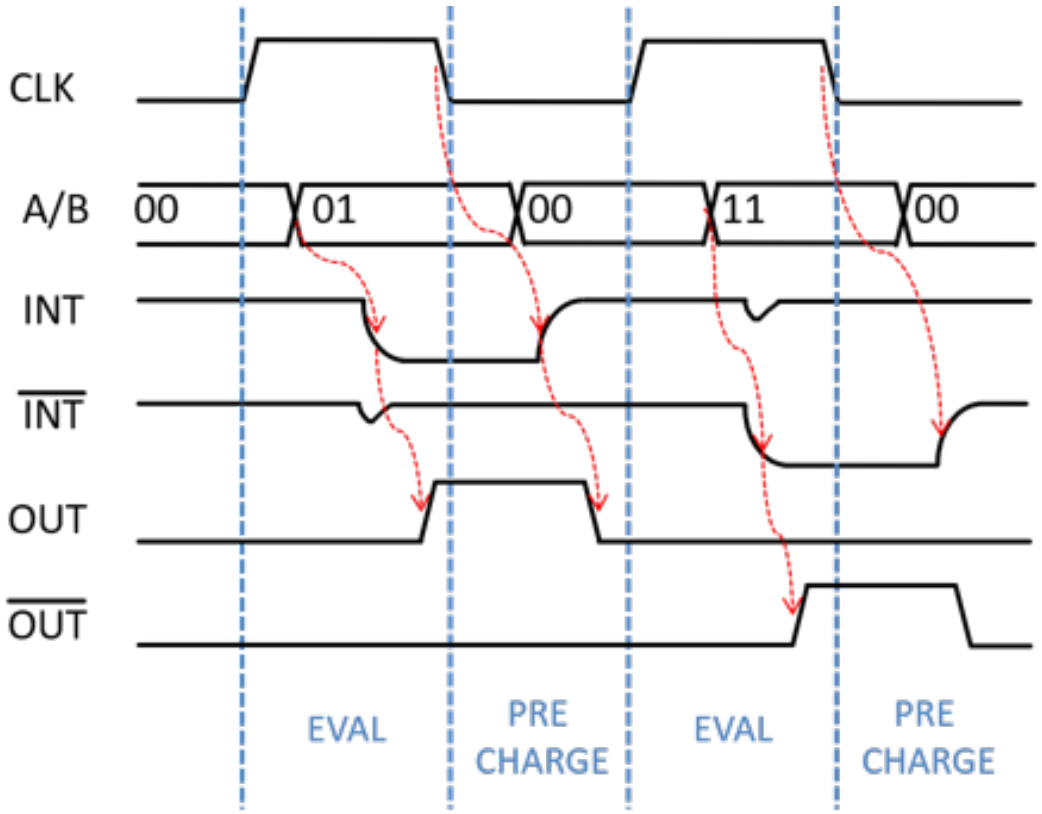
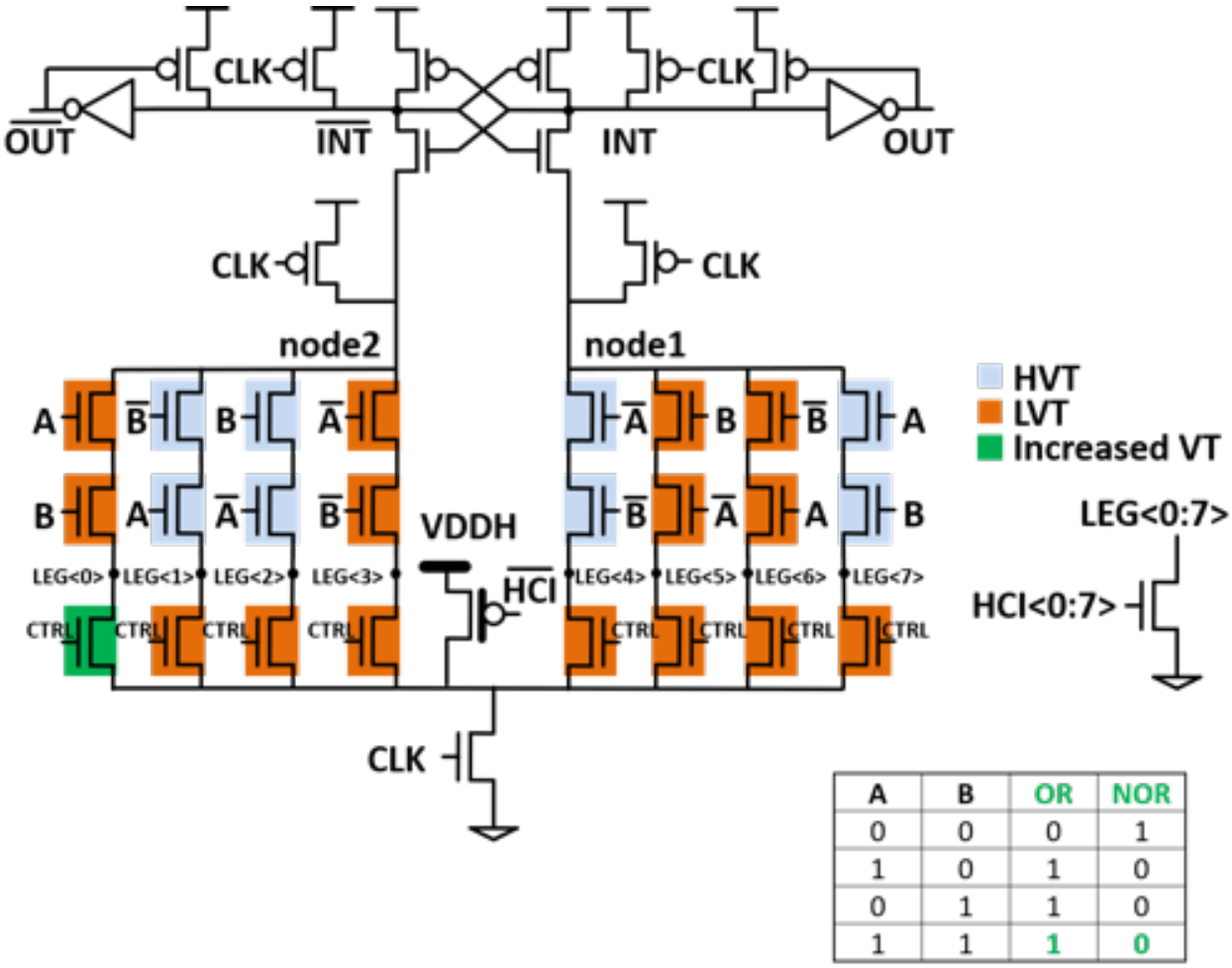


Figure 4.6: Timing diagram of a preprogrammed 2-input PMP-TVD XOR gate for the input transitions of 00 to 01 and 00 to 11.

The preprogrammed 2-input PMP-TVD XOR gate operates similar to the fixed 2-input TVD gate. However using HCI stress, the functionality of the PMP-TVD gate can be altered post-production. For example, if HCI stress is applied to the NMOS device on the most left branch, the new functionality of the gate will be an OR gate. As shown in Figure 4.7, the gate can be manufactured as a preprogrammed 2-input XOR gate. After a single HCI stress, the output value can be altered for the input combination $A/B = 1/1$. This will effectively make the gate operate as an OR gate. In addition to this method, a blank PMP-TVD gate can be manufactured and then later can be HCI stressed to operate as an OR gate as well. Figure 4.8 shows a 2-input blank PMP-TVD gate programmed into an OR gate by applying HCI stress to the required devices.

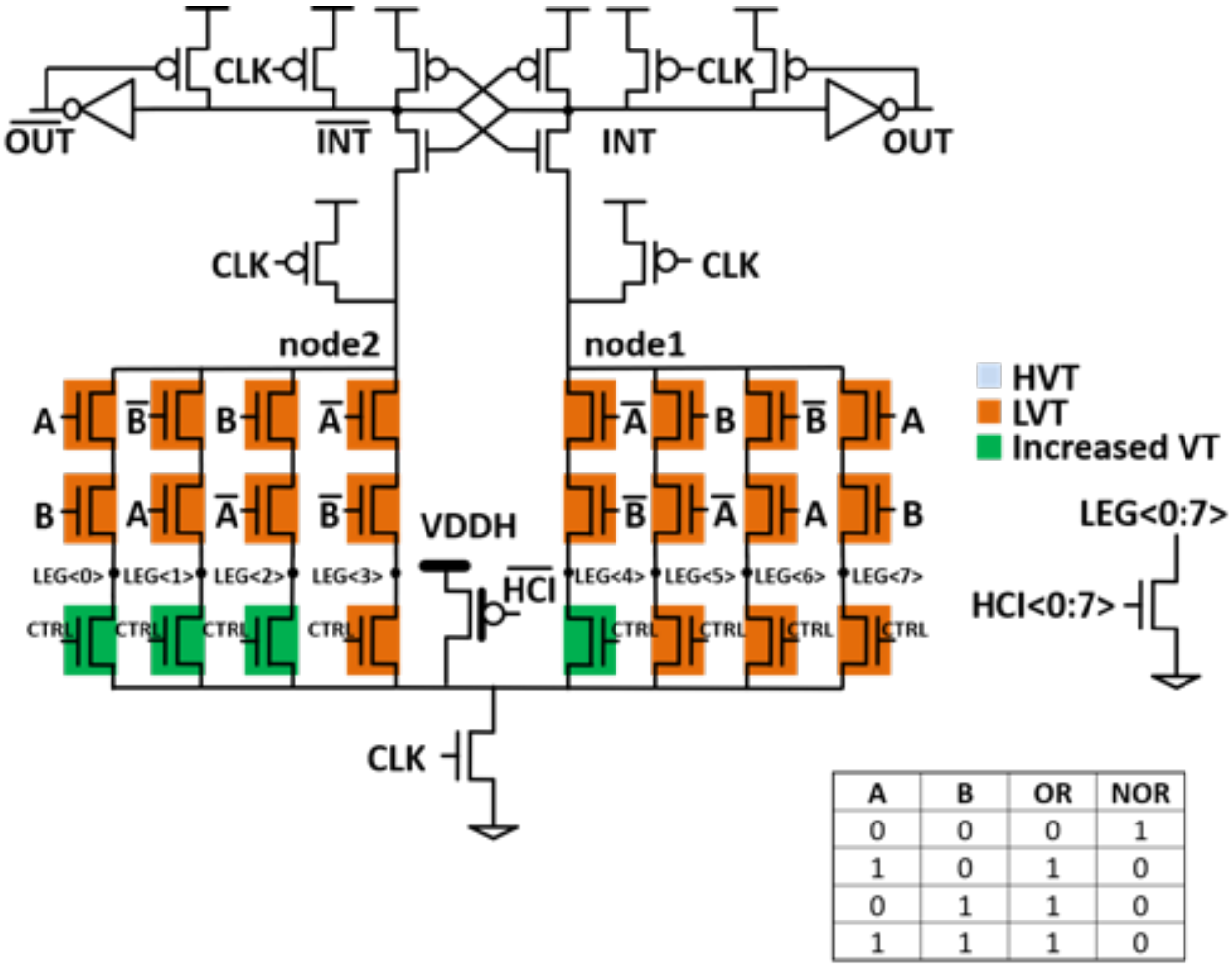


A	B	OR	NOR
0	0	0	1
1	0	1	0
0	1	1	0
1	1	1	0

Figure 4.7: 2-input preprogrammed PMP-TVD XOR gate after HCI stress to function as an OR gate. Transistors with LVT threshold implants are shown in orange, HVT transistors are shown in blue, and the increased threshold voltage devices using HCI stress are shown in green. Truth table of the new function is also shown.

4.3 PMP-TVD Gate Design

The sizing of a PMP-TVD gate depends on the trade-off between area, performance, and power of the gate, but on top of that, the HCI stress requirements affect its size as well. A PMP-TVD gate can be partitioned into the stress devices, pull-down network, and sense amplifier parts. In the stress devices, there are the stressed NMOS devices on each pull-down leg, the thick-oxide PMOS device which supplies the high HCI voltage and large HCI current, and the bottom NMOS devices which creates the ground path during the HCI stress. Pull-down network consists



A	B	OR	NOR
0	0	0	1
1	0	1	0
0	1	1	0
1	1	1	0

Figure 4.8: 2-input blank PMP-TVD gate after HCI stress to function as an OR gate. Transistors with LVT threshold implants are shown in orange, HVT transistors are shown in blue, and the increased threshold voltage devices using HCI stress are shown in green. Truth table of the new function is also shown.

of the legs with stacked NMOS devices which define the functionality of the gate. And rest of the devices, the bottom clock NMOS, cross-coupled inverters, precharge PMOSes, and output inverters, can be grouped as the sense amplifier parts. Each of these defined devices can be seen highlighted in Figure 4.9.

The design of the stress devices depends on the amount of threshold voltage shift required and the desired time amount to achieve the shift. These two variables determines the required size of the stress devices, HCI stress voltage, and HCI stress current. Detailed HCI models or empirical silicon tests are required to decide these parameters. In the next section, we have

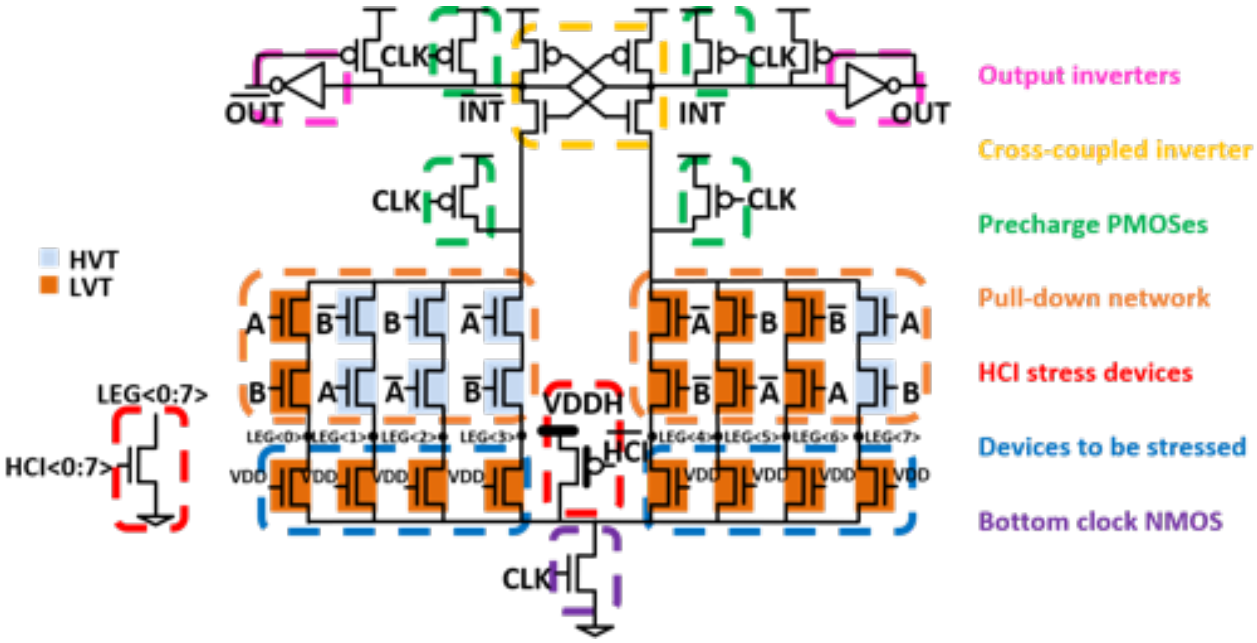


Figure 4.9: Highlighted sections of a 2-input PMP-TVD gate are shown: Output inverters (pink), cross-coupled inverter (yellow), precharge PMOSes (green), pull-down network (orange), HCI stress devices (red), devices to be stressed (blue), and bottom clock NMOS (purple).

introduced a structure to obtain data on the characterization of HCI and we have reported the results in Chapter 5. The sizing of the stressed NMOS device (and consequently the other stress devices) does not solely rely on the HCI parameters. Since the stressed NMOS device is in the NMOS series of the pull-down network, the performance of the gate is affected by its size. The width of the stressed NMOS should be on the small end for a better HCI stress control [1][14][2]. However, a small device on a large stack will decrease the performance of the gate. Therefore, a middle ground needs to be found for the sizing of the stressed NMOS gate, where the width is small enough for better HCI stress conditions, but also large enough to have a decent delay performance in the gate. After choosing the size of the stressed NMOS device, rest of the stress devices can be determined according to the HCI stress voltage and current values.

Once the stress devices are sized, the rest of the circuit can be sized with a trade-off in performance, area, and power. Since there are a stack of $n+3$ NMOSes in an n-input PMP-TVD gate, larger NMOSes should be preferred in the pull-down network. However, the pull-down

network should be also sized so that the capacitance of the internal nodes are not too large and the input capacitance is low enough that it can be driven by the previous gates.

The rest of the devices should be sized so that they have the desired efficiency in the performance/area/power trade-off. The bottom clock NMOS device should be sized so that it does not become the bottleneck in the pull-down network, but not too large so that is does not overload the clocking network. The precharge PMOSes can be sized minimum. The cross-coupled invertesr and the output inverters of the sense amplifier part can be sized in a skewed fashion. For the cross-coupled inverters, since the NMOSes are on the critical path of the gate, they can be sized larger than the PMOSes. For the output inverters, the critical output transition is from logic-0 to logic-1. Therefore, the PMOSes of the output inverters can be sized much larger than the NMOSes of the output inverters.

The layouts of 2-input PMP-TVD gates in 65nm and 28nm CMOS processes are shown in Figure 4.10 side by side. The dimensions of a PMP-TVD gate depend on factors such as the dimensions of the thick-oxide PMOS device, number of devices that can fit next to each other, the ratio of PMOS devices to NMOS devices, and the design rules of the technology node. Since PMP-TVD is a sense amplifier based design, the layout of the gate should be as symmetrical as possible to reduce the layout dependent effects. Therefore, the width of the gate is determined by either the size of the thick-oxide PMOS gate, the total width of the pull-down network devices put next to each other, or the width of the cross-coupled inverter and the output inverters put next to each other. Out of these three parts, the widest one determines the width of the gate. In the 65nm CMOS process, we can take advantage of routing the poly in any direction, but in the 28nm CMOS process, the poly needs to be unidirectional. Moreover, in 28nm CMOS process, the poly is required to be in an array with a pre-set separation from the other poly. Hence, the additional design rules in the scaling technologies reduce the efficiency in designing the custom layout of the PMP-TVD gates.

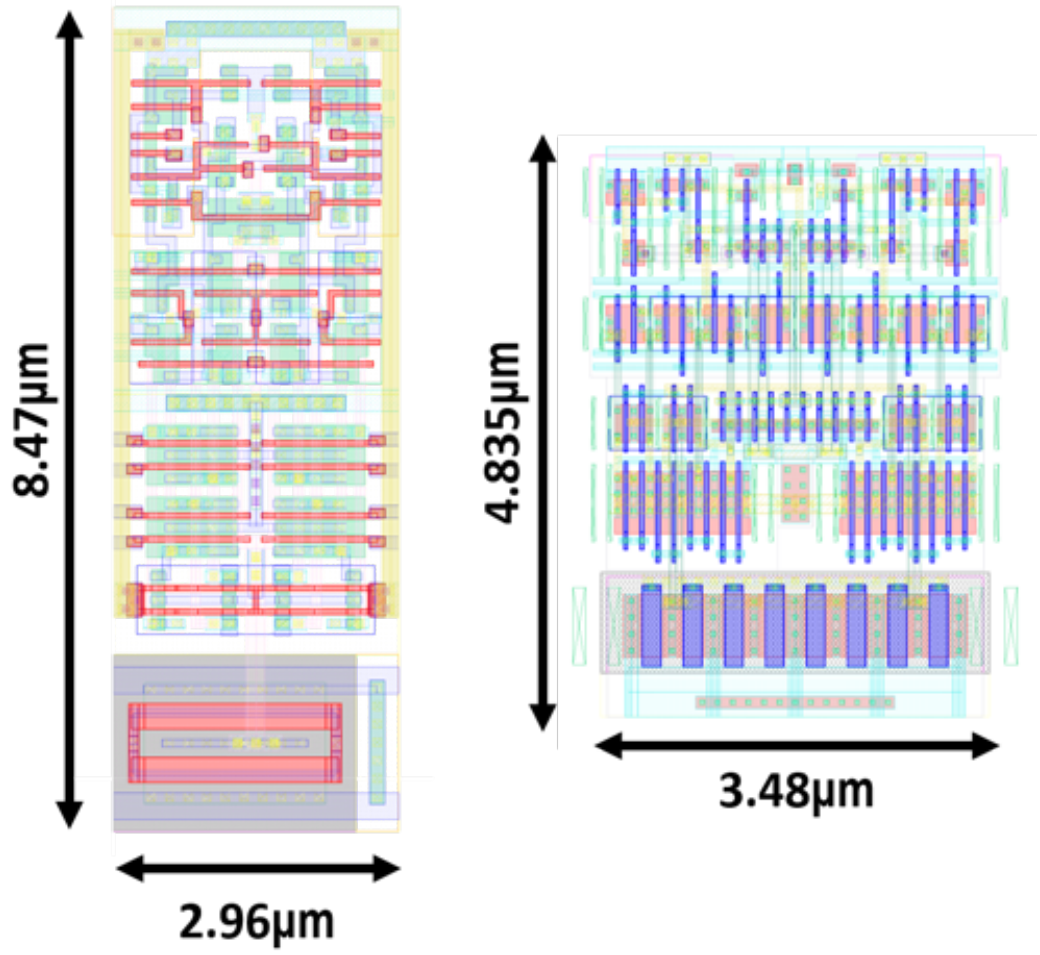


Figure 4.10: Layout views of a 2-input PMP-TVD gate in 65nm and 28nm CMOS processes.

So far, the sizing of the transistors are done with a trade-off in performance, area, and power. However, depending on the application, a metric can be favored more than the others. For a better area efficiency, a PMP-TVD gate library can be designed with smaller sized pull-down network and HCI stress devices. The area of the gate would be smaller than the proposed design, however this in turn increases the delay and the programming time of the gate. On the other hand, if a smaller programming time is required, the HCI stress devices can be designed larger, which will increase the area of the gate. In addition, different sized pull-down networks will yield gates with varying performances. Creating all these kind of different types of PMP-TVD gates will give a designer the ability to choose specific types or a combination of types of gates tailored for their

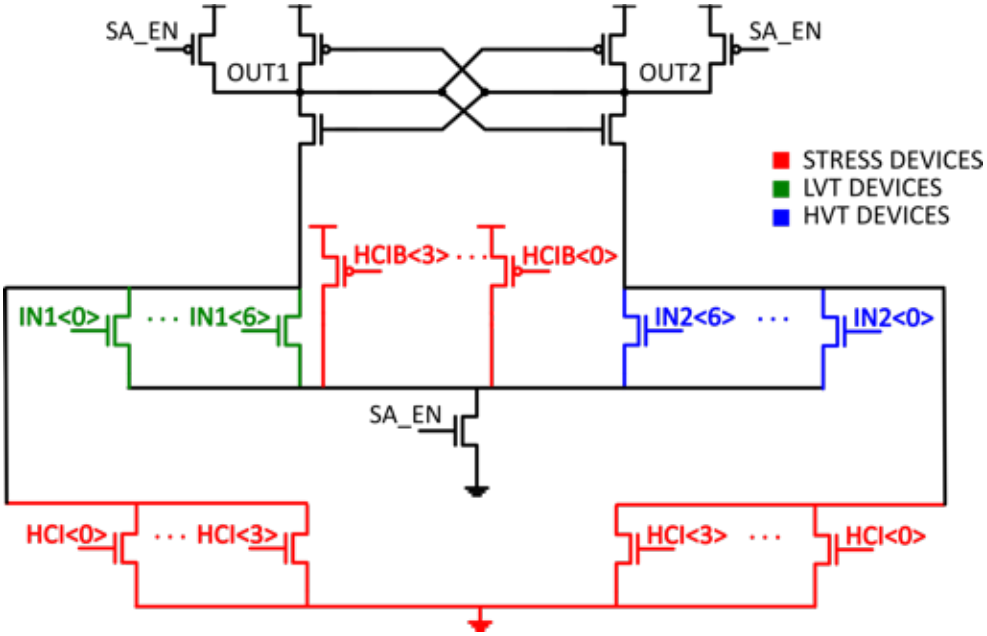
intended design.

4.4 Characterization of Hot-Carrier Injection

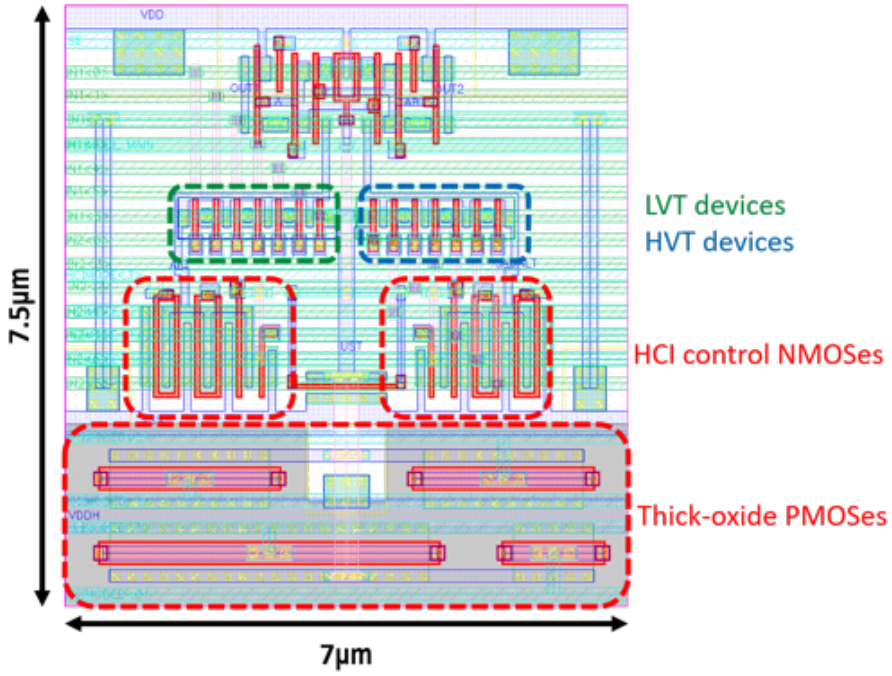
The programming time and and the shift in threshold voltage using HCI depends on many variables such as the initial HCI stress current and voltage that is applied over the stressed NMOS device, and the dimensions of the stressed NMOS device, hence the current density over it. In PMP-TVD gates, we can control or change some of these variables to achieve the required threshold voltage shift and the required programming time. In order to characterize the effects of these variables, we have designed a structure where we can alter the variables and measure the shift in threshold voltage and the time required to achieve that shift.

4.4.1 Binary Aging Element (BAE)

The schematic and the layout of a modular binary aging element (BAE) in a 65nm CMOS process is shown in Figure 4.11. The core of the BAE is similar to a sense amplifier, but the structure is intentionally designed to be unbalanced in the pull-down network. This asymmetry can be obtained in several ways. Width of *IN1* NMOSes can be greater than the width of *IN2* NMOSes, the threshold voltage of *IN1* NMOSes can be set lower than *IN2* NMOSes by making the *IN1* devices *LVT* and the *IN2* devices *HVT*, or both of these methods can be combined. To get the maximum difference in a single comparison, the proposed BAE is set to have *LVT IN1* and *HVT IN2* devices. Just like the PMP-TVD gates, BAE design also has the HCI stress structures. Thick-oxide PMOSes are used to apply the high stress voltage over the drain-source of the stressed NMOSes. The NMOSes at the bottom of the schematic are used to create the ground path during the HCI stress. For modularity, each side has seven comparison devices. In addition, there are four NMOSes that creates the path to ground during HCI stress on each side and four thick-oxide



(a)



(b)

Figure 4.11: (a) Schematic and (b) layout of a modular binary aging element (BAE) using HCI phenomenon in a 65nm CMOS process. The dimensions of the modular BAE is 7.5μm by 7μm. The sense amplifier design has modular elements on each side for multiple comparison points. The LVT and HVT comparison legs are highlighted in green and blue, respectively. The thick-oxide PMOSes and HCI control NMOSes that are used for the application of HCI stress are highlighted in red.

PMOSes which are used to apply the HCI stress. This way, depending on the configuration, different sized NMOSes under varying HCI stress and current can be compared [1][2].

As can be seen in Figure 4.11, BAEs have seven legs on each side of the inputs. Each leg has an NMOS with a width of 200nm and length of 60nm. The biased input side has *LVT* devices and the comparison side has *HVT* devices. This way HCI stress can be applied on devices with a width ranging from 200nm to 1.4μm. In addition to the input legs, the stress devices area also modular. In total there are four bottom NMOSes and four thick-oxide PMOSes with different sizes to control the current and voltage drop each legs see. Therefore, each modular BAE can be stressed with currents ranging from 40μA to 1.3mA at a 2.5V HCI stress voltage.

As mentioned before, the structure of a BAE is intentionally designed to be unbalanced in the pull-down network. Therefore, before any HCI stress is applied, when the output is sensed it will be biased and BAE will always give the same output. Before stressing the *LVT* devices, the asymmetry forces *OUT1* to be logic-0. Then, with the desired configuration and for select *IN1* NMOSes, HCI stress is applied for a certain time. HCI stress on *IN1* NMOSes increases their V_{TH} and after sometime V_{TH} of *IN1* NMOSes will increase to a point where *OUT1* will flip and become logic-1 when sensed. In this way, the BAE can measure the time that is required to increase a certain device's threshold voltage a certain amount based on HCI stress. In our modular BAE design, the width of *IN1* and *IN2*, and selection of the stress devices can be varied in order to set the threshold voltage increment and the time required to achieve that increment.

For an easier characterization, we designed a modular and self-sufficient system BAE with the capability of self-sensing when the output value flips [1][2]. Figure 4.12 shows the structure of a modular system BAE. These system BAEs can be configured in a chain. In the chain, each system BAE checks the output of the previous one and the output of itself. If the previous BAE's output has flipped and its output has not flipped, the system BAE starts the HCI stress on itself. On the other hand, if the previous BAE's output has not flipped or its output has flipped, then the

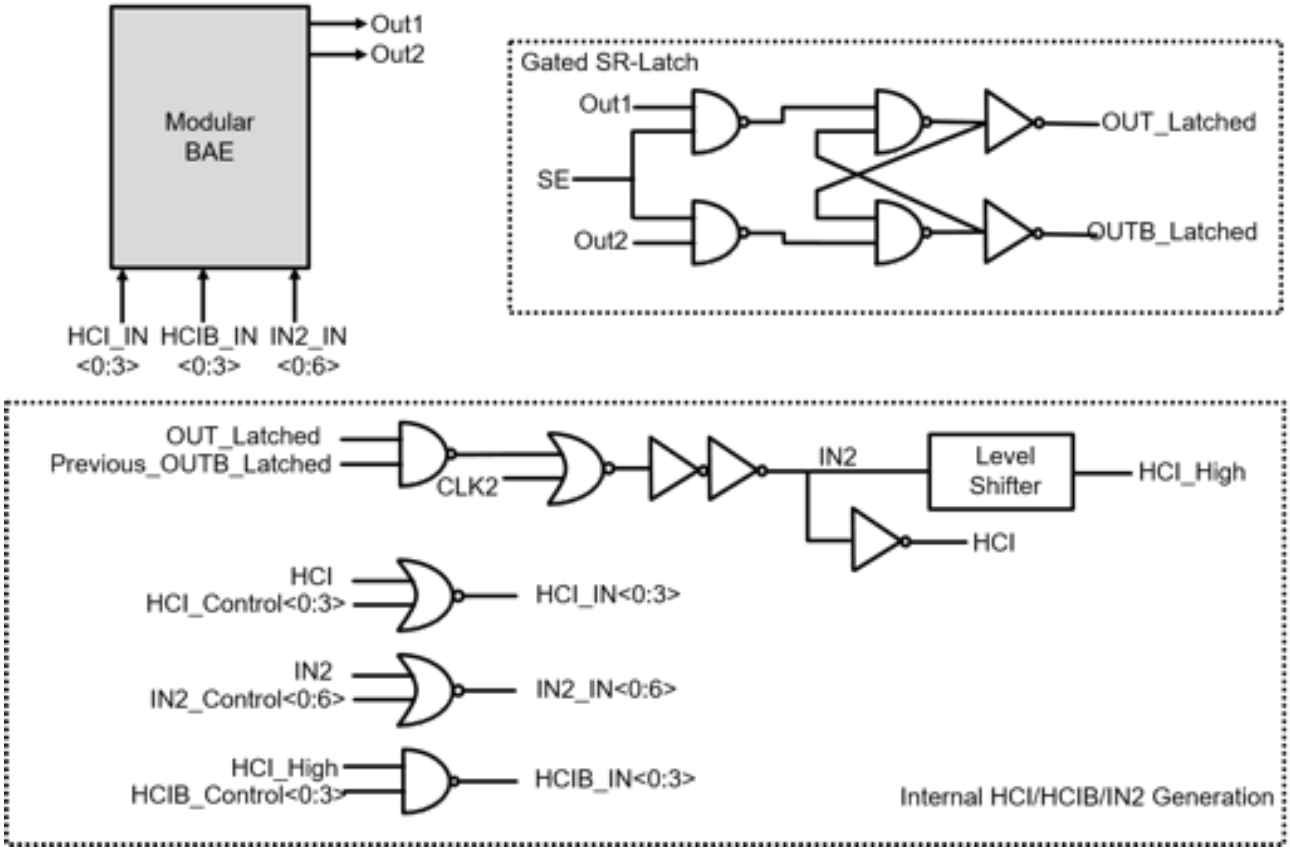


Figure 4.12: Structure of a modular system BAE. The modular system BAE consists of a modular BAE and the additional structure to self-sufficiently sense the output flip [1][2].

system BAE does not apply any HCI stress.

Use Case for Binary Aging Elements

Other than HCI characterization, binary aging elements can be also used for other purposes. Since a BAE can change the threshold voltage of a transistor in a certain time, it can be used to measure time or age in an IC. Time or age measurement in IC has been proposed by introducing structures as *Chip Odometers*. However, the proposed methods mostly use physical phenomena which are relatively easily reversible. Using a chain of system BAEs, time or age measurement in an IC can be done in a more robust fashion. By combining the BAEs as can be seen in Figure 4.13, a thermometer coded output of time or age of an IC can be obtained. For the desired

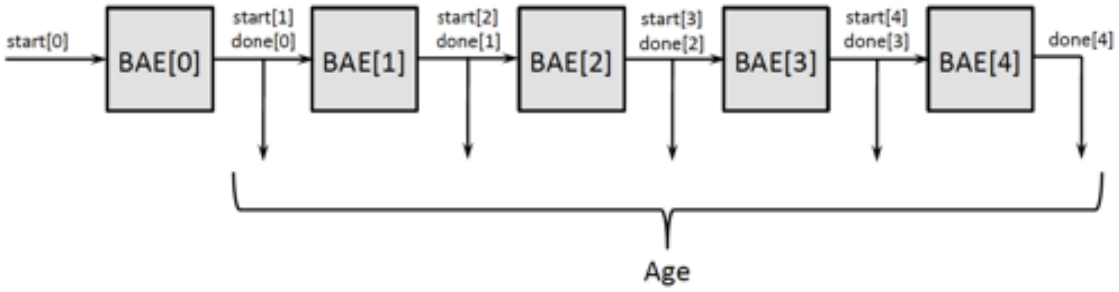


Figure 4.13: Chip odometer block diagram showing chained system binary aging elements (BAE). Each BAE is a one-shot, non-resettable unit that begins operation on assertion of *start* and asserts *done* after a known, fixed amount of time [1][2].

measurement intervals, the BAEs in the chain can be configured differently so that they will flip after different time intervals. In addition, multiple chains with different configurations can be used to measure varying time resolutions.

Combining this chain of system BAEs with other security related structures can eliminate unauthorized access to the time measurement and in addition, can provide IC authentication. Adding security related structures such as hardware encryption blocks with a physical unclonable function generated keys, a *Secure Chip Odometer* can be implemented [1][2]. An example secure chip odometer block diagram can be seen in Figure 4.14. The chain of BAEs are combined with a true random number generator and the output is fed into an encryption block using PUFs to generate encryption keys. This structure enables the secure identification and authentication of a chip, on top of the ability of measuring time or age of the IC.

4.5 Security of PMP-TVD

Hardware obfuscation methods have several different properties to thwart reverse engineering threats. Therefore, there are different security metrics to evaluate these hardware obfuscation methods. In addition, the topology of the obfuscation method can alter the required security

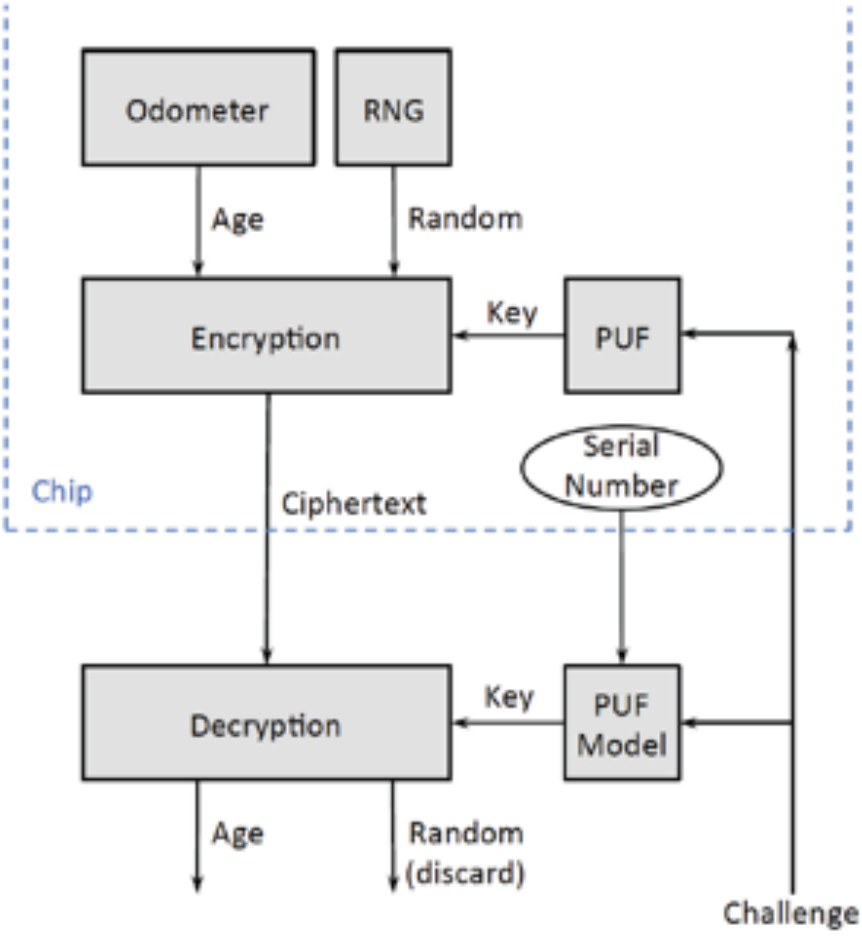


Figure 4.14: Example secure chip odometer block diagram. Our proposed odometer design is combined with a true random number generator and the output is fed into an encryption block using PUFs to generate the encryption keys. The structure enables the secure identification/authentication of a chip [1][2].

metric.

4.5.1 Security Metrics

Researchers have proposed many different security metrics. For example, the dummy via structure's security is evaluated by measuring the correlation between the inputs and outputs after some of the selected gates in a design are replaced with dummy via gates [25]. During the security evaluation of dummy via gates, two principles that form the foundations in VLSI testing in ICs are utilized: justification and sensitization [25][48][49]. In a different method presented by Chakraborty et al., a new metric is derived to quantify the level of obfuscation [17], where the security of the design is evaluated by quantifying the mismatch between the original and the obfuscated design, i.e., the higher the mismatch the more obfuscated the design is.

Alternatively, to evaluate the security of obfuscated designs such as keyed logic, measuring the required number of test patterns to determine the keys inserted in the original design is used [50]. In keyed logic, additional gates are inserted into the design to hide the functionality and the implementation. In order for the altered design to operate correctly, a valid key has to be supplied to the additional gates. The number of required test patterns exponentially increases with the number of keys inserted in the design.

We can follow this approach to evaluate the security of PMP-TVD. For an n-input PMP-TVD gate, the gate can realize all the possible 2^{2^n} functionalities, which requires all the possible input vectors to find the functionality of the gate. However, in keyed logic, some of the test vectors can be eliminated by looking at the design tools. In a regular design database, only certain types of logic gates are used (such as NAND, OR, AOI etc.). Therefore, for an n-input standard cell gate that is keyed, the required test vectors to figure out the obfuscated functionality is reduced since the search domain is limited by the defined functionalities of the standard cells.

Another important security feature of PMP-TVD is that the secret key (i.e., the functionality

of the gates) are already distributed to the gates and are embedded, which remove the need of having a secure key storage and a static key input. However, in the keyed logic, the secret key is centralized and the key inputs need to be constantly available throughout the IC operation. Therefore, even if key storage is secure by having a tamper-proof or read-proof memory, the static nature of the secret key invalidates the benefits of secure key storage [51].

4.5.2 De-camouflaging

The logic, the interconnect or both of them can be camouflaged in hardware obfuscation. Most of the proposed methods only camouflage the logic in the design, whereas methods like split manufacturing camouflages only the interconnect [52]. On the other hand, obfuscation methods that use FPGAs or LUT-entangled schemes [53] hide both the logic and interconnect design information. In PMP-TVD logic, only the logic gate functionalities are hidden. Although PMP TVD gates are designed to implement logic gate level obfuscation, interconnect obfuscation can be easily realized at a small cost by either programming PMP-TVD as 2:1 or 3:1 MUXes or increasing the size of the PMP-TVD gates and connecting an unrelated net in the circuit to the additional input. As mentioned before, an n-input PMP-TVD gate can realize 2^{2^n} possible functionalities, and a brute force attack on just one gate requires 2^{2^n} possible test vectors to de-camouflage the logic function of the gate.

To narrow down the search domain, several attack methods were proposed. Among the proposed methods, Satisfiability-based (SAT-based) method is the most efficient [21]. Later, improved versions of SAT attacks are proposed to decrease the computational effort for the attack (such as incremental SAT attack [54]). To overcome SAT-based attacks, numerous SAT-resilient camouflaging methods have been proposed. However, many of those techniques are vulnerable against other type of reverse engineering attacks [55]. Therefore, some of the obfuscation methods [27][56][57][58][59][60][61][62] focus on using key programmable logic similar to LUTs

to achieve protection against the reverse engineering attacks.

Kolhe et al. analyzed LUT-based obfuscation against SAT-based attacks and explored obfuscation for different replacement strategies, LUT size, and number of LUTs [55]. The comparison showed that with increasing percentage of camouflaging using LUTs, the resiliency against SAT attacks increase. After a certain point, the SAT attacks time-out. This time-out point depends on the structure that is obfuscated. For a DES implementation using only 2-input LUTs, the time-out for the SAT attack is reached with camouflaging only 35% of the gates [55]. Another key outcome is by using LUTs with higher number of inputs, same SAT resiliency can be achieved with a smaller camouflaging percentage compared to camouflaging with LUTs that have lower number of inputs. However, the overhead of the obfuscated structure increases with increasing number of inputs in a LUT that is used for camouflaging. In their analysis, they show that twice the number of 4-input LUTs are required if 3-input LUTs are used (or thrice the number of 4-input LUTs are required if 2-input LUTs are used) for the same SAT execution time on a synthesized ISCAS85 c7552 benchmark [55]. Therefore, a trade-off between number of inputs in a LUT and camouflaging percentage should be chosen to achieve SAT resiliency while having feasible overheads. Since n-input PMP-TVD gates can function as n-input LUTs, camouflaging a structure using PMP-TVD gates will achieve a similar resiliency as camouflaging with LUTs.

Moreover, researchers have proposed various selection algorithms for camouflaging a design to keep the overhead at a reasonable level while ensuring the security against reverse engineering attacks. PMP-TVD logic is simply another style of gate camouflaging, therefore, those algorithms can be used with PMP-TVD logic style, as the use of PMP-TVD logic gates is orthogonal to those lines of research.

4.5.3 Untrusted Fabrication

As mentioned before, protection against reverse engineering is effective if the supply chain of the production is secure. Supply chain threats such as untrusted fabrication obviates the need for later reverse engineering in the field, because the secret design information can be compromised during the manufacturing step. Therefore, the critical design information needs to be removed or hidden when it is sent to the foundry for production. A configurable or reprogrammable structure can be used so that the design information which is sent to the foundry can be overwritten with the secret design information post-production. PMP-TVD logic uses HCI stress post-manufacturing to either enhance, erase, or alter the preprogrammed functionality or program a new functionality into the blank structures. Moreover, the functionalities that are written with HCI stress can be removed by reversing the effects of HCI with a built-in mechanism in PMP-TVD gates. This makes PMP-TVD a reprogrammable structure. Using these properties of PMP-TVD gates, the critical design information can be removed from the design database and either a blank structure or a preprogrammed and easily testable structure can be manufactured. Later in the field, the desired functionalities can be programmed, and even erased for example if an attacker's tamper attempt is detected.

4.5.4 Side-channel Leakage

PMP-TVD gates also have low side-channel leakage due to their symmetrical and differential structure. The logic style has reduced inadvertent power and timing information leakage, since PMP-TVD gates with same number of inputs have similar delay and power consumption values. Moreover, PMP-TVD logic can be easily modified to have the power-analysis resilient properties of dynamic dpa-resistant logic families such as Self-timed Three-phase Dual-rail Pre-charge (ST-TDPL) logic family [41] since both of the structures are based on Sense Amplifier Based Logic (SABL) [40] and they are differential dynamic structures.

4.5.5 Security Comparison

Table 4.1: Security Comparison

	Dummy via [25]	TVD [11]	PMP-TVD [14]
Low Side-channel Leakage		●	●
Erasable/Programmable			●
Reverse Engineering	◑	●	●
Untrusted Fabrication			●

Table 4.1 gives a brief summary for the security comparison of PMP-TVD gates compared to previously proposed camouflaged gates using dummy vias [25] and fixed TVD [11]. The dummy via design only addresses reverse engineering, and only partially so, since advanced reverse engineering can typically discern real from dummy vias. Fixed TVD gates more fully address reverse engineering and have low side-channel leakage due to their differential gate topology, but they do not address untrusted fabrication or have the ability to erase or reprogram the logic function. PMP-TVD gates address both untrusted fabrication and reverse engineering threats, as well as having low side-channel leakage due to also having a symmetrical and differential gate topology.

4.6 PMP-TVD Overhead Analysis

When evaluating the power, performance, and area of the PMP-TVD gates, comparing single gates against their counterpart static CMOS standard cells can give us some insight. For TVD and PMP-TVD gates, the per gate comparison is done in [11] and [14]. However, a better comparison would be for a structure that consists of many gates with different functionalities. Therefore, we have chosen four ISCAS85 benchmark circuits [19][63] to evaluate PMP-TVD gates for functional correctness and power/performance/area overheads. To compare the overheads, we have applied two different methods. In the first one (*Gate-to-gate PMP-TVD replaced*), we have

replaced all the gates with their PMP-TVD equivalents and evaluated the performance, power consumption, and the area of the structure. In the second one (*LUT-to-gate PMP-TVD replaced*), we have created the look-up-table (LUT) version of the structure using 2- and 3- input LUTs. Since, PMP-TVD gates can be configured into any desired functionality, we have used them as LUT replacements, and evaluated the performance, power consumption, and the area of the structure. Next sections, we explain our methodology in the evaluation of overheads of PMP-TVD replaced structures and present the simulation results we gathered.

4.6.1 Methodology

For the comparison, we have used a subset of ISCAS85 benchmark circuits: c432, c1908, c3540, and c7552. At first, as the baseline comparison point, we have logically synthesized all the benchmarks on a 28nm CMOS process with the supplied standard cells using Cadence Genus (version 18.14) [64]. To have an exact comparison of 2- and 3- input PMP-TVD gates and to be able to directly map from the standard cells in the synthesized circuits to the existing PMP-TVD gates, the large cells in the library with four or more inputs are omitted in the synthesis flow using *"set_dont_use"* commands. For the synthesis, output capacitance is chosen as 25fF, and the maximum fan-out per stage is chosen as 16. With all the previously mentioned settings in common, two versions of each benchmark which are two opposite edge cases are synthesized. The two versions are: one with very tight delay constraint that trades off area and power consumption for the best possible performance (*Delay Optimized*), and one with very relaxed delay constraint to optimize for the best area (*Area Optimized*). The delay, power consumption, and area metrics are reported through the Genus reports. For the power consumption calculation, the circuits are assumed to have inputs which randomly change at an operating frequency of 100MHz. All the simulations are run with post-layout extracted views of the standard cells. In addition to the logical synthesis of the benchmark circuits, place and route (PnR) of the *Delay Optimized* and

Area Optimized standard cell implementations are done using Cadence Innovus (version 17.12) foundation flow [65]. Same power, performance, and area metrics are reported after the PnR stage.

The *Area Optimized* circuits, which have substantially fewer number of gates compared to their *Delay Optimized* counterparts, are used as a template for mapping the PMP-TVD gates to implement the benchmark circuits. In order to map the synthesized gates to PMP-TVD gates, first, a library of all the possible 2- and 3- input preprogrammed PMP-TVD gates (16 2-input and 256 3-input PMP-TVD gates) are constructed in Cadence Virtuoso [66] using a SKILL script [67]. Since the only difference between the preprogrammed PMP-TVD gates are the threshold voltage types (either low threshold voltage - LVT or high threshold voltage - HVT) of the NMOSes in the pull-down network, the script changed the device types in the schematics, and changed the doping layer mask in the layout views to construct the gates. After constructing all the possible PMP-TVD gates, Calibre jobs are run in batch mode to extract the post-layout parasitic views for each of them. To implement the gate-to-gate replacement, the cells in the *Area Optimized* netlist are replaced one by one with a PMP-TVD cell that was preprogrammed to implement the identical logical functionality as the replaced cell. If there is a buffer in the netlist, it is not replaced but kept. Instead, an additional buffer is added at the complementary output of the PMP-TVD gate before the buffer since PMP-TVD is a differential logic family. If there is an inverter in the netlist, the inverter is removed, and instead of it, the outputs of the PMP-TVD gate before the inverter are connected to the next gate in an inverted manner (i.e., OUT of the previous gate is connected to the INB of the next gate, and $OUTB$ of the previous gate is connected to the IN of the next gate). The new mapped verilog netlist is imported to Cadence Virtuoso [66] and the functionality is verified using Spectre simulations. Using the post-layout extracted views of the PMP-TVD gates, the mapped benchmarks are characterized using the same conditions as the standard cell synthesized benchmark circuits to report delay, area, and power.

Doing one-to-one gate replacement of standard cells to PMP-TVD gates is not the most

efficient way of camouflaging the structure using PMP-TVD gates. A given logical function can be implemented with fewer number of gates if look-up-tables are used. An n-input, single output PMP-TVD gate can realize many more functionalities than standard cells with the same input and output numbers. For this reason, another set of circuit netlists are created for each benchmark circuit by first synthesizing the verilog files into 2- and 3- input LUTs using the open source synthesis tool, Yosys [68]. After the netlists with LUTs are generated, using a script, the LUTs are replaced with their equivalent 2- and 3- input PMP-TVD gates from the PMP-TVD library that was created. This approach leads to more efficient realizations of the logic functions. Therefore, using the LUT version of the netlists for camouflaging with PMP-TVD gates leads to lower overheads than the standard cell to PMP-TVD mapped circuits. In addition, another flavor of this approach is also used where a buffer is added after each PMP-TVD gate's differential outputs. Since the generation of netlists with LUTs does not take into account of drive strength but just generates the LUT equivalent of the logic, adding a buffer at each output of the PMP-TVD gates improves the driving capability of the gates at the expense of a small increase in the power consumption and area. Both of the non-buffered and buffered versions of the benchmark circuits are characterized in Cadence Virtuoso using the post-layout extracted views of the PMP-TVD gates under the identical testing conditions as the previous methods.

For all the tests, when measuring the performance, the delay is calculated by measuring from the inputs to the last available output. For the PMP-TVD gates, only the evaluation time is taken into account. Power consumption is calculated by averaging the power over many cycles with randomly generated input vectors, where in the PMP-TVD gate replaced structures power consumption includes both the evaluation and precharge phases. The area is the summation of the areas of all the gates are used (In PMP-TVD gate replaced structures, the area of the inverters and the buffers are also taken into account).

4.6.2 Overhead Comparison Results

The overhead of the PMP-TVD gate implementations using the ISCAS85 benchmark circuits c432, c1908, c3540, and c7552 are shown in Figures 4.15, 4.16, 4.17, and 4.18, respectively. The detailed results are given in table format in Appendix A.

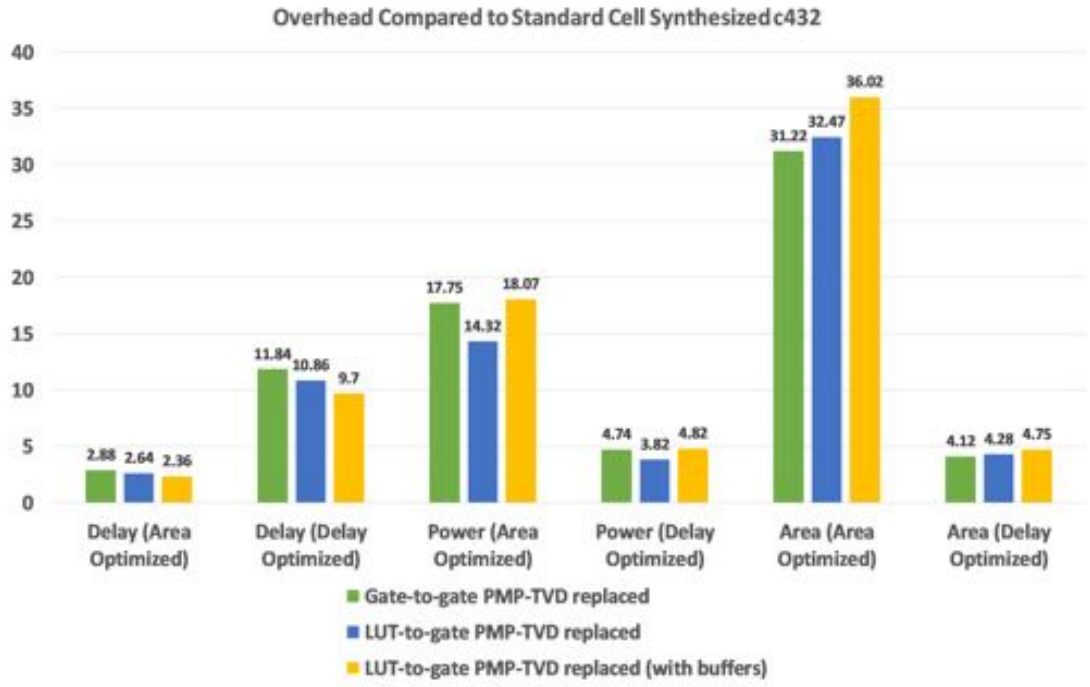


Figure 4.15: Overhead results of gate-to-gate PMP-TVD replaced (green), LUT-to-gate PMP-TVD replaced (blue), and LUT-to-gate PMP-TVD replaced with buffers (yellow) compared to *Area Optimized* standard cell synthesized and *Delay Optimized* standard cell synthesized are shown for the benchmark c432.

Depending on the structure and the design choice, the overhead values vary. Optimizing the design for delay or area gives us the two opposite edge cases. The design choice will be between these two edge cases, therefore the overhead values for *Area Optimized* and *Delay Optimized* will give the lower and upper boundaries for the delay, power, and area overheads. The results show that PMP-TVD replaced designs have a lower overhead in delay compared to the *Area Optimized* standard cell synthesized designs. This is expected since PMP-TVD gates have higher input and internal capacitance, and stacked NMOSes in their pull-down networks, they will have smaller delay overhead compared to *Area Optimized* designs, where smaller and fewer gates are

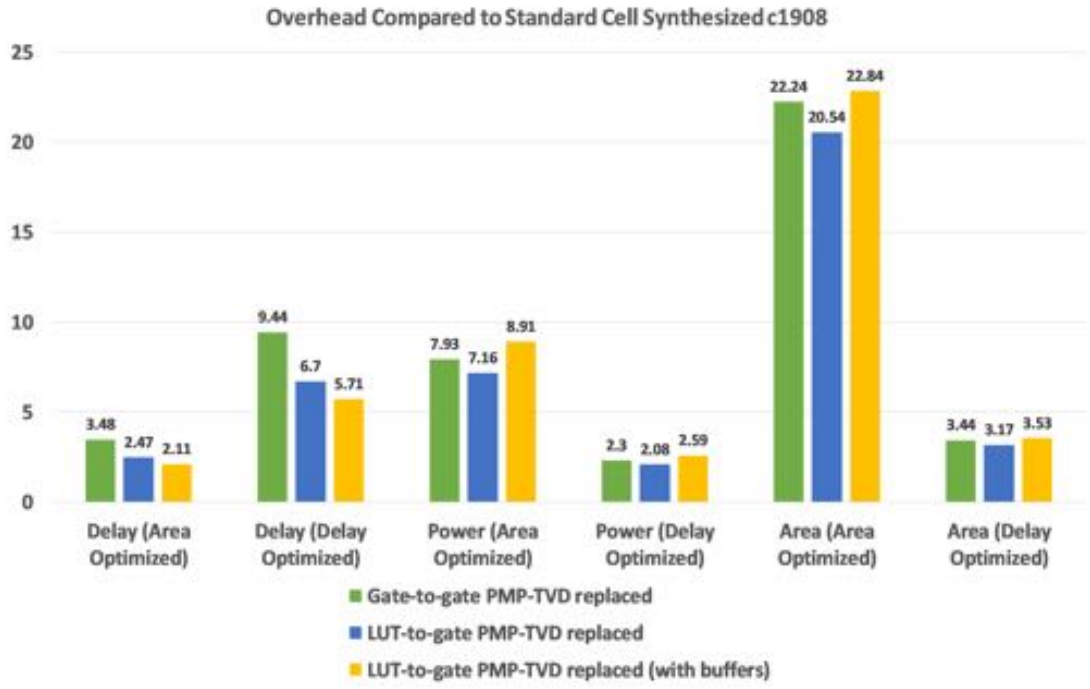


Figure 4.16: Overhead results of gate-to-gate PMP-TVD replaced (green), LUT-to-gate PMP-TVD replaced (blue), and LUT-to-gate PMP-TVD replaced with buffers (yellow) compared to *Area Optimized* standard cell synthesized and *Delay Optimized* standard cell synthesized are shown for the benchmark c1908.

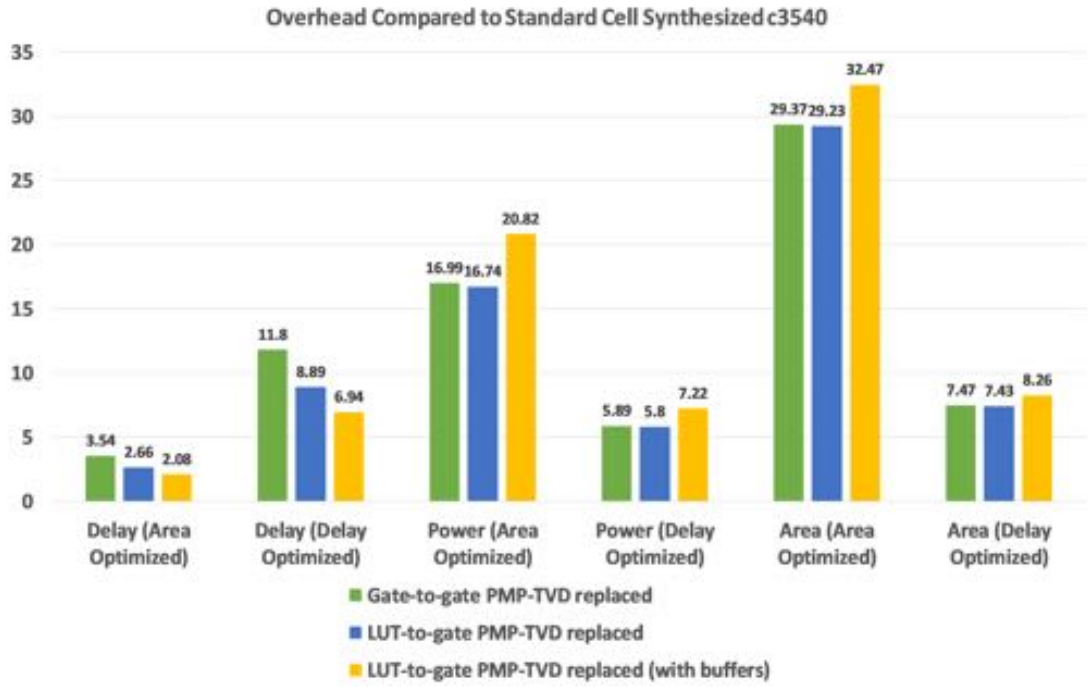


Figure 4.17: Overhead results of gate-to-gate PMP-TVD replaced (green), LUT-to-gate PMP-TVD replaced (blue), and LUT-to-gate PMP-TVD replaced with buffers (yellow) compared to *Area Optimized* standard cell synthesized and *Delay Optimized* standard cell synthesized are shown for the benchmark c3540.

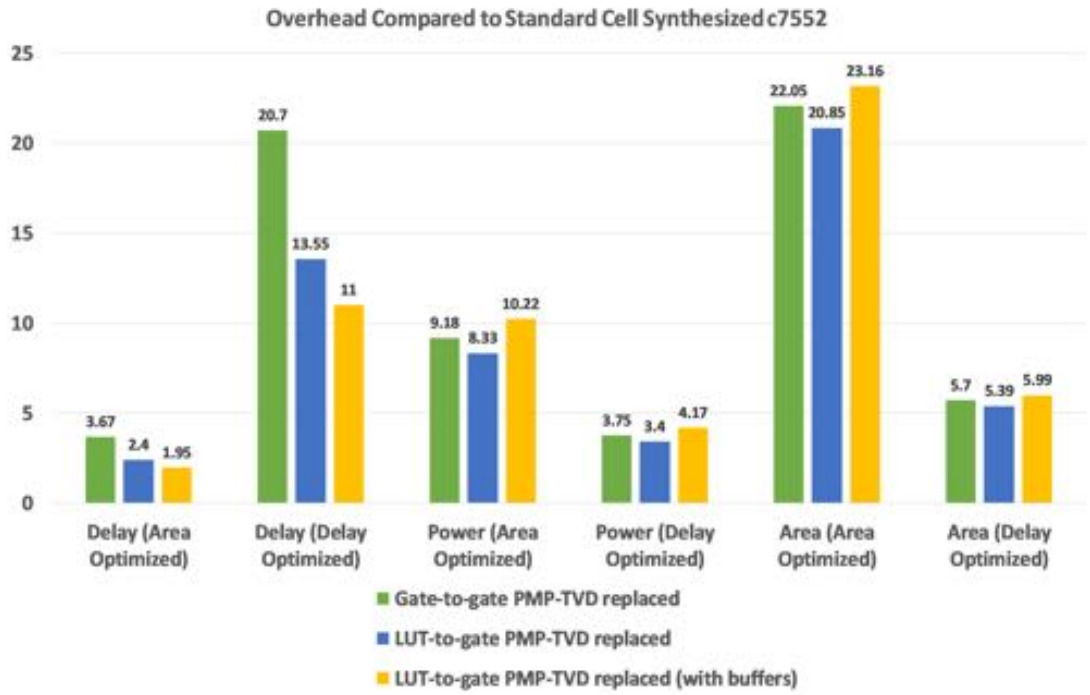


Figure 4.18: Overhead results of gate-to-gate PMP-TVD replaced (green), LUT-to-gate PMP-TVD replaced (blue), and LUT-to-gate PMP-TVD replaced with buffers (yellow) compared to *Area Optimized* standard cell synthesized and *Delay Optimized* standard cell synthesized are shown for the benchmark c7552.

used in expense of performance. On the other hand, PMP-TVD replaced designs have the lower overheads in power and area compared to the *Delay Optimized* standard cell synthesized designs, where larger and stronger devices are used to achieve a better performance.

The LUT representation of the benchmarks have fewer gates than the standard cell synthesized versions. Therefore, compared to the gate-to-gate replacement, LUT-to-gate replacement results in fewer PMP-TVD gates. This results in smaller delay, power, and area overheads in LUT-to-gate replacement compared to gate-to-gate replacement. However, as mentioned earlier, the LUT representation of the structure does not take drive strength of the gates into account. Therefore, additional buffers at both of the outputs of each PMP-TVD gate are required to achieve a lower delay overhead. Although, additional buffers provide lower delay overhead, this benefit comes at the expense of increased power and area overheads since the number of added buffers are twice the number of existing PMP-TVD gates (one buffer for OUT and one buffer

Table 4.2: Overhead of Place and Route Step for Standard Cell Synthesized Structures

Designs	Number of Gates	Delay	Power	Area
c432				
Area Optimized	1.01x	1.29x	1.51x	1.09x
Delay Optimized	1.08x	1.66x	1.39x	1.04x
c1908				
Area Optimized	2.48x	1.39x	1.35x	1.66x
Delay Optimized	1.12x	1.74x	1.23x	1.1x
c3540				
Area Optimized	1.00x	1.28x	1.46x	1.02x
Delay Optimized	1.06x	1.78x	1.82x	1.06x
c7552				
Area Optimized	1.00x	1.38x	1.24x	1.02x
Delay Optimized	1.20x	1.91x	1.49x	1.08x

for $OUTB$ are added after each PMP-TVD gate).

The overhead of the PnR step on the benchmarks synthesized with standard cells are shown in Table 4.2. The PnR step adds significant increase in delay, power consumption, and area for the structures synthesized with standard cells. This is due to wire capacitance being comparable to the input capacitance of the standard cells. On the other hand, PMP-TVD gates have all the possible input combinations in their pull-down network. Hence, the input capacitance of a PMP-TVD gate is much higher compared to a standard cell with the same number of inputs. This results in minuscule increase in delay after PnR step for the structures with PMP-TVD gates. To examine the effects of PnR on PMP-TVD gates, we have run simulations on a 16-bit carry select adder built with 2- and 3- input PMP-TVD gates, which we also implemented in our second prototype testchip (Chapter 5). The first set of simulations are run using the post-layout extracted views of just the PMP-TVD gates which ignores routing parasitics. The second set of simulations are run using the post-layout extracted view of the whole 16-bit adder after a full-custom PnR step which takes into account routing parasitics.

Table 4.3: Overhead Increase of Place and Route Step

Designs	Delay	Power	Area
PMP-TVD Adder	11%	16%	30%
Average for Area Optimized Standard Cell Synthesized Structures	34%	39%	20%
Average for Delay Optimized Standard Cell Synthesized Structures	78%	48%	7%

Table 4.3 shows the increase in delay, power, and area overheads after the PnR step for the PMP-TVD adder structure, *Area Optimized* standard cell synthesized structures, and *Delay Optimized* standard cell synthesized structures. The delay and power overhead increase in PnR step for PMP-TVD gates are much smaller compared to the PnR step of standard cells as can be seen in Table 4.2. Thus, after the PnR step, the total delay and power overhead of PMP-TVD gate replacement is expected to be smaller than the overhead values shown in Figures 4.15, 4.16, 4.17, and 4.18.

The reported overheads represent only the increase in delay, power, and area for the camouflaged structures. The structures that require camouflaging are only a small part of an IC. Therefore, the effective delay, power, and area overheads incurred by the PMP-TVD camouflaging are smaller overall.

4.7 Comparison of PMP-TVD with Other Countermeasures

Researchers have proposed various countermeasures to mitigate reverse engineering and untrusted fabrication threats. Design obfuscation techniques aimed at these security threats include: split manufacturing, camouflaged logic, logic locking, and configurable logic. Each of the proposed methods provides different trade-offs associated with delay, power, and area overheads, and additional manufacturing costs.

In split manufacturing, the fabrication of the IC is split into two parts, namely front-end-

of-line and back-end-of-line [3][52]. The front-end-of-line which includes the fabrication of the transistors and lower level metals can be taken up by an untrusted but high-end foundry. The back-end-of-line, where higher-level interconnects are fabricated, can be carried in a trusted foundry. This way, the complete design information is kept away from the untrusted foundry. The main unintended consequence of this method is that it increases the manufacturing costs of the IC and not every foundry supports this type of manufacturing style. Despite these increased costs to address security concerns, the complete design is still vulnerable to reverse engineering attacks post-production.

In camouflaged logic, methods like look-alike gates [28] or structures with dummy vias [25] depend on the limited resolution of the reverse engineering attacks. On top of the delay, power, and area overheads, dummy via structures require a non-standard process to manufacture. On the other hand, camouflaging methods that employs using different threshold voltage transistors do not rely on the imaging capabilities of the reverse engineers, since threshold voltage is not a physical structure. Instead it is an implant density, which is extremely difficult for a reverse engineer to determine, especially on a large scale. Notably, all of the camouflaged logic methods fail at securing the hardware when there is an untrusted fabrication threat, since the camouflaged design information is sent to the foundry.

In logic locking, additional gates are implemented in the design such that with only correct inputs (i.e., key inputs) to those gates the IC becomes functionally correct. If an incorrect key is supplied, the IC generates faulty outputs. As the correct key is only known by the design house, an untrusted foundry does not have access to a functionally correct IC. Similar to logic locking, configurable logic protects the design information from an untrusted fabrication by having a configurable design fabric. Both of these methods are subject to non-invasive attacks to extract the secret information. Among these attacks, Satisfiability-based (SAT-based) attacks are the most efficient [21]. Most of the logic locking methods are vulnerable to these attacks, therefore obfuscation methods using configurable logic similar to LUTs are proposed to achieve SAT-resiliency

[55]. The proposed methods that employ either logic locking or configurable logic methodology have the following incomplete assumptions regarding the adversary's capabilities: in both methodologies, the proposed solutions either only focus on non-invasive attacks and ignore invasive attacks or assume that the memory storing the secret key and the delivery of the key inputs to the logic are tamper- and read- proof [51]. The proposed methods might be standard CMOS process compatible and can incur small overheads, however, instead of ignoring the mentioned issues, having a tamper- and read- proof memory should be included in the overhead calculation.

In PMP-TVD, we aimed to have a secure camouflaging method without the need for any non-standard process steps. Moreover, PMP-TVD logic has reduced side-channel leakage which the other proposed methods do not have. While PMP-TVD camouflaging incurs large overheads, it offers security without the need of having a secure read- and tamper- proof memory. PMP-TVD camouflaging shows SAT-resiliency similar to the LUT-based solutions. Moreover, because only a small percentage of the chip is camouflaged, the effective overhead increase will be smaller overall.

4.8 Summary

In this chapter, we have shown the circuit details and analysis of the proposed secure camouflaged logic family, post-manufacturing programmed threshold voltage defined logic (PMP-TVD). We have shown how a PMP-TVD gate operates and explained the design knobs of the structure. Later, we have introduced binary aging elements (BAE), that can be used to characterize HCI which is used for programming of the PMP-TVD structures. Then, we have evaluated the security of the PMP-TVD gates and shown an overhead analysis compared to standard cell synthesized structures.

With the addition of post-manufacturing programmability on top a TVD gate, PMP-TVD

achieves security against untrusted fabrication on top of protection against reverse engineering which is inherited by the TVD topology. In addition, PMP-TVD logic allows enhancing, erasing, or changing the functionality of the preprogrammed design by applying HCI stress post-production. Furthermore, reprogrammability gives the designer an advantage of being able to upgrade their design in the field.

Chapter 5

Prototype Testchips with Securely Camouflaged Structures

In the previous chapters, we have presented two secure camouflaging techniques, threshold voltage defined (TVD) logic and post-manufacturing programmed threshold voltage defined (PMP-TVD) logic, respectively for reverse engineering and for both reverse engineering and untrusted fabrication. In addition, we have introduced binary aging element (BAE), a structure to characterize hot-carrier injection (HCI) which is a technique used in PMP-TVD gates to achieve programmability and erasability. Our design goal was to achieve minimal overhead in area, performance, and delay while providing camouflaging against reverse engineering and untrusted fabrication. We implemented and taped-out two prototype testchips which include structures built with TVD and PMP-TVD gates, and BAEs as proof-of-concepts for our designs. The results from the prototype testchips demonstrate that PMP-TVD gates can be used as a camouflaging method for reverse engineering and untrusted fabrication with feasible overheads.

5.1 Testchip in a 65nm CMOS Process

5.1.1 Overview

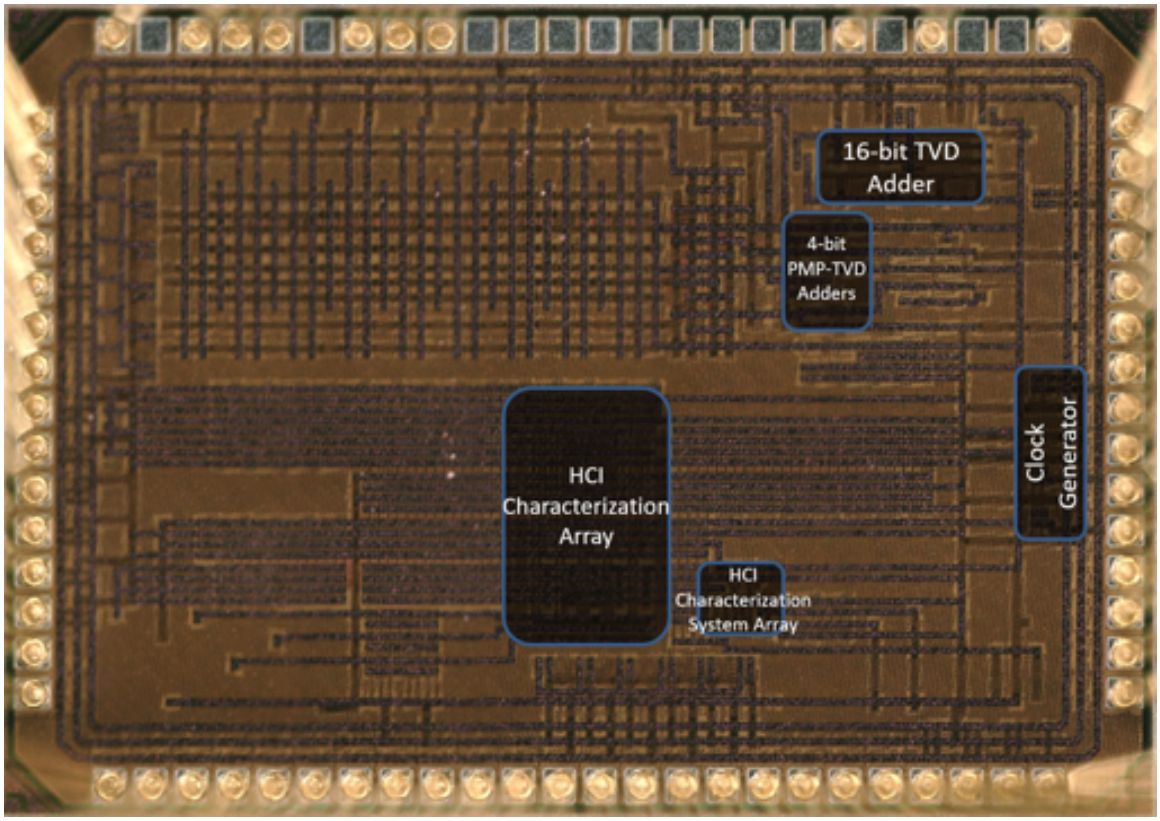


Figure 5.1: Die shot of the first prototype testchip. 16-bit TVD adder, 4-bit PMP-TVD adder and 4-bit PMP-TVD blank structures, HCI characterization array, and HCI characterization system array are highlighted [1][14][2].

The first prototype testchip is implemented in an industrial 65nm CMOS process with 9-metal layers. The testchip die shot can be seen in Figure 5.1. The die area is 1.2mm by 1.7mm and it has 78 I/O pads along the periphery. Table 5.1 summarizes the technology and prototype testchip features.

On the testchip, there are thirteen different voltage domains, and each of them has their own power grid. Out of the thirteen voltage domains, two of them are used to power the I/O ring with 1V and 3V. From the remaining voltage domains, HCI stress related ones are at 3V and the rest are supplying 1V to the structures. Each structure has its own test infrastructure, and these test

Table 5.1: Technology and Features of the First Prototype Testchip

Technology	65nm CMOS with 9-metal layers	
FO4 in TTLH	35ps	
Supply Voltage	1.0V	
Chip Area	2.04mm^2 (1.2mm x 1.7mm)	
Number of I/O Pads	78	
Area of the Structures	**Core**	**Including Test Structures**
16-bit TVD Adder	2875.12μm^2	28840μm^2
4-bit PMP-TVD Adder	941.85μm^2	8640μm^2
HCI Characterization Array	40000μm^2	64000μm^2
HCI Characterization System	2914μm^2	5694μm^2

circuitry have separate supply voltages to enable measurements at the core with different voltage levels.

The testchip in Figure 5.1 contains the following structures:

1. A 16-bit carry select adder using 2- and 3- input fixed TVD gates (i.e., no HCI programming devices)
2. A pipelined 4-bit carry select adder using 2-input preprogrammed PMP-TVD gates
3. A pipelined 4-bit carry select adder using 2-input blank PMP-TVD gates
4. An HCI characterization array consisting of 500 modular BAEs
5. A self-contained HCI characterization array consisting of 16 modular system BAEs (i.e., single BAE is characterized at a time; each stressed BAE senses when the desired stress amount is achieved and then starts the HCI stress process of the following BAE)

The structures on the chip are clocked by using an on-chip ring oscillator based clock generator with a wide-range of frequency configuration. In the clocking infrastructure, there are four ring oscillators with four different base clock frequencies (i.e., 2.89GHz, 3.88GHz, 4.62GHz, and 5.73GHz). The voltage supply of these ring oscillators are separate than the rest of the infrastructure so that desired clock frequencies can be generated. These generated clocks are fed

into a twelve-step divide-by-two stages to generate wide-range of clock frequency options (i.e., 708kHz to 5.73GHz at nominal voltage supply). In addition, in case of an issue with the on-chip ring oscillators, a pad that can take an off-chip generated clock signal is fed into the clocking infrastructure. A 14:1 MUX stage selects the configured clock signal from the generated wide-range of clock signals, and then the selected signal is distributed to all of the structures' own clock distribution network. The distributed clock signal is also divided by 4096 times and then fed to a pad to measure the operating frequency of the chip.

5.1.2 TVD and PMP-TVD Structures

Both of the TVD and PMP-TVD structures are carry select adders built by using either TVD gates or PMP-TVD gates. Like other dynamic logic families, both TVD and PMP-TVD gates have 2 phases of operation (precharge and evaluate), so the adders are split into two phases. For both of the structures, first half consists of the carry and sum generators and the second half consists of the carry selection MUXes. The data values between the halves and at the end of the structure are latched. The carry and sum generators, and the selection MUXes in the 16-bit TVD adder is built by using 2- and 3- input TVD gates. The latches in between and at the end are standard CMOS gates. In the 4-bit PMP-TVD adder, only the carry and sum generators are built with 2-input PMP-TVD gates. The latches and the selection MUXes are standard CMOS gates. The structures and the layouts of the 16-bit TVD adder and the 4-bit PMP-TVD adder can be seen in Figures 5.2, 5.3, 5.4, and 5.5. The 16-bit TVD adder is divided into 4-bit full adder sections. The lowest four bits are added up assuming the carry-in value as 0. The remaining twelve bits are added up for carry-in as both 0 and 1. Then these values are latched in between. The second half of the carry select adder selects the correct carry and sum values, and then the correct sixteen sum bits and the carry bit are latched. The 4-bit PMP-TVD adder is divided into 1-bit full adder sections. Similar to the 16-bit TVD adder, the first bits are added up assuming

the carry-in value as 0. The remaining three bits are added up for carry-in as both 0 and 1. Just like the TVD adder, the values in between are latched. After, the correct carry and sum values are MUXed and the sum bits and the carry bit are latched.

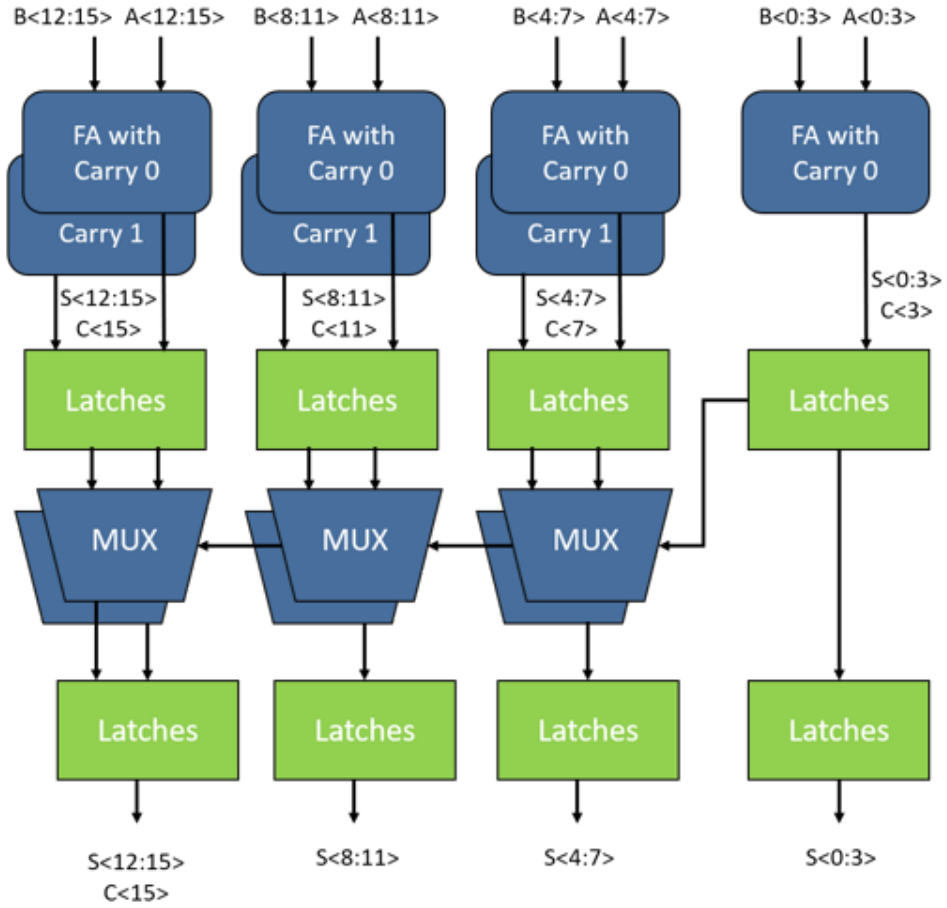


Figure 5.2: Structure of the 16-bit TVD carry select adder. When clock is high, the full adders evaluate, and generate the sum and carry bits for carry in being 0 and 1, then these bits are latched. When clock is low, according to the carry bits the true sum and carry bits are MUXed and latched[14].

The details of the structures are as follows: the dimensions of the 16-bit TVD adder are 67.27μm by 42.74μm, and the dimensions of the 4-bit PMP-TVD adders are 34.5μm by 27.3μm. All the adders have self-test circuits to be able to test them at speed. Each test structure has scan-enabled single-ended shift registers that provide input data and capture output data. The input registers for the 16-bit TVD adder can hold 16 test vectors and the output registers can store 16 most recent responses. The input registers for the 4-bit PMP-TVD structures can hold 4

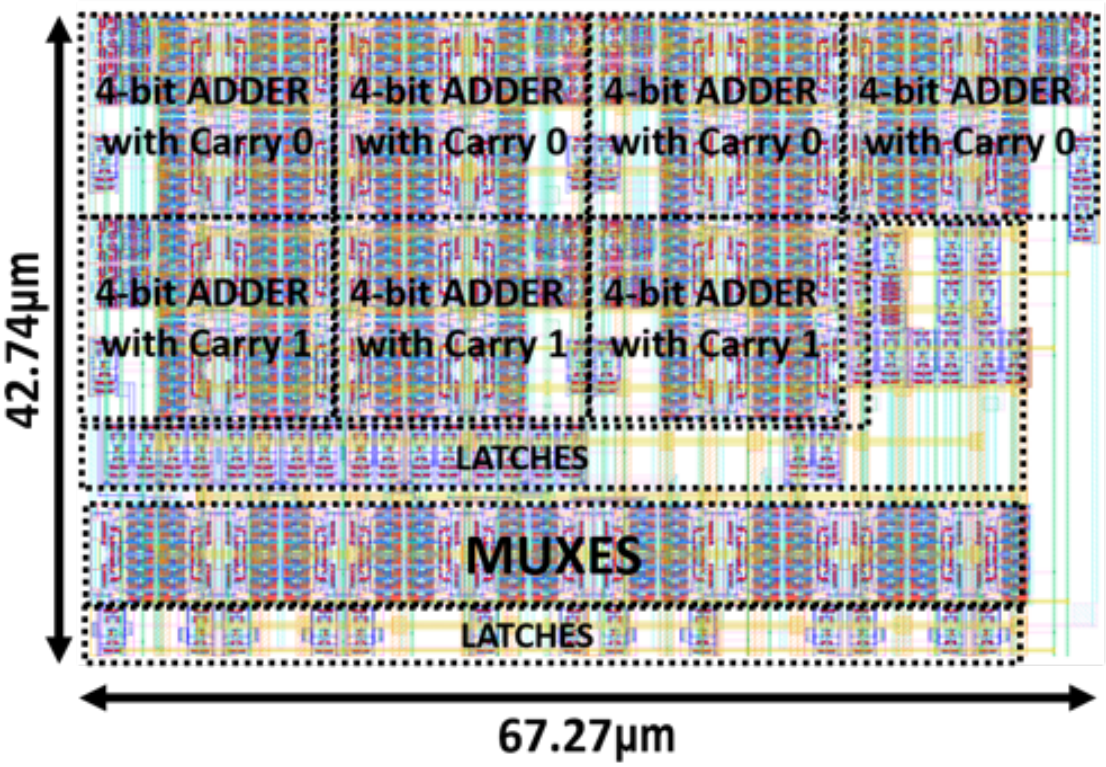


Figure 5.3: Layout of the 16-bit TVD carry select adder. When clock is high, the full adders evaluate, and generate the sum and carry bits for carry in being 0 and 1, then these bits are latched. When clock is low, according to the carry bits the true sum and carry bits are MUXed and latched[14].

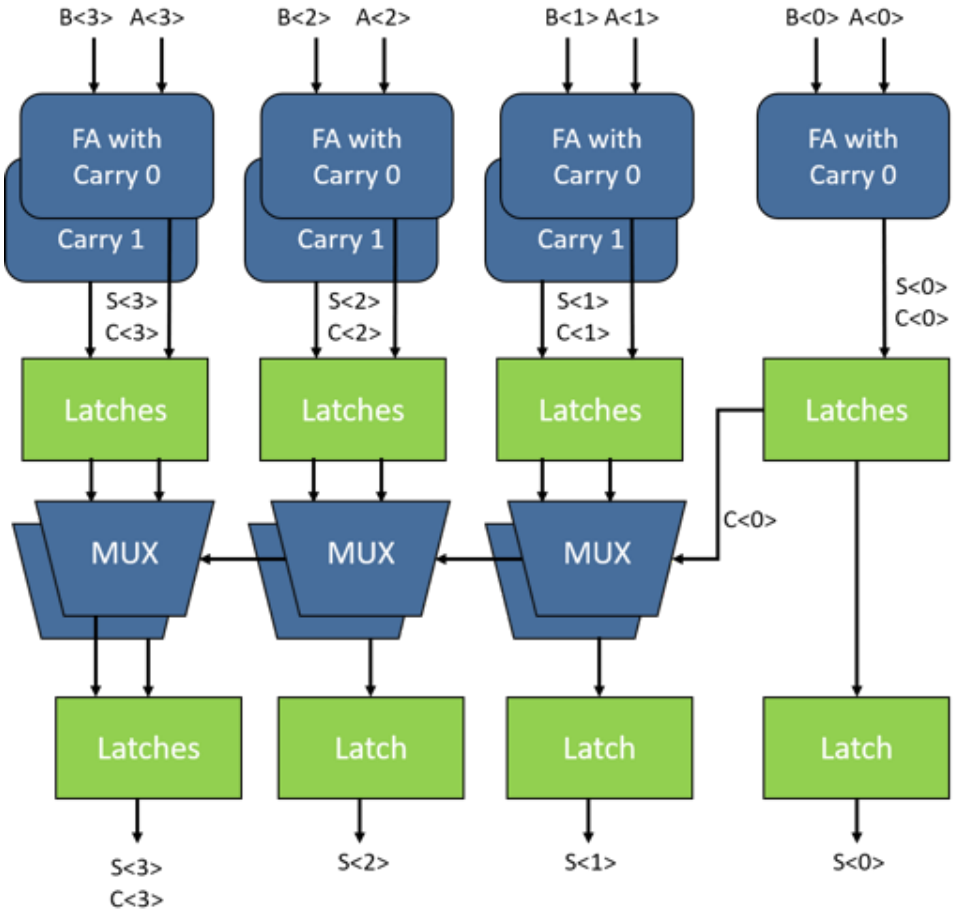


Figure 5.4: Structure of the 4-bit PMP-TVD carry select adder. When clock is high, the full adders evaluate, and generate the sum and carry bits for carry in being 0 and 1, then these bits are latched. When clock is low, according to the carry bits the true sum and carry bits are MUXed and latched. During the HCI stress, clock is pulled low, and the stress is applied according to the configuration[14].

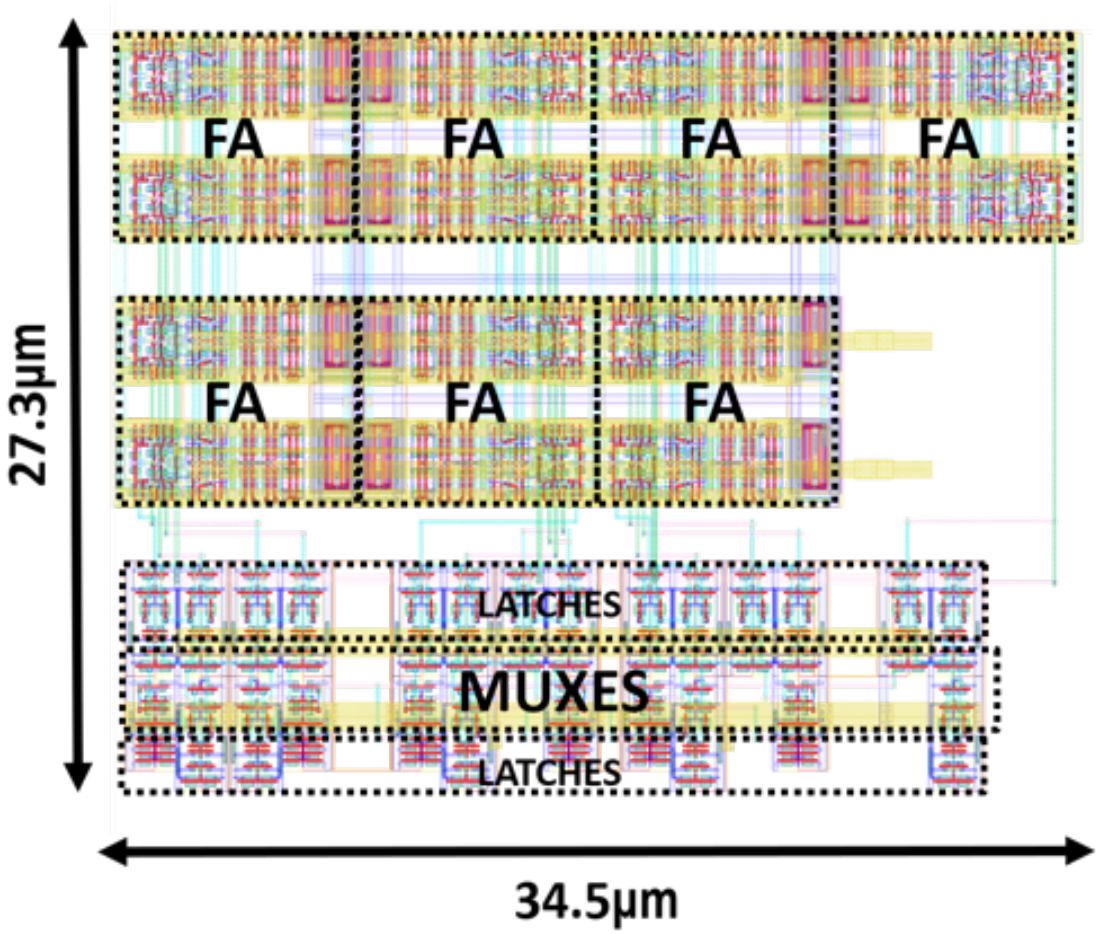


Figure 5.5: Layout of the 4-bit PMP-TVD carry select adder. When clock is high, the full adders evaluate, and generate the sum and carry bits for carry in being 0 and 1, then these bits are latched. When clock is low, according to the carry bits the true sum and carry bits are MUXed and latched. During the HCI stress, clock is pulled low, and the stress is applied according to the configuration[14].

test vectors and the output registers can store 4 most recent responses. The input registers are designed to operate in a loop to provide continuous data. At the end of each input register loop, a 3-2 fork generates both true and complement test vector signals which are needed by the TVD and PMP-TVD gates. At the output registers, only the true signals are captured. In addition, the 4-bit PMP-TVD adders have shift registers to provide the HCI stress configuration. After the HCI stress configuration is loaded, it is latched. This way the changing data in the shift registers doesn't affect the stress configuration.

Test Methodology

The designs are simulated and tested at 1V nominal operation voltage and the PMP-TVD structures are HCI stressed at 3V stress voltage. All the tests are done at room temperature. To test the 16-bit TVD adder, randomly generated 16 vectors are loaded into the input registers. First, the functionality of the structure is confirmed for different random vectors. Then, at full speed, the random input vectors are continuously looped, and the energy and frequency are measured.

For the 4-bit PMP-TVD structures, same methodology as 16-bit TVD adder is applied. Using the randomly generated vectors in the input registers, first the functionality of the structures are confirmed, and then they are run at speed in a loop to measure the energy and frequency.

Using HCI stress, the preprogrammed PMP-TVD gates can either be "boosted" (HCI stress is used to reinforce the preprogrammed logic function) or "reversed" (HCI stress is used to program in a different logic function than the preprogrammed functionality). Before any HCI stress, we first checked the functionality and performance of the preprogrammed adder structures as the baseline with a supply voltage range of 0.7V-1.2V where the nominal VDD is 1V. Then, we started exploring HCI programmability by inducing the HCI stress for 60 seconds. We have applied the HCI stress in boost stress and reverse function stress modes, and checked the functionality and performance. In addition, we have used HCI stress to program a functionality into

the blank PMP-TVD structures. The HCI stress voltage is set at 3V, which resulted in a current density and voltage drop per leg of 18.4mA/μm^2 and 2.67V.

Measurement Results

A summary of the silicon results for 4-bit PMP-TVD preprogrammed adder before HCI stress, 4-bit PMP-TVD preprogrammed adder after reverse stress (i.e., after applying 60 seconds of HCI stress to change the functionality), 4-bit PMP-TVD preprogrammed adder after boost stress (i.e., after applying 60 seconds of HCI stress that is reinforcing the adder functionality), 4-bit PMP-TVD blank adder after HCI programming (i.e., after 60 seconds of HCI stress that configures the adder functionality, and 16-bit TVD adder in the 65nm CMOS process can be seen in Table 5.2.

Table 5.2: 65nm Testchip Results for TVD and PMP-TVD Structures

	4-bit PMP-TVD				**16-bit TVD**
	Preprogrammed	**Reverse Stressed**	**Boost Stressed**	**Blank**	**Adder**
Area	0.007mm^2 (Core: 0.001mm^2)				0.029mm^2 (Core: 0.003mm^2)
Frequency at 1V	3.2GHz	2.9GHz	3.7GHz	3.6GHz	1.0GHz
Power at 1V	1.14mW	0.96mW	1.09mW	1.09mW	3.22mW
Leakage at 1V	0.15mW	0.14mW	0.14mW	0.14mW	0.26mW

Performance of 16-bit TVD Adder

The 16-bit adder with fixed TVD gates operates between 474MHz and 1.21GHz at a power supply ranging from 0.7V to 1.2V. The power consumption of the adder is between 0.889mW and 5.46mW for the same power supply range. The shmoo plot of the structure at room temperature is shown in Figure 5.6. At the nominal 1V VDD, the 16-bit adder operates at 1.03GHz with

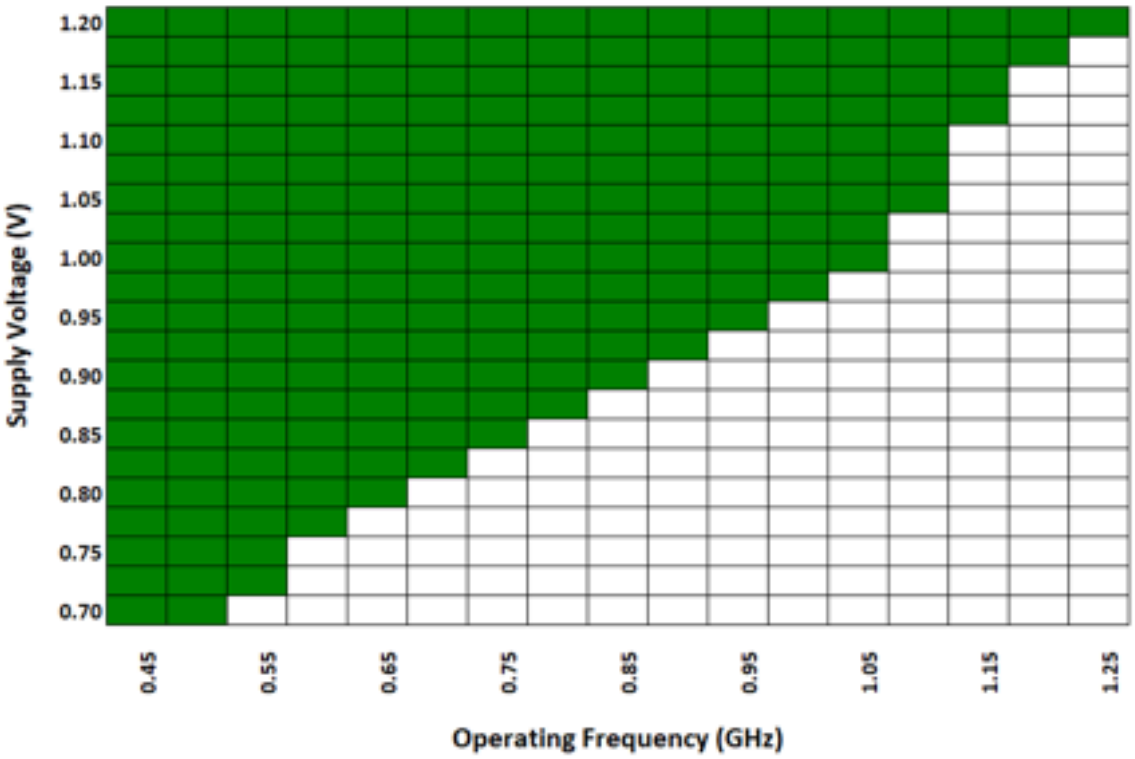


Figure 5.6: Shmoo plot at room temperature for the 16-bit TVD adder [14].

a power consumption of 3.22mW. The leakage at this operating point is 8% of the total power consumption.

Performance of 4-bit PMP-TVD Structures Before and After HCI Stress

The preprogrammed 4-bit adder operates between 1.8-4.08GHz at a power supply range of 0.7-1.2V. For the same power supply range, the 4-bit adder consumes between 0.35mW to 2.15mW. At nominal 1V VDD, the adder operates at 3.21GHz with a power consumption of 1.14mW. At this operating point, the leakage of the adder is 13% of the total power consumption.

After the same 4-bit PMP-TVD adder is HCI stressed that reinforced the adder functionality, the operating range increased from 1.8-4.08GHz to 1.87-4.3GHz at a power supply ranging from 0.7-1.2V. As can be seen from the shmoo plot in Figure 5.7, the upper boundary on the operating range is same for the power supply between 1.1-1.2V. This upper range is not limited by the

PMP-TVD adder, but it is limited by the testing structure of the adder.

When the same HCI configuration to boost the adder functionality is applied to a blank structure, the adder functionality is programmed into the PMP-TVD structure. After this HCI stress, the blank version with the adder functionality achieves a similar performance with the same range of operating frequency.

When a 4-bit PMP-TVD adder is HCI stressed to change the functionality (i.e., in this case a 4-bit subtraction functionality is programmed into the preprogrammed 4-bit PMP-TVD adder), the new functionality achieves operation between 1.32-3.78GHz at a power supply range of 0.7-1.2V. At this power supply range, the new functionality consumes between 0.29-1.78mW power.

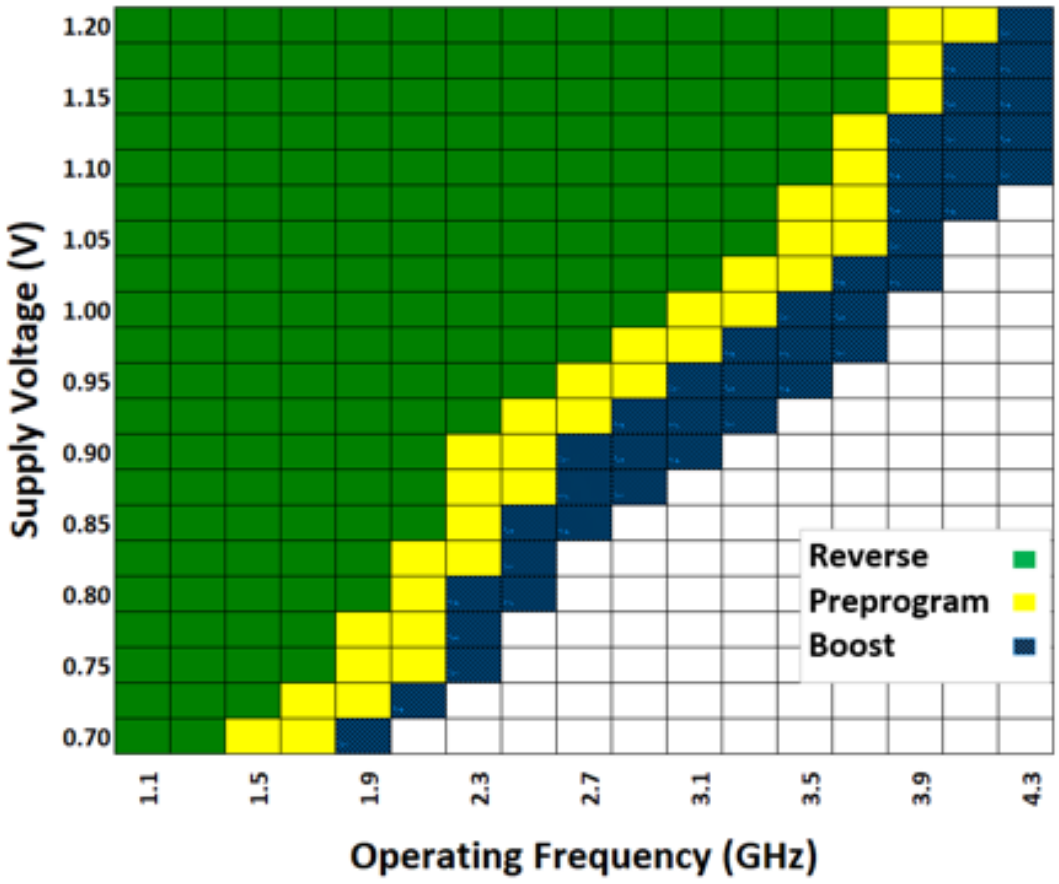


Figure 5.7: Shmoo plot at room temperature for the 4-bit PMP-TVD preprogrammed adder: preprogrammed baseline (yellow), 60 seconds of reverse stress (green), and 60 seconds of boost stress (blue) [14].

The overlapped shmoo plots of the 4-bit PMP-TVD preprogrammed adder, preprogrammed

adder after boost stress, and preprogrammed adder after reverse stress are shown in Figure 5.7. The operating frequencies, power consumption and leakage percentages of the PMP-TVD structures at the nominal 1V VDD are summarized in Table 5.2.

HCI Programming and Permanence

We have explored the HCI stress time required to program a functionality into a blank PMP-TVD gate, and reversing the functionality of a preprogrammed PMP-TVD gate. We applied the HCI stress for 60 seconds in 10 second steps for a preprogrammed adder to reverse the functionality and for a blank structure to program an adder functionality. Figure 5.8 shows the operating frequency of the blank and preprogrammed PMP-TVD designs as a function of stress time.

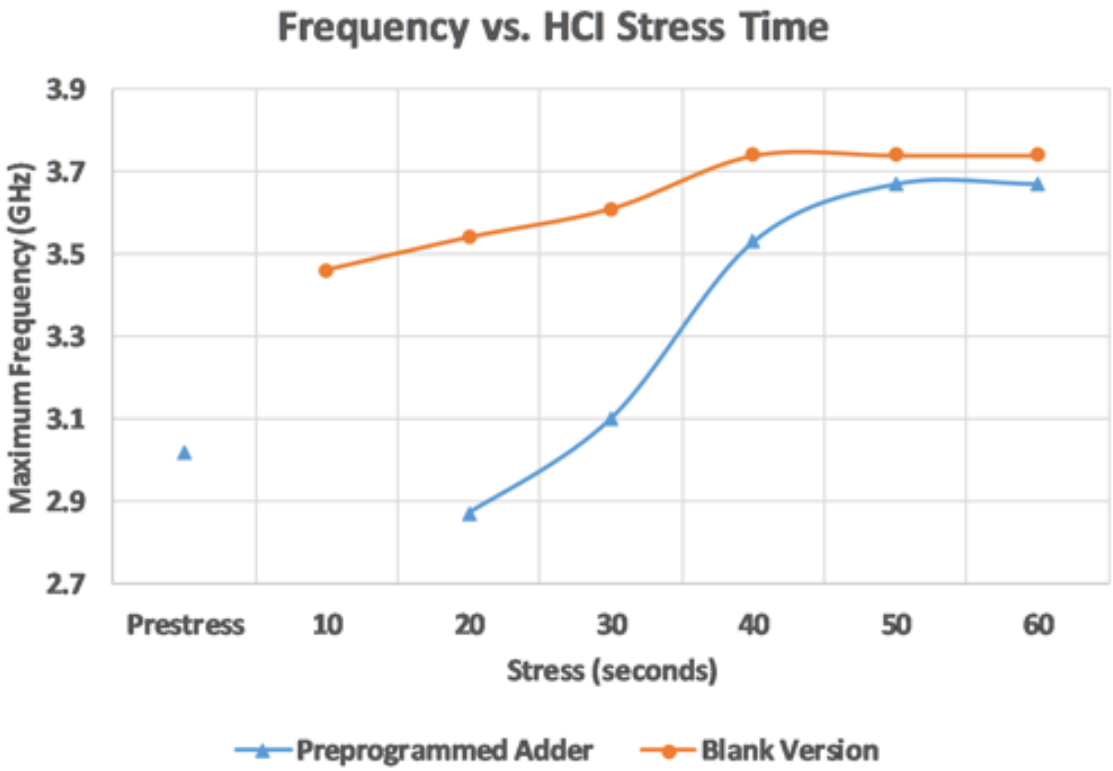


Figure 5.8: Frequency vs. HCI stress time plot of 4-bit blank PMP-TVD adder at 1V and room temperature (orange). Also, blue line shows stress time needed to reverse preprogrammed PMP-TVD adder (20 seconds) and subsequent boosting of the reverse function [14].

The orange line in the figure shows the blank structure under HCI stress to program an adder

functionality. Initially, the blank design does not have any functionality. However, even with 10 seconds of stress, the blank design is sufficiently programmed to function correctly as an adder. After the initial programming, further HCI stress with the adder programming reinforces the adder functionality and increases the performance of the structure. After 60 seconds of HCI stress, the performance increase plateaus, and further stress does not increase the performance of the new function.

The blue line in the figure shows the preprogrammed adder under HCI stress to change the functionality. Initially, before any HCI stress, the structure has the adder functionality. However, just after 10 seconds of HCI stress, the adder functionality is removed from the structure. At this point, the structure's functionality is neither an adder nor the new functionality that we are trying to program in. With an additional 10 seconds of HCI stress, the structure gets it's new functionality. Just like the blank structure, after continuous HCI stress, the performance of the new functionality increases, and after 60 seconds of total stress time, the performance increase plateaus and further stress does not have an effect on the performance.

After exploring HCI programming on preprogrammed and blank PMP-TVD structures, we have tested the permanence of HCI programming. To test the permanence of the HCI programming, we baked a testchip at 125°C for 48 hours (in two 24 hour steps) in a temperature chamber. After the initial 24 hours, the structure's maximum frequency at nominal VDD and room temperature has shown a 5% decrease. However, after the second 24 hours, the performance of the structure remained the same, showing a slight reversal from baking, but a plateauing and program retention under high temperature.

5.1.3 HCI Characterization Structures

For HCI characterization purposes, the prototype testchip has an array of 500 modular binary aging elements (BAE) and a self-stressing system with 16 modular BAEs. The array of 500

modular BAEs provides a baseline to characterize different configuration of BAEs and the effect of HCI. The schematic and layout of a single modular BAE, and the structure of a modular system BAE are shown in Figures 4.11 and 4.12. The modular BAE array has the dimensions of 200μm by 200μm. The self-stressing modular system's dimensions are 62μm by 47μm. Each modular BAE has an area of 52.5μm^2, and each modular system BAE has an area of 182.9μm^2.

Test Methodology

The designs are simulated and tested at 1V nominal operation voltage and 2.5V HCI stress voltage. The modularity of the design provides 693 possible combinations for different stress current and current density values. For all possible combinations the initial stress current, initial stress current density, and the initial voltage drop that the stressed devices see are recorded to analyze the different parameters' effect on HCI.

Our testing approach to measure the HCI effects on V_{TH} is comparing the input offset value. Since the sense amplifier based BAE design has an initial bias, if given the same input (i.e., 1V nominal VDD in this case), the biased side will have an output value of *0*. With HCI stress, V_{TH} of the biased input side will start to increase. With this effect, the input offset required to flip the output will start to decrease. After some point, with the same nominal input for both inputs, the output will be flipped. With these stress tests, we can gather the data of required time of HCI stress to shift a certain amount of threshold voltage in a given transistor size.

Before beginning the stress test in the characterization array, input values are swept to find the initial input offset value for all the possible device size combinations. After the initial input offset value for a certain configuration is recorded, in a loop, a certain time of HCI stress is applied and inputs are swept to measure the new input offset. This way, the effect of HCI stressing on input offset with time is recorded.

As an example, we have stressed multiple inputs legs at the same time to obtain multiple char-

acterization data. After the multiple legs are stressed, during sweeping the input values, multiple comparisons are done. For a case of three legs stressing, there were seven input sweepings: 3 for single legs, 3 for two of the legs at the same time and 1 for all legs at the same time. The comparison is done with the same number of legs for both of the inputs. With this configuration stress test data for 3 different sizes are obtained. These results are shown in the next section.

Measurement Results

Table 5.3: 65nm Testchip Results for HCI Characterization

	Time Required to Flip the Output					
Stressed Device Width (nm)	**Configuration 1**		**Configuration 2**		**Configuration 3**	
Without Grouping	**Mean (hour)**	**std (hour)**	**Mean (hour)**	**std (hour)**	**Mean (hour)**	**std (hour)**
200	86.76	42.79	1.19	0.65	7.06	2.64
400	101.79	41.93	1.2	0.62	7.85	2.48
600	117.63	39.26	1.42	0.8	9.0	2.86
With a Grouping of 3	**Mean (hour)**	**std (hour)**	**Mean (hour)**	**std (hour)**	**Mean (hour)**	**std (hour)**
200	80.52	34.42	1.2	0.6	7.15	2.46
400	102.36	41.54	1.26	0.49	7.84	1.98
600	126.85	35.98	1.4	0.58	8.09	1.97

Some exemplar test results for three different current and voltage drop configuration for single and multiple legs are given in Table 5.3. The first configuration is 92μA and 1.67V per leg, the second configuration is 94.6μA and 2.05V per leg, and the third configuration is 167μA and 1.68V per leg for HCI stress current and HCI stress voltage over the stressed devices. The results are given for the BAEs with an initial input offset of 160mV.

As can be seen from the results in Table 5.3, for the same current density and the same stress voltage, the stress time required to flip the output of BAE increases with increasing device width. Furthermore, for the same current density and same device width, the stress time required to flip

the output of BAE increases with decreasing voltage that the device sees. Also, for the similar voltage that the device sees and same device width, the stress time required to flip the output of BAE increases with decreasing current density.

The flip time of the BAEs does show some variability. One method of mitigating the effects of variation would be to employ a majority voting scheme. In Table 5.3, the top part of the results show the stress time required to flip an output of a single BAE. The bottom part of the table shows the results for a group of 3 BAEs acting as a single BAE, and the stress time is measured by the majority voting of the 3 BAEs.

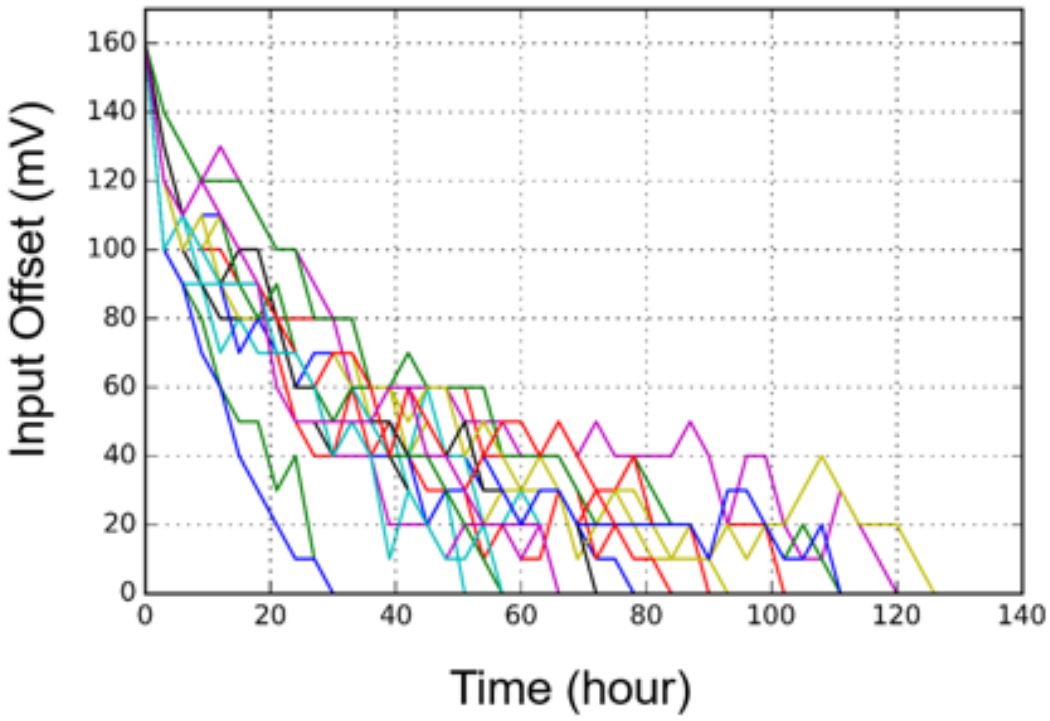


Figure 5.9: Input offset vs time plot for configuration 1 with 160mV initial offset and 200nm device width. With increasing HCI stress time, the input offset decreases. When the input offset reaches 0, the output of the BAE flips.

Figure 5.9 shows input offset change with time of configuration 1 with 160mV initial offset for 200nm devices. As can be seen, after a certain point of offset shift, with increasing stress time the variation in offset shift increases. Therefore, to reduce the variation in the time required

to achieve a certain amount of threshold voltage shift, either a configuration that can achieve the shift in a shorter time or a configuration that requires a smaller shift should be chosen.

Figure 5.10 shows the mean flip time for 2.25V, 2.3V, 2.36V and 2.41V HCI stress voltages over the stressed device, and 50mV, 100mV, 150mV and 200mV initial input offset values while the HCI stress current is set at 224μA. When the HCI stress current and stress voltage are set constant, with increasing initial input offset, the mean time to flip increases. For the same initial input offset and same HCI stress current, with increasing HCI stress voltage, the mean time to flip decreases.

Depending on the desired stress time or desired threshold voltage shift amount, the configuration can be chosen accordingly from these results. In addition, using the presented silicon measurements the intermediate points for HCI characterization can be extrapolated.

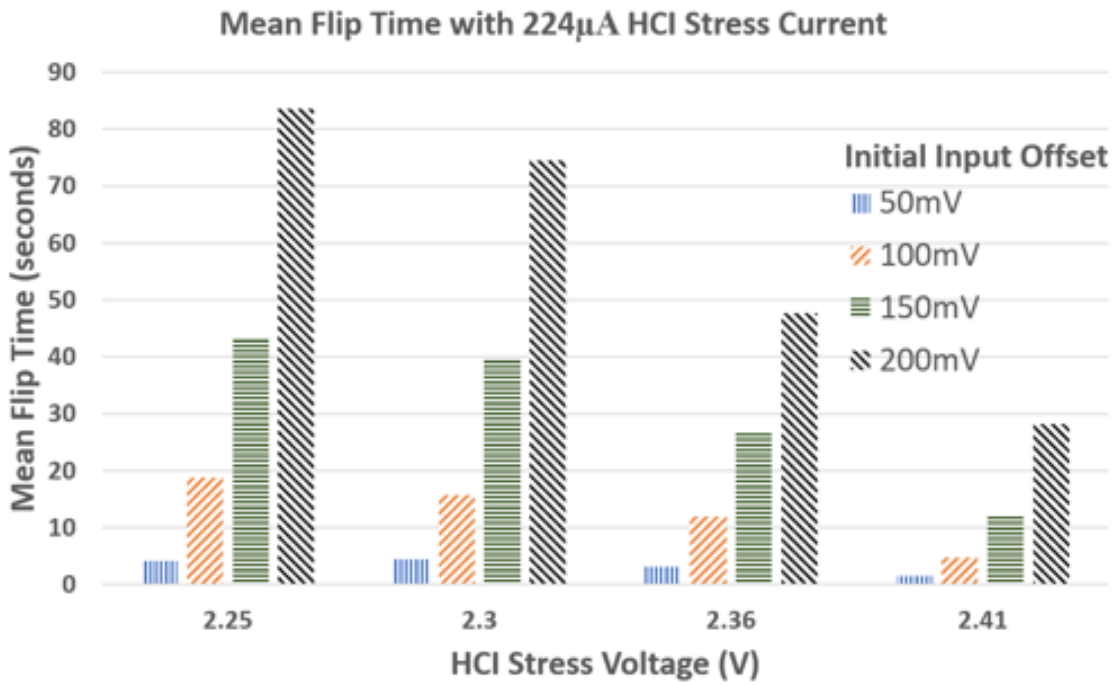


Figure 5.10: Mean flip time with 224μA HCI stress current for different HCI stress voltages and different initial input offset values. For the same HCI stress voltage and stress current, with increasing initial input offset, the mean time to flip increases. For the same initial input offset, with increasing HCI stress voltage, the mean time to flip decreases.

5.2 Testchip in a 28nm CMOS Process

5.2.1 Overview

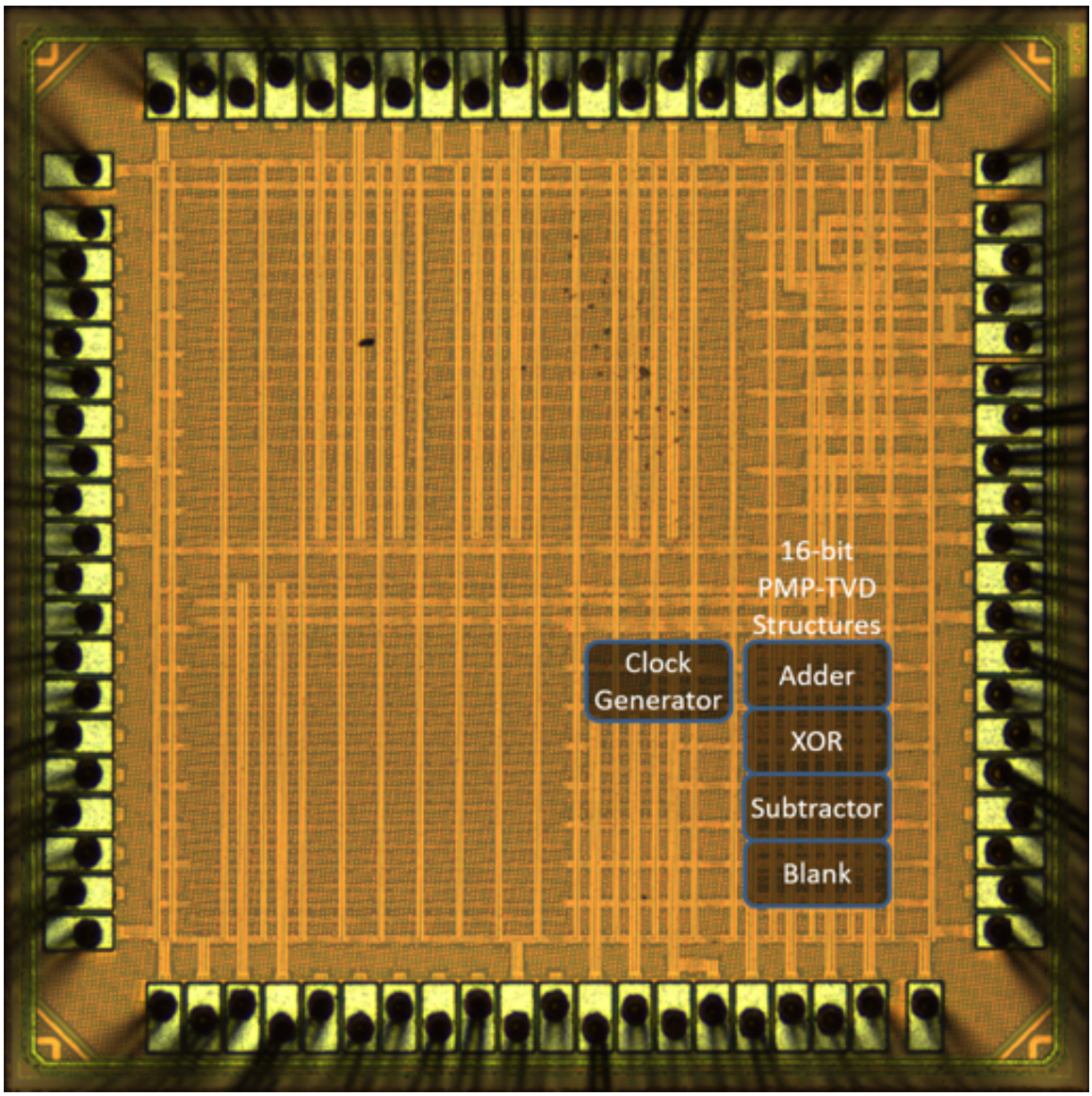


Figure 5.11: Die shot of the second prototype testchip. 16-bit TVD adder, subtractor, XOR, and blank structures are highlighted.

The second prototype testchip is implemented in an industrial 28nm CMOS process with 9-metal layers. The testchip die shot can be seen in Figure 5.11. The die area is 1.152mm by 1.152mm and it has 80 I/O pads along the periphery. Table 5.4 summarizes the technology and

prototype testchip features.

Table 5.4: Technology and Features of the Second Prototype Testchip

Technology	28nm CMOS with 9-metal layers
FO4 in TTLH	22.3ps
Supply Voltage	0.9V
Chip Area	1.327mm^2 (1.152mm x 1.152mm)
Number of I/O Pads	80
Core Area of the 16-bit PMP-TVD Structure	2183.26μm^2 (30.92μm x 70.61μm)
Area of the 16-bit PMP-TVD Structure Including Test Structures	6897.15μm^2 (58.5μm x 117.9μm)

On the testchip, PMP-TVD structures have four different voltage domains, and each of them has their own power grid. For the voltage domains, HCI stress related ones are at 3V and the rest are supplying 0.9V to the structures. Each PMP-TVD structure has its own test infrastructure, and these test circuitry have separate supply voltages to enable measurements at the core with different voltage levels.

The testchip in Figure 5.11 contains four 16-bit PMP-TVD structures: a carry select adder, a subtractor, a XOR, and a blank structure. Each structure has the exact same layout other than the threshold voltage doping masks. All four structures are created using 2- and 3- input PMP-TVD gates.

Just like the first prototype testchip, the structures on the second testchip are clocked by using an on-chip ring oscillator based clock generator with a wide-range of frequency configuration. In the clocking infrastructure, there are four ring oscillators with four different base clock frequencies (i.e., 2.46GHz, 3.17GHz, 3.83GHz, and 5.34GHz). The voltage supply of these ring oscillators are separate than the rest of the infrastructure so that desired clock frequencies can be generated. These generated clocks are fed into a twelve-step divide-by-two stages to generate wide-range of clock frequency options (i.e., 600kHz to 5.34GHz at nominal voltage supply). In

addition, in case of an issue with the on-chip ring oscillators, a pad that can take an off-chip generated clock signal is fed into the clocking infrastructure. A 14:1 MUX stage selects the configured clock signal from the generated wide-range of clock signals, and then the selected signal is distributed to all of the structures' own clock distribution network. The distributed clock signal is also divided by 4096 times and then fed to a pad to measure the operating frequency of the chip.

5.2.2 PMP-TVD Structures

The PMP-TVD structures on the testchip have the exact same layouts other than their threshold voltage doping layer masks. Depending on the functionality of the gates, the doping layers are different. Since all four PMP-TVD structures have an almost exact layout, as an example, the structure and the layout of the 16-bit PMP-TVD carry select adder is shown in Figures 5.12 and 5.12 . The dimensions of the individual 16-bit PMP-TVD structures are 30.92μm x 70.61μm. Including the test structures, the dimensions are 118μm by 59μm. The total dimensions of the all four structures including the test structures are 120μm by 256μm.

Just like the first prototype testchip, the PMP-TVD structures are split into two phases. For the first half, there are sum and carry generators built by using 2- and 3- input PMP-TVD gates. For the second half, there are carry selection MUXes. In between the halves and at the end of the structure, there are standard CMOS latches to capture the data. Similar to the 16-bit TVD adder in the first testchip, the 16-bit PMP-TVD adder in the second testchip is divided into 4-bit full adder sections. The lowest four bits are added up assuming the carry-in as 0, and the rest of the bits are summed up for carry-in as both 0 and 1. After that, the generated sum and carry bits are latched. Then in the second phase, the correct sum and carry bits are selected by the MUXes and the latches at the end capture the correct sixteen sum bits and the carry bit.

To test the PMP-TVD structures, there are 8-deep scan-enabled input and output shift reg-

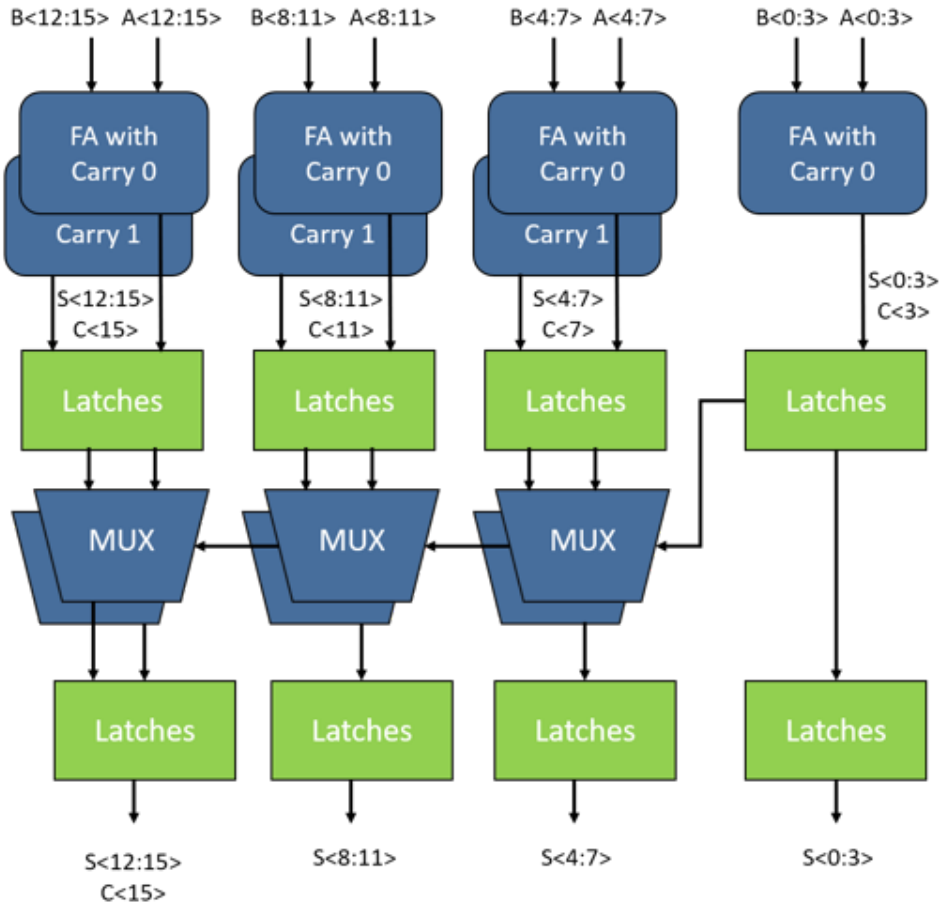


Figure 5.12: Structure of the 16-bit PMP-TVD carry select adder. When clock is high, the full adders evaluate, and generate the sum and carry bits for carry in being 0 and 1, then these bits are latched. When clock is low, according to the carry bits the true sum and carry bits are MUXed and latched.

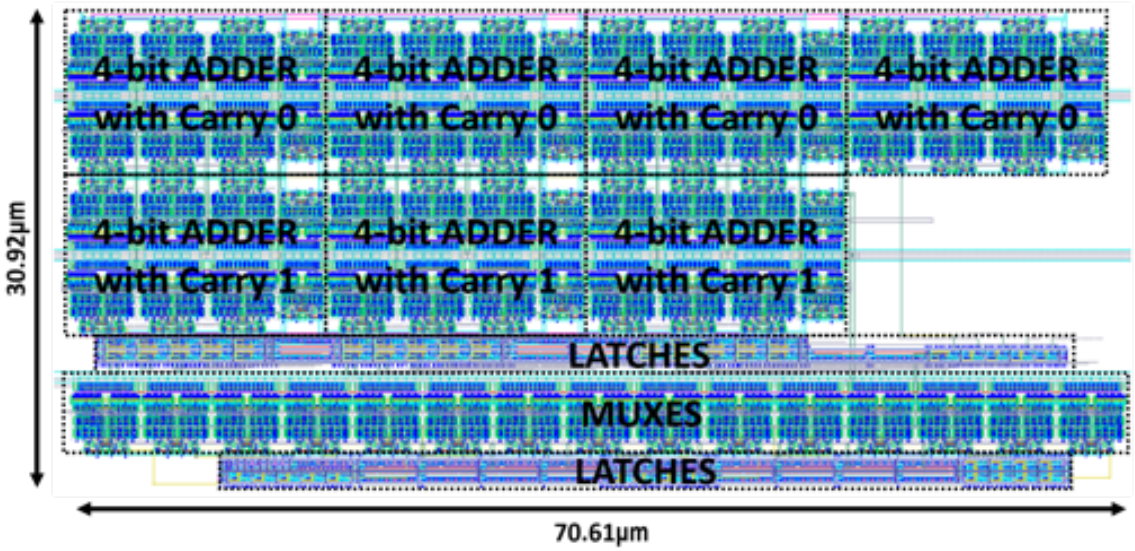


Figure 5.13: Layout of the 16-bit PMP-TVD carry select adder. When clock is high, the full adders evaluate, and generate the sum and carry bits for carry in being 0 and 1, then these bits are latched. When clock is low, according to the carry bits the true sum and carry bits are MUXed and latched.

isters. Input shift registers can hold eight different inputs which are loaded during the scan in. During the normal operation, input shift registers operate in a circular manner, where the stored eight inputs rotate and continuous input is supplied. The output shift registers capture the most current eight outputs. Since the PMP-TVD is a dual-rail based logic style, the inputs of the gates require both the true and complementary versions. Therefore, the input shift registers that are connected to adder structure generates both the true and complementary versions, while the other input shift registers are single-ended. The output shift registers only capture the true version of the output and all of them are single-ended. In addition to the input and output shift registers, there are HCI configuration registers. These registers hold the data that decides which PMP-TVD gate to HCI stress into which functionality during HCI stress. During normal operation or during HCI stress, these registers hold their data constant.

Test Methodology

The PMP-TVD structures are tested at 0.9V nominal VDD and the HCI stress voltage is set at 3V. All the performance and HCI stress tests are done at room temperature. Similar to the first testchip, the tests are applied using randomly generated test vectors in the input registers. After the functionalities of the structures are confirmed, performance tests are applied at speed to measure frequency and power. For the HCI stress tests, the same tests as the first testchip are applied. The preprogrammed structures are HCI stressed to boost the performance and reverse stressed to change the functionality. The blank structure is HCI stressed to program a functionality into it. On top of these HCI tests, after a functionality is programmed into the blank structure, reprogrammability is explored by reversing the HCI effects and then applying the HCI stress again to write the same or a different functionality.

Measurement Results

A summary of the silicon results for the 16-bit PMP-TVD preprogrammed structures before HCI stress and the 16-bit PMP-TVD blank structure after adder functionality is programmed in is shown in Table 5.5. The results shown are between 18-20% slower than the simulations performed on post-layout extracted views. However, the discrepancy between the simulation and silicon results are due to the testchips being on a slow corner. This founding is also confirmed with the on-chip ring oscillators, where their silicon performance is also 18-20% slower compared to the simulation results.

Performance of the Preprogrammed Structures

The 16-bit PMP-TVD preprogrammed adder, subtractor, and XOR operates at 401MHz-1.18GHz, 419MHz-1.16GHz, and 419MHz-1.19MHz, respectively, at a power supply range of 0.7V to 1.1V. The power consumption of the structures are between 0.582-4.33mW, 0.607-4.05mW, and

Table 5.5: 28nm Testchip Results for PMP-TVD Structures

	16-bit PMP-TVD Preprogrammed			16-bit PMP-TVD Blank
	Adder	**Subtractor**	**XOR**	**Programmed into Adder**
Area	6897.15 μm^2 (Core: 2183.26 μm^2)			
Frequency at 0.9V	790MHz	819MHz	869MHz	731MHz
Power at 0.9V	1.9mW	1.87mW	1.77mW	1.9mW
Leakage at 0.9V	0.067mW	0.0677mW	0.0669mW	0.0762mW

0.516-3.67mW for the same power supply range. The shmoo plots of the 16-bit PMP-TVD adder, subtractor, and XOR at room temperature are shown in Figures 5.14, 5.15, and 5.16. As can be seen from the figures, the performance of the structures are pretty close to each other at the same supply voltage levels, and the minuscule difference between the results can be interpreted as a measurement offset.

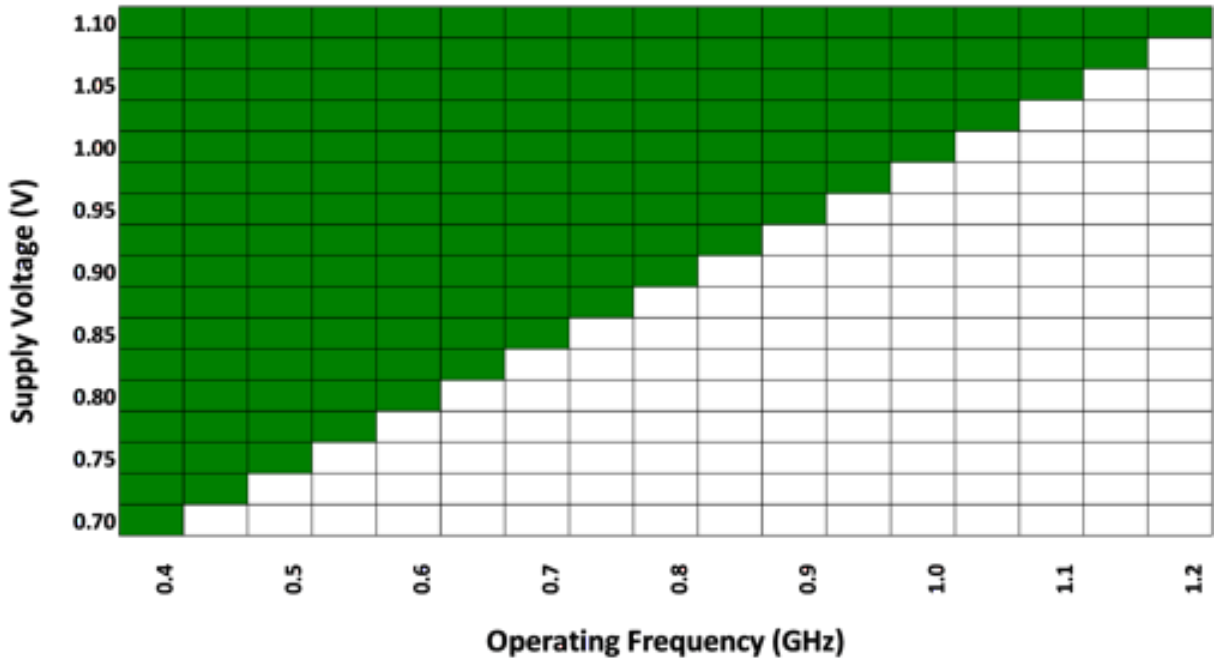


Figure 5.14: Shmoo plot at room temperature for the 16-bit PMP-TVD preprogrammed adder.

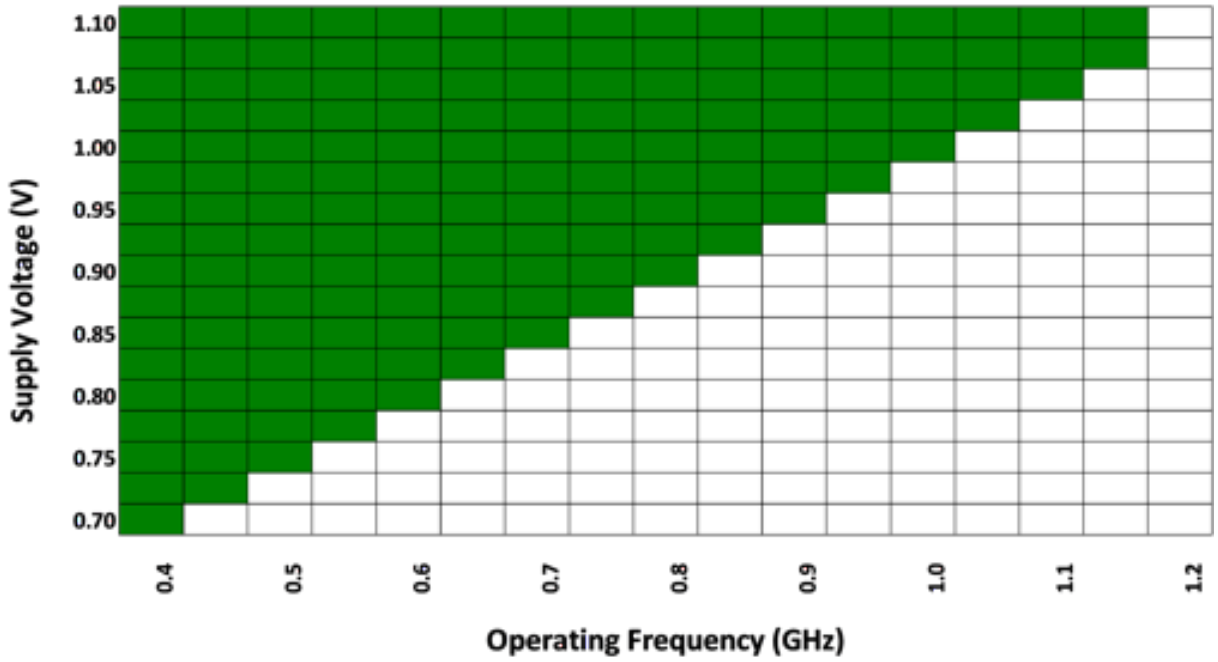


Figure 5.15: Shmoo plot at room temperature for the 16-bit PMP-TVD preprogrammed subtractor.

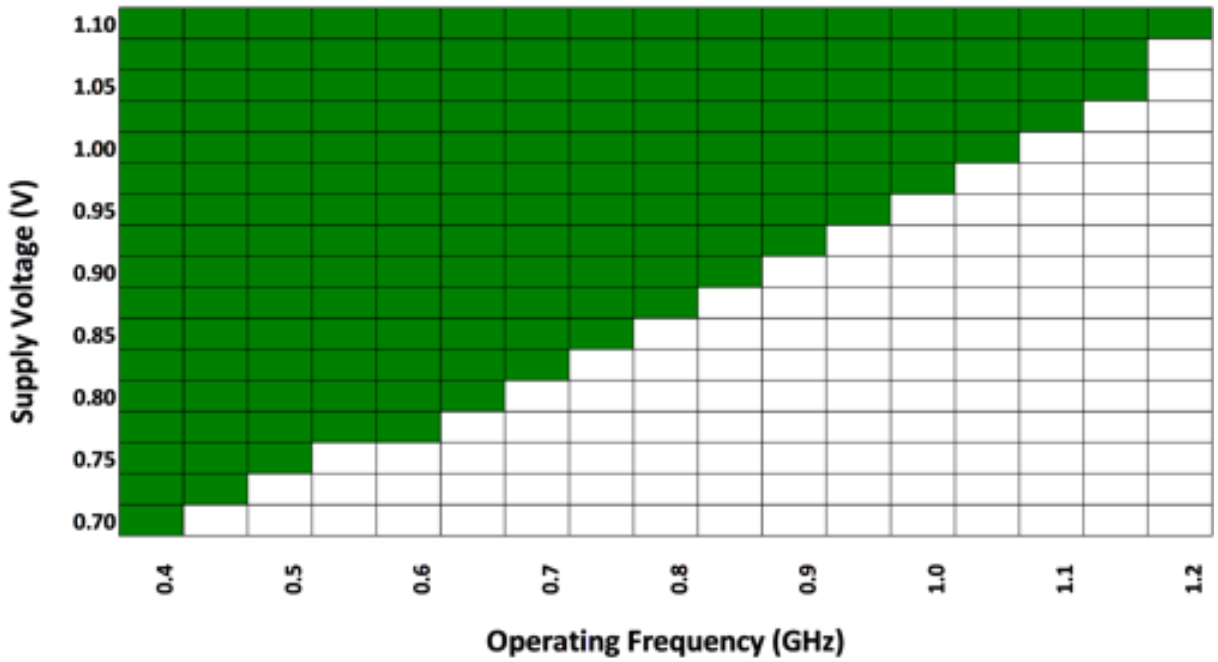


Figure 5.16: Shmoo plot at room temperature for the 16-bit PMP-TVD preprogrammed XOR.

HCI Programming and Permanence

After getting all the initial performance of the preprogrammed structures, we have explored HCI reprogramming. Just like the first testchip, we have applied HCI stress at 3V at room temperature. The only difference is that the core structures are powered at 0.9V nominal VDD.

After 10 minutes of HCI stress, we are able to erase the functionality of the preprogrammed structure by applying the HCI stress to program in a different functionality. However, continuous HCI stress did not yield in the new functionality being programmed in. Furthermore, when we tried to increase the performance of the preprogrammed structures by applying the HCI stress, we were not able to see any enhancement in the performance. After the initial exploratory HCI stress tests, we have tried HCI stress with stress voltage ranging from 1.8-4V and stress time ranging from seconds to hours. Above 3.5V stress voltage, the I/O pads could not handle the voltage level and the circuitry becomes damaged. However, for the remaining stress voltage range, we were still not able to see either performance increment or functionality changing. Although we were able to increase the performance and change the functionality of preprogrammed PMP-TVD structures in the first testchip, the inability to change the structures could be caused by the testchips being in an off-corner.

On the other hand, we successfully programmed a functionality into the blank structures when we applied 3V HCI stress. For the blank structures, HCI stress ranging from 2.09-3V are applied to explore the programming time. The programming time is close to an hour on the lower bound and is in tens of seconds on the upper bound of HCI stress range. To reduce the testing time and programming time, 3V is chosen as the HCI stress level. Figure 5.17 shows a 16-bit blank PMP-TVD structure under 3V HCI stress to program in an adder functionality. The HCI stress is administered in steps of 20 seconds. As can be seen, initially the structure does not have any functionality at all. However, after just 20 seconds of stress, the structure is sufficiently programmed to function as an adder at an operating frequency of 626MHz. With each 20 seconds of HCI stress step, the performance of the structure increases. After 80 seconds

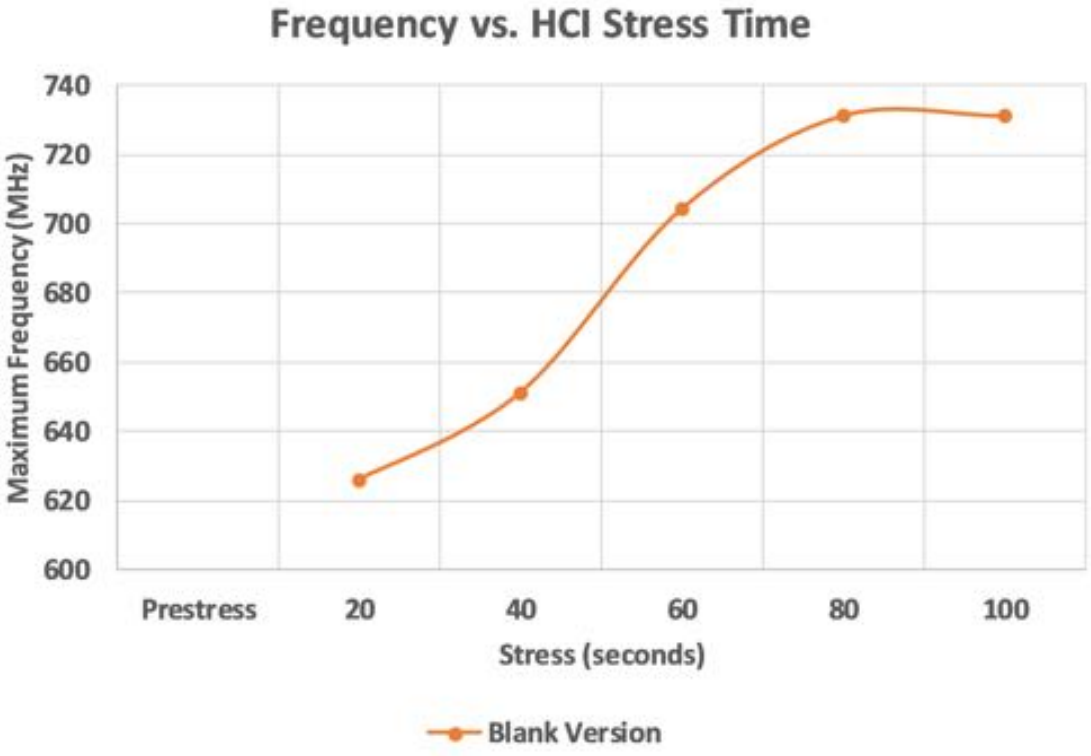


Figure 5.17: Frequency vs. HCI stress time plot of 16-bit blank PMP-TVD adder at 0.9V and room temperature. HCI stress for an adder functionality is applied at 3V at room temperature in 20 seconds intervals.

of stress, the structure reaches 731MHz at nominal 0.9V VDD. However, further stress does not increase the performance of the structure, as the performance plateaus and stays around 730MHz operating frequency. At this operation point, the structure consumes 1.9mW power where the leakage is 4% of it at nominal 0.9V VDD and room temperature.

After successfully programming a functionality into a blank structure, we have explored the permanence of the HCI programming. Similar to the tests with first testchips, we baked the second testchips. This time we have baked them at 130°C for 72 hours (in three 24 hour steps) in a temperature chamber. After the initial 24 hours of baking, the programmed blank structure's maximum frequency at nominal 0.9 VDD and room temperature showed a 3.5% decrease from 731MHz to 705MHz. However, after the second and third 24 hours of baking under 130°C, the performance of the structure remained same. Just like the first testchip, the structure showed a

slight reversal from the baking, but then with further baking it showed a plateauing and program retention under high temperature.

In addition to these tests, we have also explored reprogrammability by trying to reverse the effects of HCI and then programming a new functionality. In the first testchips, the designed and implemented PMP-TVD structures did not have control on the gate voltage of the stressed NMOSes. However, as mentioned in Chapter 4, if we can reverse the effects of trapped charges similar to [45], [46], and [47], we can remove the programmed functionality in the field and then put a different functionality using HCI stress again. Therefore, in the second testchip, we have implemented PMP-TVD gates with the ability to control the gate voltage of the stressed NMOS devices.

To reverse the effects of HCI, we have applied the high HCI voltage while turning off the stressed NMOS devices. Hence, the stressed devices with increased threshold voltage levels will endure high voltage bias at their drain while the channel is not formed. According to the [45], [46], and [47], HCI reversing is more effective if the stress voltage is higher during the erasing process compared to the programming process. To achieve a higher stress voltage over the drain and source of the stressed NMOSes, we can either increase the voltage at the drain of the stressed NMOS by increasing the applied HCI stress voltage, or reduce the voltage at the source of the stressed NMOS by reducing the VSS of the stress devices lower than the VSS of the rest of the circuitry. However, due to the I/O pads we have been supplied by the foundry, we could not neither supply a voltage level higher than a certain level nor supply a voltage level lower than VSS. Therefore, to reverse the effects of HCI, we have applied the same HCI stress voltage that is used for the programming.

For the reprogrammability exploration, first, we have programmed in a functionality into the blank structure using 3V HCI stress voltage at room temperature. After, we have successfully erased the functionality by reversing the effects of HCI with applying 3V HCI stress while the

stressed NMOS devices are off at room temperature. The erasing process took 10 minutes after the initial HCI programming of 80 seconds. After erasing the functionality from the blank structure, a different functionality is programmed using 3V HCI stress. The second programming of the structure has an increased programming time of one hour. After the second programming, the erase process took 10 minutes. However, after the second erase, a third programming could not have been achieved. These results show that, using the same HCI stress voltage for programming and erasing a functionality, 100% reversal of the HCI effects is not achievable. However, according to Khan et al., even with a higher erasing voltage level than the programming voltage level, the effects of charge trapping cannot be fully reversed. Furthermore, consecutive charge entrapment cannot reach the same performance as the initial one, because the charge entrapment reaches saturation quicker [47].

5.3 Summary

In this chapter, we discussed the details of our two prototype testchips which consist of structures built by using TVD and PMP-TVD gates, and HCI characterization array. We have used several different 4-bit and 16-bit structures to benchmark the characteristics of the TVD and PMP-TVD logic families. We have evaluated power consumption, performance, and area of the structures. We have run multiple tests with multiple different variables to present certain data points in the characterization of HCI. In addition, we have explored programming and erasing functionality in PMP-TVD gates using HCI.

In summary, we demonstrated that structures can be built using TVD and PMP-TVD logic families against reverse engineering and untrusted fabrication. Although TVD structures have fixed functionalities, the PMP-TVD structures can be programmed, erased and/or reprogrammed with different functionalities in the field. In addition, using the HCI characterization gathered by the silicon results, we can trade-off between the programming time and the area, performance,

and power consumption of the gates.

Chapter 6

Conclusions and Future Work

6.1 Summary

Myriad of security vulnerabilities can be exposed via the reverse engineering of the integrated circuits contained in electronics systems. The goal of IC reverse engineering is to uncover the functionality and internal structure (e.g., gate netlist, circuit schematic, layout, manufacturing process details) of the chip via techniques such as depackaging/delayering, high-resolution imaging, probing, and side-channel examination. With this knowledge, an attacker can more efficiently mount various attacks (e.g., fault injection, side-channel), clone/counterfeit the design possibly with hardware Trojans inserted, and discover trade secrets including proprietary algorithms, hard-coded keys and instruction sequences. To combat reverse engineering, researchers have proposed a number of countermeasures including gate camouflaging wherein an attacker cannot discern the functionality of a particular logic gate based solely on its observable physical characteristics.

In this work, we provided background on hardware reverse engineering countermeasures and discussed some example of effective countermeasures. Next, we explained the disadvantages

of the current solutions and proposed a secure camouflaging method, threshold voltage defined (TVD) logic, against reverse engineering. However, even if a design is protected against reverse engineering, the design can be compromised in the supply chain, obviating the need for later reverse engineering. Therefore, to overcome this issue, we proposed post-manufacturing programmed threshold voltage defined (PMP-TVD) logic. PMP-TVD is a secure camouflaging method that can remove the critical design information from the design database by introducing a reprogrammability feature. PMP-TVD is a logic gate topology that uses different threshold voltage transistors, but with identical layouts, to determine the logic gate function. The camouflaging technique does not rely on limited delayering and imaging resolution, does not require any additional process steps or masks, and is fully compatible with modern CMOS process technology. It has a reprogrammability feature that uses HCI phenomenon to set the functionality, change the functionality, or remove the functionality post-production. To evaluate the overhead of PMP-TVD structures, we have 100% camouflaged a subset of ISCAS85 benchmark circuits with PMP-TVD, and compared them against standard cell synthesized versions. For camouflaging, we have compared two different methods. In the first method, we replaced all the gates with their PMP-TVD equivalents, and in the second method we created a functionally identical circuit with LUTs and used PMP-TVD gates instead of LUTs. Last, we showed the differences between the methods for delay, power, and area overheads. In addition to the secure camouflaging methods, we also proposed a structure to characterize HCI, which is used in PMP-TVD structures.

Silicon results from our prototype testchips prove the feasibility and applicability of TVD and PMP-TVD camouflaging. We showed the viability of camouflaging using PMP-TVD gates in 65nm and 28nm CMOS processes. In addition, we gathered HCI characterization data in the 65nm CMOS process. Moreover, we explored HCI phenomenon to reprogram and erase PMP-TVD gate functionalities. Despite the overhead in area, power, and performance, we showed that there are significant security benefits of PMP-TVD camouflaging compared to existing coun-

termeasures. Therefore, PMP-TVD is a very promising secure camouflaging method that can provide both concealment of critical IP from the foundry and high resistance against reverse engineering.

6.2 Conclusions

Countermeasures to mitigate reverse engineering and untrusted fabrication incur either delay, power, and area overheads or additional manufacturing costs. If delay, power, and area overheads are not desired in a design, then the cost of security will be either in using non-standard process structures or having a secure memory. While the use of specialized technologies (e.g., 3D integrated non-volatile memory) or elaborate fabrication flows (e.g., split manufacturing) could mitigate the security threats, the cost and complexity of such solutions render them infeasible for many applications. Moreover, some methods might require additional secure memory elements. When evaluating these methods, the evaluation of the topology should not be confined to itself, but also other factors that are necessary to secure the design methodology should be considered.

Although PMP-TVD gates incur delay, power, and area overheads, the structures they replace are only a small percentage of an IC. Therefore, the effective overheads incurred by these security methods are smaller overall. Using CMOS logic process compatible methods, such as PMP-TVD, which provides strong security with configurability and erase on tamper features, may prove to be a cost-effective solution for protecting secure IP against reverse engineering and untrusted fabrication.

6.3 Future Research Directions

The ideas and contributions presented in this work are open to further exploration, improvement, and new uses of applications in other domains. The reliability and applicability of HCI

is the essence of PMP-TVD logic. We demonstrated that HCI can be used to reprogram and erase functionalities in PMP-TVD gates in 65nm and 28nm processes. Although the effects of HCI are shown in more advanced technology nodes (i.e., sub-28nm, FinFETs) [69][70][71], the applicability of HCI for PMP-TVD structures in those technology nodes is yet to be tested.

Additionally, using HCI in a favorable way is not limited to PMP-TVD logic. HCI can be used in different applications such as hiding the configuration for LUTs. Then these LUTs can be used for camouflaging a structure as well. This method's application is not limited to camouflaging. For example, the bitstream of an FPGA can be protected through one-time pad encryption using die-specific responses generated by HCI-Enabled Sense Amplifier Physical Unclonable Functions (HCI-SA PUF) [44][53].

One of the main challenges in designing the PMP-TVD is reducing the delay, power, and area overheads of the logic family. Due to the limitation on the size of the stressed NMOS device and the number of stacked NMOSes on the pull-down network, the overheads of PMP-TVD are larger than some of the current countermeasures. One way to tackle this problem is to simplify the structure by branching out the pull-down network. A similar method is applied on TVD gates to reduce the power and area overheads by 42% and 26%, respectively [72]. After the simplification of PMP-TVD logic, a much more efficient PMP-TVD gate with more than 3 inputs can be designed. Effectively, this will make PMP-TVD camouflaging more effective since using camouflaged gates with a higher number of inputs increases the efficiency in camouflaging a structure and increases the resiliency of the structure against attacks [55].

However, reducing the overheads of the PMP-TVD logic family might not be enough and they can still be too high for certain design choices. In these cases, the overhead problem can be approached from a different angle. Instead of reducing the overheads of PMP-TVD logic family, new architectures of secure elements can be explored to reduce the size of structures that require security. If the percentage of the IC that needs to be secured gets smaller, the overall overhead

caused by camouflaging with PMP-TVD logic would also get smaller and would not stand out.

Appendix A

Overhead Analysis Simulation Results

Table A.1: Overhead Comparison Results for c432

Overhead Compared to Area Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	80	2.88x	17.75x	31.22x
LUT-to-gate PMP-TVD Replaced	81	2.64x	14.32x	32.47x
LUT-to-gate PMP-TVD Replaced (with Buffers)	243	2.36x	18.07x	36.02x
Overhead Compared to Delay Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	80	11.84x	4.74x	4.12x
LUT-to-gate PMP-TVD Replaced	81	10.86x	3.82x	4.28x
LUT-to-gate PMP-TVD Replaced (with Buffers)	243	9.70x	4.82x	4.75x

Table A.2: Overhead Comparison Results for c1908

Overhead Compared to Area Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	167	3.48x	7.93x	22.24x
LUT-to-gate PMP-TVD Replaced	143	2.47x	7.16x	20.54x
LUT-to-gate PMP-TVD Replaced (with Buffers)	429	2.11x	8.91x	22.84x
Overhead Compared to Delay Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	167	9.44x	2.30x	3.44x
LUT-to-gate PMP-TVD Replaced	143	6.70x	2.08x	3.17x
LUT-to-gate PMP-TVD Replaced (with Buffers)	429	5.71x	2.59x	3.53x

Table A.3: Overhead Comparison Results for c3540

Overhead Compared to Area Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	539	3.54x	16.99x	29.37x
LUT-to-gate PMP-TVD Replaced	501	2.66x	16.74x	29.23x
LUT-to-gate PMP-TVD Replaced (with Buffers)	1503	2.08x	20.82x	32.47x
Overhead Compared to Delay Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	539	11.80x	5.89x	7.47x
LUT-to-gate PMP-TVD Replaced	501	8.89x	5.80x	7.43x
LUT-to-gate PMP-TVD Replaced (with Buffers)	1503	6.94x	7.22x	8.26x

Table A.4: Overhead Comparison Results for c7552

Overhead Compared to Area Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	616	3.67x	9.18x	22.05x
LUT-to-gate PMP-TVD Replaced	535	2.40x	8.33x	20.85x
LUT-to-gate PMP-TVD Replaced (with Buffers)	1605	1.95x	10.22x	23.16x
Overhead Compared to Delay Optimized Standard Cell Synthesized				
	Number of Gates	**Delay**	**Power**	**Area**
Gate-to-gate PMP-TVD Replaced	616	20.7x	3.75x	5.7x
LUT-to-gate PMP-TVD Replaced	535	13.55x	3.40x	5.39x
LUT-to-gate PMP-TVD Replaced (with Buffers)	1605	11.00x	4.17x	5.99x

Table A.5: Overhead of Place and Route Step

Designs	Number of Gates	Delay (ps)	Power (μW)	Area (μm^2)
c432				
Area Optimized	86	862	11.7	45
Area Optimized Post-PnR	87	1114	17.7	49
Overhead	1.01x	1.29x	1.51x	1.09x
Delay Optimized	220	210	43.8	341
Delay Optimized Post-PnR	237	349	61.1	354
Overhead	1.08x	1.66x	1.39x	1.04x
c1908				
Area Optimized	174	650	44.94	122.5
Area Optimized Post-PnR	432	901	60.72	203.87
Overhead	2.48x	1.39x	1.35x	1.66x
Delay Optimized	454	240	154.42	791.66
Delay Optimized Post-PnR	509	418	189.4	873.56
Overhead	1.12x	1.74x	1.23x	1.1x
c3540				
Area Optimized	569	997	63.3	304.3
Area Optimized Post-PnR	568	1274	92.65	310.84
Overhead	1.00x	1.28x	1.46x	1.02x
Delay Optimized	880	299	182.5	1195.27
Delay Optimized Post-PnR	930	532	331.27	1269.2
Overhead	1.06x	1.78x	1.82x	1.06x
c7552				
Area Optimized	665	1183	150.57	456.3
Area Optimized Post-PnR	664	1634	186.57	464.2
Overhead	1.00x	1.38x	1.24x	1.02x
Delay Optimized	1096	210	368.33	1762.7
Delay Optimized Post-PnR	1315	401	547.75	1907.9
Overhead	1.20x	1.91x	1.49x	1.08x

Appendix B

Test Infrastructure

The testchips are packaged in a ceramic PGA package and tested on a custom PCB shown in Figure B.1. The level shifters reduce the 5V signals supplied by the Ni-DAQ to the voltage level that the testchip pads require. The different voltage domains are supplied by the BNC connectors from the Agilent power supplies. The operating clock frequency of the testchip is divided by 4096 times and supplied out using the SMA connector and fed to an Agilent 548559A digital sampling oscilloscope. For the communication between the PC and the PCB, a Ni-DAQ 6259 board is used. The Ni-DAQ board is connected to PCB using the highlighted I/O port in the figure. The test software is written in C, and the test input vector generation, test output data processing, and test automation are done in Python. The temperature stress tests are done in a TestEquity 107 Benchtop Temperature Chamber.

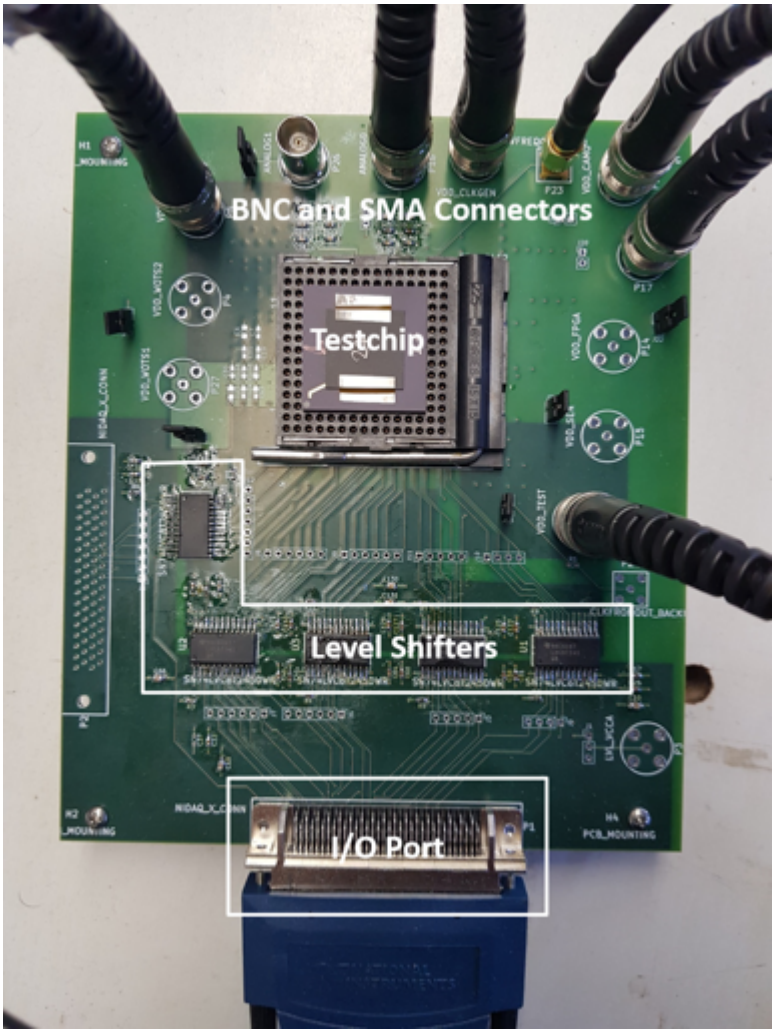


Figure B.1: A custom printed circuit board (PCB) to test the second testchip.

Bibliography

[1] N. E. C. Akkaya, B. Erbagci, and K. Mai. Combatting IC Counterfeiting Using Secure Chip Odometers. In *2017 IEEE International Electron Devices Meeting (IEDM)*, pages 39.5.1–39.5.4, Dec 2017. doi: 10.1109/IEDM.2017.8268523. (document), 4.3, 4.4.1, 4.4.1, 4.12, 4.13, 4.4.1, 4.14, 5.1

[2] N. E. C. Akkaya, B. Erbagci, and K. Mai. Secure Chip Odometers Using Intentional Controlled Aging. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 111–117, April 2018. doi: 10.1109/HST.2018.8383898. (document), 4.3, 4.4.1, 4.4.1, 4.12, 4.13, 4.4.1, 4.14, 5.1

[3] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu, and L. Pileggi. Building Trusted ICs Using Split Fabrication. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 1–6, May 2014. doi: 10.1109/HST.2014.6855559. 1.2, 4.7

[4] K. Bennett. Newegg Selling Fake Intel CPUs. URL `http://www.hardocp.com/article/2010/03/05/newegg_selling_fake_intel_cpus`. `http://www.hardocp.com/article/2010/03/05/newegg_selling_fake_intel_cpus/`. 1.3

[5] US Senate Armed Service Committee. Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain. 1.3

[6] US General Accounting Office. DOD Supply Chain Suspect Counterfeit Electronic

Parts Can Be Found on Internet Purchasing Platforms. URL http://www.gao.gov/assets/590/588736.pdf. 1.3

[7] Sergei Skorobogatov and Christopher Woods. Breakthrough Silicon Scanning Discovers Backdoor in Military Chip. In *CHES*, 2012. 1.3

[8] M. Tehranipoor and F. Koushanfar. A Survey of Hardware Trojan Taxonomy and Detection. *Design Test of Computers*, 2010. 1.3

[9] Chipworks. Intel's 22-nm Tri-gate Transistors Exposed. URL http://www.chipworks.com/blog/technologyblog/2012/04/23/intels-22-nm-trigate-transistors-exposed/. 1.3, 2, 2.1.3

[10] TAEUS. Reverse Engineering. URL https://taeus.com/reverse-engineering/. https://taeus.com/reverse-engineering/. 1.3

[11] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai. A Secure Camouflaged Threshold Voltage Defined Logic Family. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 229–235, May 2016. doi: 10.1109/HST.2016.7495587. 1.4, 2, 2.1.3, 2.1.4, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 4, 4.2, 4.1, 4.5.5, 4.6

[12] Mudit Bhargava and Ken Mai. A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013*, pages 90–106, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-40349-1. 1.4, 4.1.1, 4.2

[13] M. Bhargava, K. Sheikh, and K. Mai. Robust True Random Number Generator Using Hot-carrier Injection Balanced Metastable Sense Amplifiers. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 7–13, May 2015. doi: 10.1109/HST.2015.7140228. 1.4

[14] N. E. C. Akkaya, B. Erbagci, and K. Mai. A Secure Camouflaged Logic Family Using

Post-manufacturing Programming with a 3.6ghz Adder Prototype in 65nm CMOS at 1V Nominal VDD. In *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*, pages 128–130, Feb 2018. doi: 10.1109/ISSCC.2018.8310217. 1.4, 4.3, 4.3, 4.1, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8

[15] R. Torrance and D. James. The State-of-the-art in Semiconductor Reverse Engineering. In *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 333–338, June 2011. 2

[16] Yousra M. Alkabani and Farinaz Koushanfar. Active hardware metering for intellectual property protection and security. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, SS'07, pages 20:1–20:16, Berkeley, CA, USA, 2007. USENIX Association. ISBN 111-333-5555-77-9. URL `http://dl.acm.org/citation.cfm?id=1362903.1362923`. 2

[17] R. S. Chakraborty and S. Bhunia. HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 28(10):1493–1502, Oct 2009. ISSN 0278-0070. doi: 10.1109/TCAD.2009.2028166. 2, 4.5.1

[18] Lap Wai Chow, James P. Baukus, Bryan J. Wang, and Ronald P. Cocchi. Camouflaging a Standard Cell Based Integrated Circuit, 2012. URL `https://patents.google.com/patent/US8151235B2`. 2

[19] Mark C. Hansen et al. Unveiling the ISCAS-85 Benchmarks: A Case Study in Reverse Engineering. *Design Test of Computers*, 1999. 2, 4.6

[20] Mohamed El Massad, Siddharth Garg, and Mahesh V. Tripunitara. Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes. In *NDSS*, 2015. 2

[21] P. Subramanyan, S. Ray, and S. Malik. Evaluating the Security of Logic Encryption Algo-

rithms. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 137–143, May 2015. doi: 10.1109/HST.2015.7140252. 2, 4.5.2, 4.7

[22] Degate. URL `https://degate.org/`. 2

[23] W. Li, Z. Wasson, and S. A. Seshia. Reverse Engineering Circuits Using Behavioral Pattern Mining. In *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 83–88, June 2012. doi: 10.1109/HST.2012.6224325. 2

[24] P. Subramanyan, N. Tsiskaridze, K. Pasricha, D. Reisman, A. Susnea, and S. Malik. Reverse Engineering Digital Circuits Using Functional Analysis. In *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 1277–1280, March 2013. doi: 10.7873/DATE.2013.264. 2

[25] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. Security Analysis of Integrated Circuit Camouflaging. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer and ; Communications Security (CCS)*, pages 709–720, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2477-9. doi: 10.1145/2508859.2516656. URL `http://doi.acm.org/10.1145/2508859.2516656`. 2, 2.1.2, 2.2, 2.1.3, 3.3, 4.5.1, 4.1, 4.5.5, 4.7

[26] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. Logic Encryption: A Fault Analysis Perspective. In *2012 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 953–958, March 2012. doi: 10.1109/DATE.2012.6176634. 2

[27] A. Baumgarten, A. Tyagi, and J. Zambreno. Preventing IC Piracy Using Reconfigurable Logic Barriers. *IEEE Design Test of Computers*, 27(1):66–75, Jan 2010. ISSN 0740-7475. doi: 10.1109/MDT.2010.24. 2, 4.5.2

[28] SypherMedia. Circuit Camouflage Technology. URL `https://www.insidesecure.com/content/download/1689/18690/file/Inside-Secure-Datasheet-Camo.pdf`. 2, 2.1, 2.1.1, 4.7

[29] Wilfried Vandervorst, Trudo Clarysse, and Pierre Eyben. Spreading Resistance Roadmap

Towards and Beyond the 70 nm Technology Node. *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena*, 20(1):451–458, 2002. doi: 10.1116/1.1446455. URL https://avs.scitation.org/doi/abs/10.1116/1.1446455. 2.1.4

[30] N. Duhayon, P. Eyben, M. Fouchier, T. Clarysse, W. Vandervorst, D. Álvarez, S. Schoemann, M. Ciappa, M. Stangoni, W. Fichtner, P. Formanek, M. Kittler, V. Raineri, F. Giannazzo, D. Goghero, Y. Rosenwaks, R. Shikler, S. Saraf, S. Sadewasser, N. Barreau, T. Glatzel, M. Verheijen, S. A. M. Mentink, M. von Sprekelsen, T. Maltezopoulos, R. Wiesendanger, and L. Hellemans. Assessing the Performance of Two-dimensional Dopant Profiling Techniques. *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena*, 22(1):385–393, 2004. doi: 10.1116/1.1638775. URL https://avs.scitation.org/doi/abs/10.1116/1.1638775. 2.1.4

[31] C. C. Williams. Two-dimensional Dopant Profiling by Scanning Capacitance Microscopy. *Annual Review of Materials Research*, 29:471–504, 11 2003. doi: 10.1146/annurev.matsci.29.1.471. 2.1.4

[32] Ch. Sommerhalter, Th. W. Matthes, Th. Glatzel, A. Jäger-Waldau, and M. Ch. Lux-Steiner. High-sensitivity Quantitative Kelvin Probe Microscopy by Noncontact Ultra-high-vacuum Atomic Force Microscopy. *Applied Physics Letters*, 75(2):286–288, 1999. doi: 10.1063/1.124357. URL https://doi.org/10.1063/1.124357. 2.1.4

[33] Edgar Völkl, Lawrence F. Allard, and David C. Joy. *Introduction to Electron Holography*. Springer US, 1999. ISBN 978-1-4613-7183-0. doi: 10.1007/978-1-4615-4817-1. 2.1.4

[34] Y. Huang, C. C. Williams, and H. Smith. Direct Comparison of Cross-sectional Scanning Capacitance Microscope Dopant Profile and Vertical Secondary Ion-mass Spectroscopy Profile. *Journal of Vacuum Science & Technology B: Microelectronics and Nanome-*

ter Structures Processing, Measurement, and Phenomena, 14(1):433–436, 1996. doi: 10.1116/1.588489. URL https://avs.scitation.org/doi/abs/10.1116/1.588489. 2.1.4

[35] V. Vartanian, M. Sadaka, S. Zollner, A. V.-Y. Thean, T. White, B.-Y. Nguyen, M. Zavala, L. McCormick, L. Prabhu, D. Eades, S. Parsons, H. Collard, K. Kim, J. Jiang, V. Dhandapani, J. Hildreth, R. Powers, G. Spencer, N. Ramani, J. Mogab, M. Kottke, M. Canonico, Q. Xie, X.-D. Wang, J. Vella, L. Contreras, D. Theodore, B. Lu, T. Kriske, R. Gregory, and R. Liu. Metrology Challenges for 45 Nm Strained-si Devices. *AIP Conference Proceedings*, 788(1):214–221, 2005. doi: 10.1063/1.2062965. URL https://aip.scitation.org/doi/abs/10.1063/1.2062965. 2.1.4

[36] Maria Virginia Stangoni. *Scanning Probe Techniques for Dopant Profile Characterization, Swiss Federal Institute of Technology Zurich*. PhD thesis, 2005. 2.1.4

[37] Peter De Wolf, R. Stephenson, T. Trenkler, Trudo Clarysse, Thomas Hantschel, and Wilfried Vandervorst. Status and Review of Two-Dimensional Carrier and Dopant Profiling Using Scanning Probe Microscopy. *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures*, 18:361, 01 2000. doi: 10.1116/1.591198. 2.1.4

[38] I. R. Nirmala, D. Vontela, S. Ghosh, and A. Iyengar. A Novel Threshold Voltage Defined Switch for Circuit Camouflaging. In *2016 21th IEEE European Test Symposium (ETS)*, pages 1–2, May 2016. doi: 10.1109/ETS.2016.7519286. 2.1.4, 2.1.4, 2.4, 2.1.4

[39] Maria I. Mera Collantes, Mohamed El Massad, and Siddharth Garg. (threshold-dependent camouflaged cells to secure circuits against reverse engineering attacks). In *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 443–448, 07 2016. doi: 10.1109/ISVLSI.2016.89. 2.1.4, 2.1.4, 2.5

[40] K. Tiri, M. Akmal, and I. Verbauwhede. A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Dower Analysis

on Smart Cards. In *Proceedings of the 28th European Solid-State Circuits Conference (ESSCIRC)*, pages 403–406, Sept 2002. 3.1, 4.2, 4.5.4

[41] N. E. C. Akkaya, B. Erbagci, R. Carley, and K. Mai. A DPA-Resistant Self-Timed Three-Phase Dual-Rail Pre-Charge Logic Family. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 112–117, May 2015. doi: 10.1109/HST.2015.7140248. 3.2, 4.5.4

[42] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pages 388–397, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg. ISBN 978-3-540-48405-9. 3.3

[43] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 104–113, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg. ISBN 978-3-540-68697-2. 3.3

[44] Mudit Bhargava. *Reliable, Secure, Efficient Physical Unclonable Functions, Carnegie Mellon University*. PhD thesis, May 2013. 4.1.1, 4.2, 6.3

[45] T. Ong, M. Levi, P. Ko, and C. Hu. Recovery of Threshold Voltage After Hot-carrier Stressing. *IEEE Transactions on Electron Devices*, 35(7):978–984, July 1988. ISSN 0018-9383. doi: 10.1109/16.3354. 4.2, 5.2.2

[46] F. Khan, E. Cartier, C. Kothandaraman, J. C. Scott, J. C. S. Woo, and S. S. Iyer. The Impact of Self-Heating on Charge Trapping in High-k-Metal-Gate nFETs. *IEEE Electron Device Letters*, 37(1):88–91, Jan 2016. ISSN 0741-3106. doi: 10.1109/LED.2015.2504952. 4.2, 5.2.2

[47] F. Khan, E. Cartier, J. C. S. Woo, and S. S. Iyer. Charge Trap Transistor (CTT): An Embedded Fully Logic-Compatible Multiple-Time Programmable Non-Volatile Memory Element for High- k -Metal-Gate CMOS Technologies. *IEEE Electron Device Letters*, 38(1):44–47,

Jan 2017. ISSN 0741-3106. doi: 10.1109/LED.2016.2633490. 4.2, 5.2.2

[48] Vishwani D. Agrawal Michael L. Bushnell. *Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits*. Springer, Boston, MA, 2002. ISBN 978-0-7923-7991-1. doi: https://doi.org/10.1007/b117406. 4.5.1

[49] Miron Abramovici, Melvin A. Breuer, and Arthur D. Friedman. *Digital Systems Testing and Testable Design*. Wiley-IEEE Press, 1994. ISBN 978-0-780-31062-9. 4.5.1

[50] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. Security Analysis of Logic Obfuscation. In *DAC Design Automation Conference 2012*, pages 83–89, June 2012. doi: 10.1145/2228360.2228377. 4.5.1

[51] Susanne Engels, Max Hoffmann, and Christof Paar. The End of Logic Locking? A Critical View on the Security of Logic Locking. *IACR Cryptology ePrint Archive*, 2019:796, 2019. 4.5.1, 4.7

[52] Intelligence Advanced Research Projects Activity (IARPA). Trusted Integrated Chips (TIC) Program - Broad Agency Announcement, 2011. URL `https://www.fbo.gov/utils/view?id=b8be3d2c5d5babbdffc6975c370247a6`. 4.5.2, 4.7

[53] Burak Erbagci. *Hardware-Entangled Inherently Secure Field Programmable Gate Arrays, Carnegie Mellon University*. PhD thesis, December 2018. 4.5.2, 6.3

[54] C. Yu, X. Zhang, D. Liu, M. Ciesielski, and D. Holcomb. Incremental SAT-Based Reverse Engineering of Camouflaged Logic Circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 36(10):1647–1659, Oct 2017. ISSN 0278-0070. doi: 10.1109/TCAD.2017.2652220. 4.5.2

[55] Gaurav Kolhe, Hadi Mardani Kamali, Miklesh Naicker, Tyler David Sheaves, Setareh Rafatirad, Avesta Sasan, Sai Manoj Pudukotai Dinakarrao, Hamid Mahmoodi, and Houman Homayoun. Security and Complexity Analysis of LUT-based Obfuscation: From Blueprint to Reality. In *International Conference On Computer Aided Design (ICCAD)*, Appearing

in November, 2019. 4.5.2, 4.7, 6.3

[56] Aliyar Attaran, Tyler David Sheaves, Praveen Kumar Mugula, and Hamid Mahmoodi. Static Design of Spin Transfer Torques Magnetic Look Up Tables for ASIC Designs. In *Proceedings of the 2018 on Great Lakes Symposium on VLSI*, GLSVLSI '18, pages 507–510, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-5724-1. doi: 10.1145/3194554.3194651. URL http://doi.acm.org/10.1145/3194554.3194651. 4.5.2

[57] B. Liu and B. Wang. Embedded Reconfigurable Logic for ASIC Design Obfuscation Against Supply Chain Attacks. In *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 1–6, March 2014. doi: 10.7873/DATE.2014.256. 4.5.2

[58] Hadi Mardani Kamali, Kimia Zamiri Azar, Kris Gaj, Houman Homayoun, and Avesta Sasan. LUT-Lock: A Novel LUT-Based Logic Obfuscation for FPGA-Bitstream and ASIC-Hardware Protection. pages 405–410, 07 2018. doi: 10.1109/ISVLSI.2018.00080. 4.5.2

[59] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja. Advancing Hardware Security Using Polymorphic and Stochastic Spin-hall Effect Devices. In *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 97–102, March 2018. doi: 10.23919/DATE.2018.8341986. 4.5.2

[60] A. Rezaei, Y. Shen, S. Kong, J. Gu, and H. Zhou. Cyclic Locking and Memristor-based Obfuscation Against CycSAT and Inside Foundry Attacks. In *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 85–90, March 2018. doi: 10.23919/DATE.2018.8341984. 4.5.2

[61] T. Winograd, H. Salmani, H. Mahmoodi, K. Gaj, and H. Homayoun. Hybrid STT-CMOS Designs for Reverse-engineering Prevention. In *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6, June 2016. doi: 10.1145/2897937.2898099. 4.5.2

[62] Jianlei Yang, Xueyan Wang, Qiang Zhou, Zhaohao Wang, Hai Li, Yiran Chen, and Weisheng Zhao. Exploiting Spin-Orbit Torque Devices As Reconfigurable Logic for Cir-

cuit Obfuscation. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 38:57–69, 2019. 4.5.2

[63] Franc Brglez and Hideo Fujiwara. A Neutral Netlist of 10 Combinational Benchmark Circuits and a Targeted Translator in FORTRAN. In *Special Session on Recent Algorithms for Gate-Level ATPG with Fault Simulation and Their Performance Assessment, 1985 IEEE Int. Symp. on Circuits and Systems, June 5-7, 1985, Kyoto, Japan*, 06 1985. 4.6

[64] Cadence. Genus Synthesis Solution, . URL `https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/synthesis/genus-synthesis-solution.html`. 4.6.1

[65] Cadence. Innovus Implementation System, . URL `https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/soc-implementation-and-floorplanning/innovus-implementation-system.html`. 4.6.1

[66] Cadence. Virtuoso Schematic Editor, . URL `https://www.cadence.com/content/cadence-www/global/en_US/home/tools/custom-ic-analog-rf-design/circuit-design/virtuoso-schematic-editor.html`. 4.6.1

[67] T. J. Barnes. SKILL: a CAD System Extension Language. In *27th ACM/IEEE Design Automation Conference*, pages 266–271, June 1990. doi: 10.1109/DAC.1990.114865. 4.6.1

[68] Clifford Wolf. Yosys Open Synthesis Suite. URL `http://www.clifford.at/yosys/`. 4.6.1

[69] Yang-Kyu Choi, Daewon Ha, E. Snow, J. Bokor, and Tsu-Jae King. Reliability Study of CMOS FinFETs. In *IEEE International Electron Devices Meeting 2003*, pages 7.6.1–7.6.4,

Dec 2003. doi: 10.1109/IEDM.2003.1269206. 6.3

[70] M. Cho, P. Roussel, B. Kaczer, R. Degraeve, J. Franco, M. Aoulaiche, T. Chiarella, T. Kauerauf, N. Horiguchi, and G. Groeseneken. Channel Hot Carrier Degradation Mechanism in Long/Short Channel n-FinFETs. *IEEE Transactions on Electron Devices*, 60(12): 4002–4007, Dec 2013. ISSN 0018-9383. doi: 10.1109/TED.2013.2285245. 6.3

[71] E. Chung, K. Nam, T. Nakanishi, S. Park, H. Yang, T. Kauerauf, G. Jiao, D. Kim, K. H. Hwang, H. Kim, H. Lee, and S. Pae. Investigation of Hot Carrier Degradation in Bulk Finfet. In *2017 IEEE International Reliability Physics Symposium (IRPS)*, pages XT–6.1–XT–6.4, April 2017. doi: 10.1109/IRPS.2017.7936420. 6.3

[72] P. Mohan, N. E. C. Akkaya, B. Erbagci, and K. Mai. A Compact Energy-efficient Pseudo-static Camouflaged Logic Family. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 96–102, April 2018. doi: 10.1109/HST.2018.8383896. 6.3

A Secure Camouflaged Logic Family for Untrusted Fabrication and Reverse Engineering

Nail Etkin Can Akkaya
Electrical and Computer Engineering
Carnegie Mellon University
09/13/2019

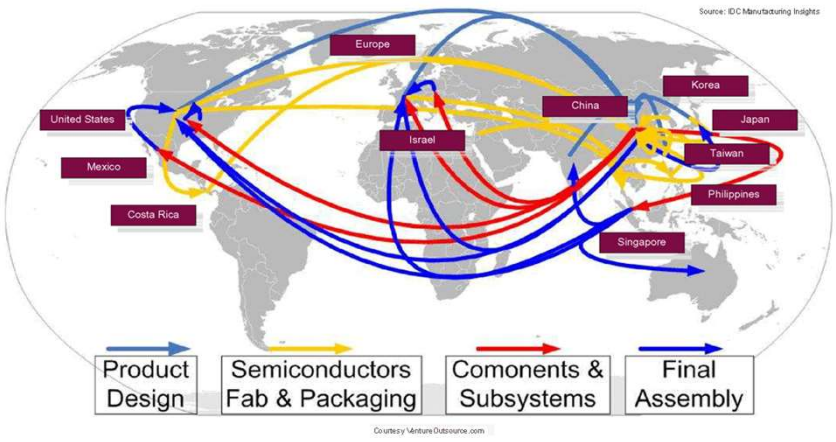
Carnegie Mellon
Electrical & Computer ENGINEERING

Supply Chain and Reverse Engineering Threats

“VAX – when you care to steal (from) the very best”

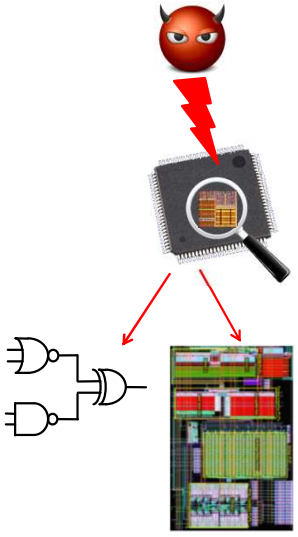
Carnegie Mellon
Electrical & Computer ENGINEERING
2/78

Globalized Supply Chain



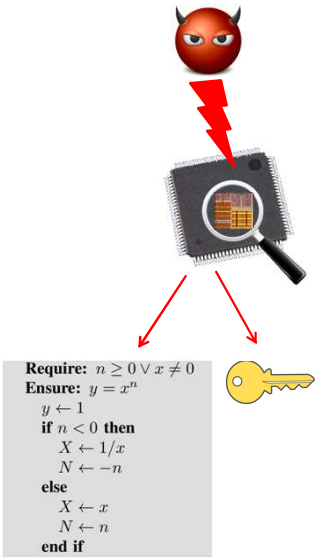
Attacker Model

- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks



Attacker Model

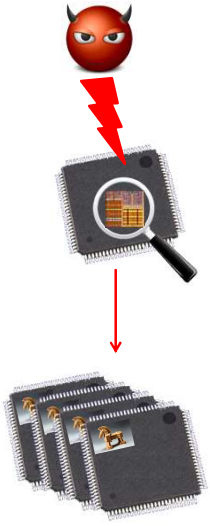
- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks



Require: $n \geq 0 \vee x \neq 0$
Ensure: $y = x^n$
$y \leftarrow 1$
if $n < 0$ **then**
$X \leftarrow 1/x$
$N \leftarrow -n$
else
$X \leftarrow x$
$N \leftarrow n$
end if

Attacker Model

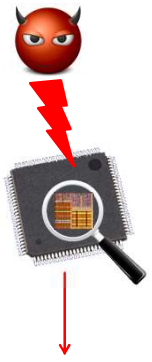
- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks

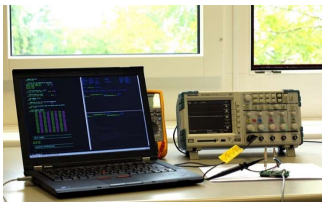


Clone ICs

Attacker Model

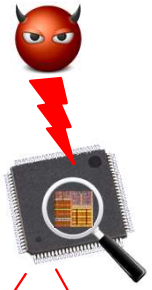
- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks

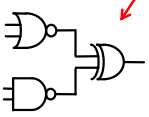


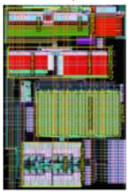


Attacker Model

- **Attacks mounted on ICs during**
  - Manufacturing
  - Deployment
- **Attacks during manufacturing**
  - Foundry has physical access
  - Extracting the design information
- **Attacks during employment**
  - Invasive
  - Non-invasive
- **Metrics**
  - Design information obfuscation
  - SAT-based attack resiliency







Hardware Obfuscation

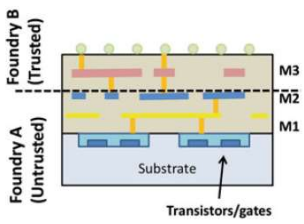
- **Hardware obfuscation**
  - Lock the functionality/structure
  - Conceal the functionality
- **Example methods**
  - Split manufacturing
  - Logic encryption
  - Gate camouflaging

[1] Springer, 2017

Hardware Obfuscation

- **Hardware obfuscation**
  - Lock the functionality/structure
  - Conceal the functionality
- **Example Methods**
  - Split manufacturing
  - Logic encryption
  - Gate camouflaging

Split Manufacturing

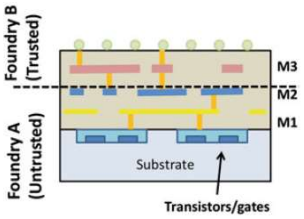


[1] Springer, 2017

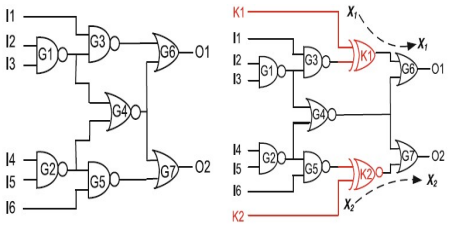
Hardware Obfuscation

- **Hardware obfuscation**
  - Lock the functionality/structure
  - Conceal the functionality
- **Example Methods**
  - Split manufacturing
  - Logic encryption
  - Gate camouflaging

Split Manufacturing

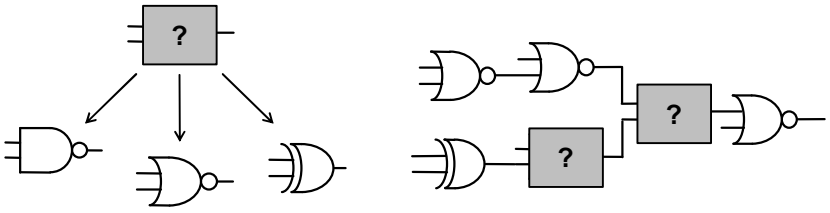


Keyed Logic



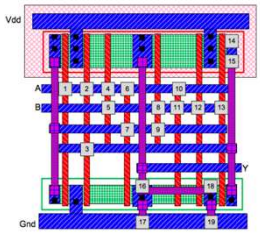
[1] Springer, 2017

Camouflaged Gates

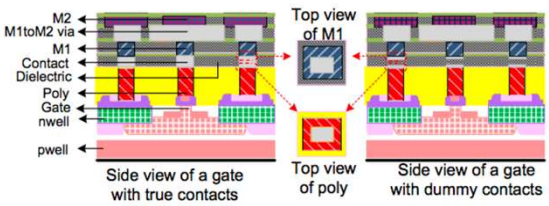


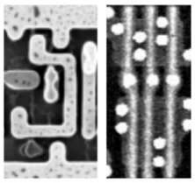
- **Hide logical function of gate from attacker**
- **Replace some gates w/ camouflaged ones**
- **Use look-alike gates**
  - Very similar layouts
  - Different Boolean function

Example Camouflaged Gates

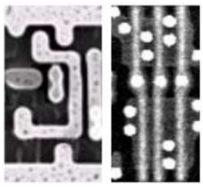


[J. Rajendran et al.]





SypherMedia Regular AND2 gate[2]

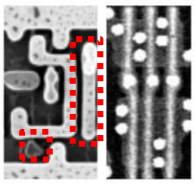


SypherMedia AND2 look-alike gate[2]

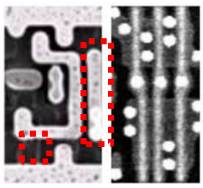
[1] Rajendran et al., CCS'13
[2] Syphermedia

Issues w/ Current Camouflaged Gates

- **Security relies on limited RE resolution**
  - Dummy contact detectable with careful de-processing
  - Look-alike gates may be discernable



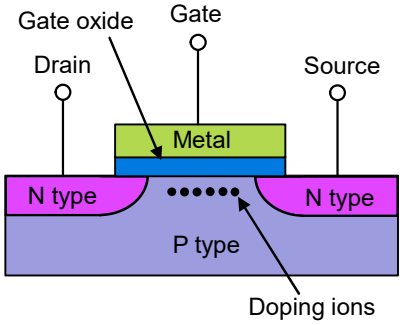
SypherMedia Regular AND2 gate

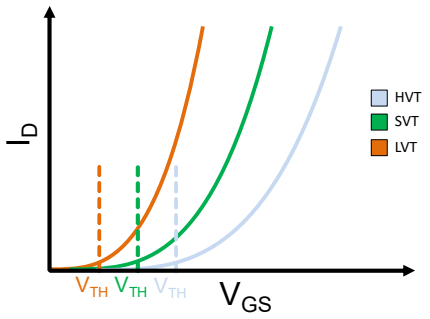


SypherMedia AND2 look-alike gate

- **Incompatibility with standard process and tools**
  - Additional mask layers and process steps
  - DRC waivers and non-standard structures

Threshold Voltage





- Today's processes offer multiple transistor V_{TH}'s
- Devices differ only in # ions implanted in channel
- Allow designers to trade-off speed and power

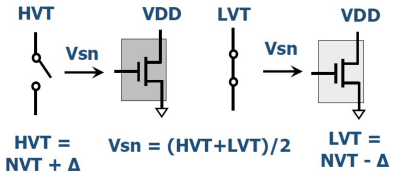
Threshold Voltage Based Solutions

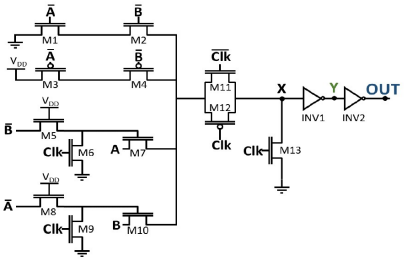
- **Primary requirement**
  - Amplify V_{TH} difference
- **Single-ended amplification**
  - Threshold voltage-defined switches[1]
  - Threshold-dependent camouflaged cells[2]
- **Differential amplification**
  - Threshold voltage defined (TVD) logic[3]

[1] Nirmala et al., ETS'16
[2] Collantes et al., ISVLSI'16
[3] Erbagci et al., HOST'16

Threshold Voltage Based Solutions

- **Single-ended amplification**
  - Small V_{TH} difference in the process
  - Sensitive to PVT variations, leakage, and noise

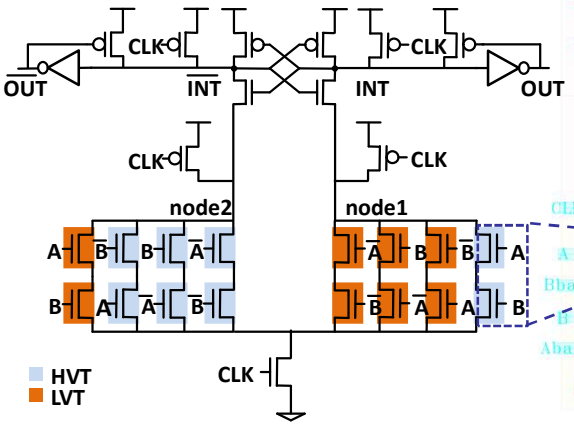


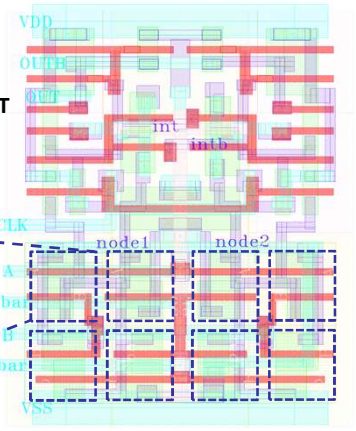


[1] Nirmala et al., ETS'16
[2] Collantes et al., ISVLSI'16

- **→Differential amplification for robustness**

Threshold Voltage Defined (TVD) Logic



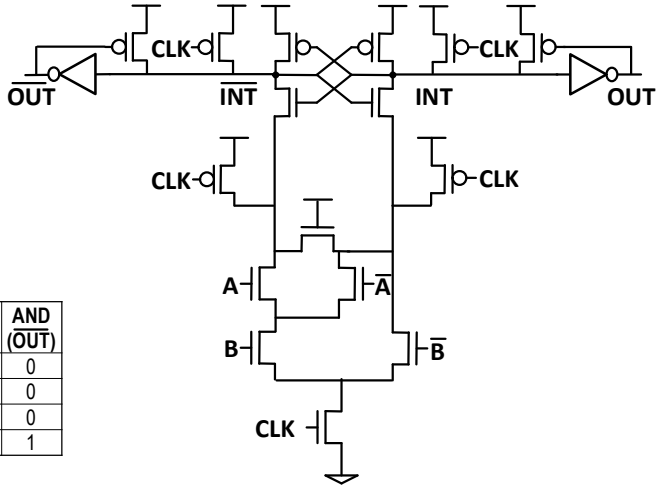


[1] Erbagci et al., HOST'16

- **Differential dynamic amplifying gate**
- **Logic function set by V_{TH} implant**
- **All gates have identical layout (except V_{TH} masks)**

Sense Amplifier Based Logic (SABL)

- Dual-rail dynamic logic
- Two phases
  - Pre-charge
  - Evaluate

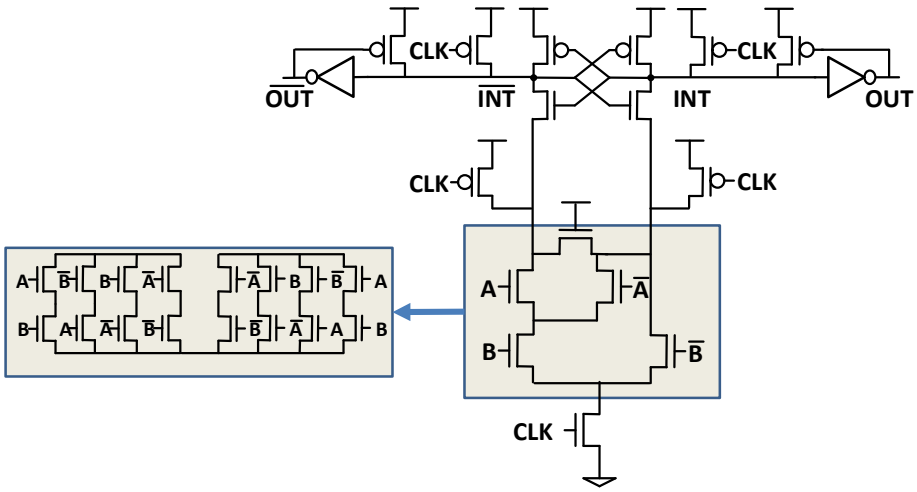


A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

[1] Tiri et al., ESSCIRC'02

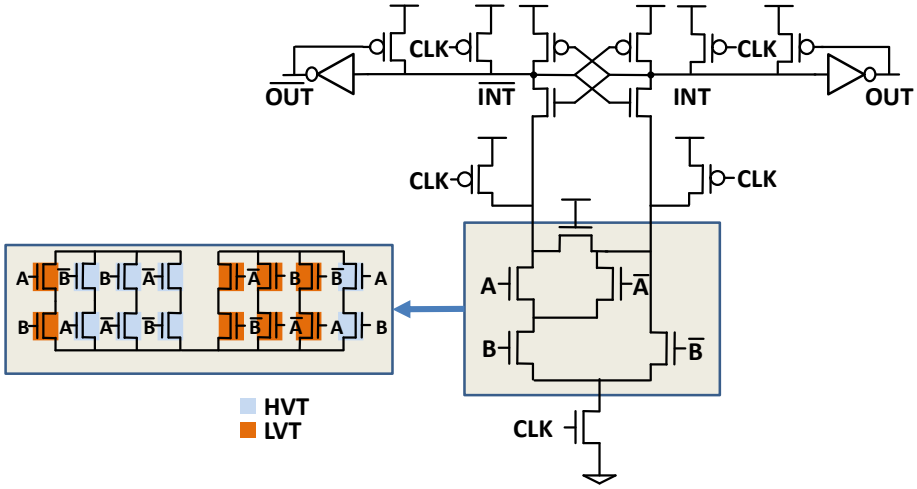
Threshold Voltage Defined (TVD) Logic

- Replace the pull-down network with generic one



Threshold Voltage Defined (TVD) Logic

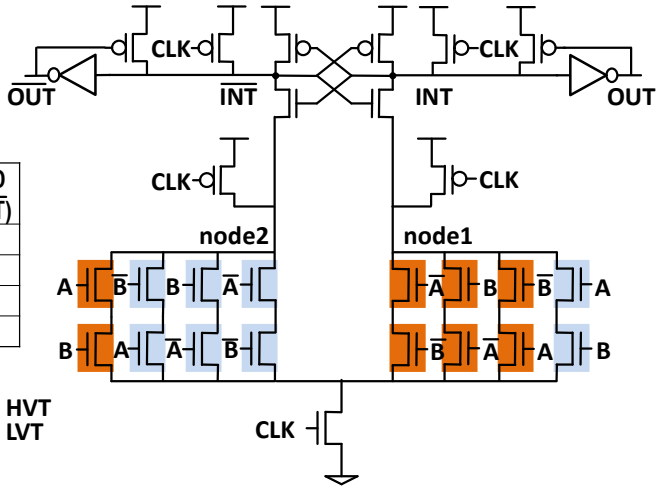
- Different V_{TH} implants to implement different functions



Threshold Voltage Defined (TVD) Logic

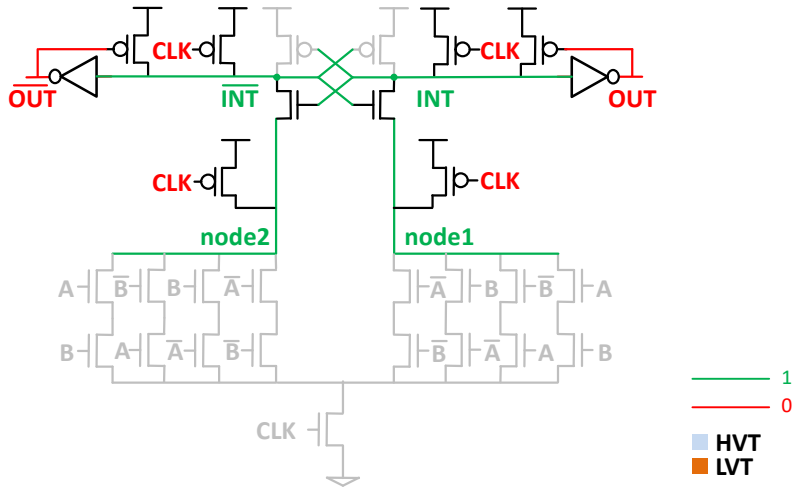
- Dual-rail dynamic amplifying logic family
- Two phases:
  - Pre-charge
  - Evaluate

A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1



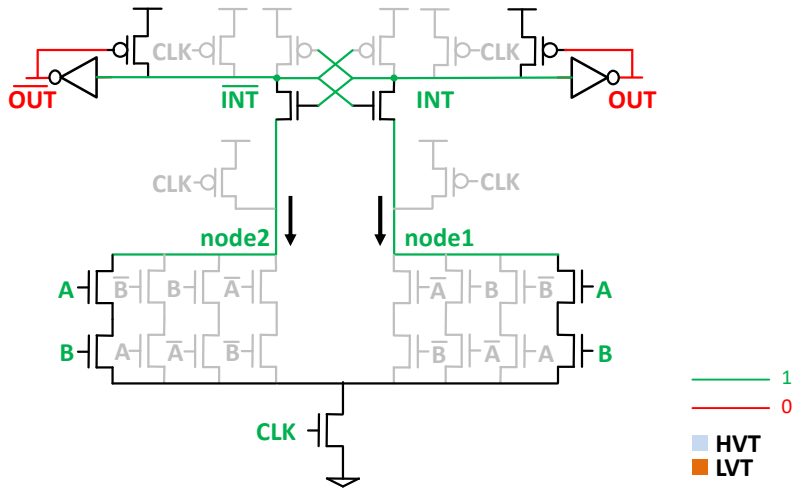
[1] Erbagci et al., HOST'16

TVD Operation: Pre-charge



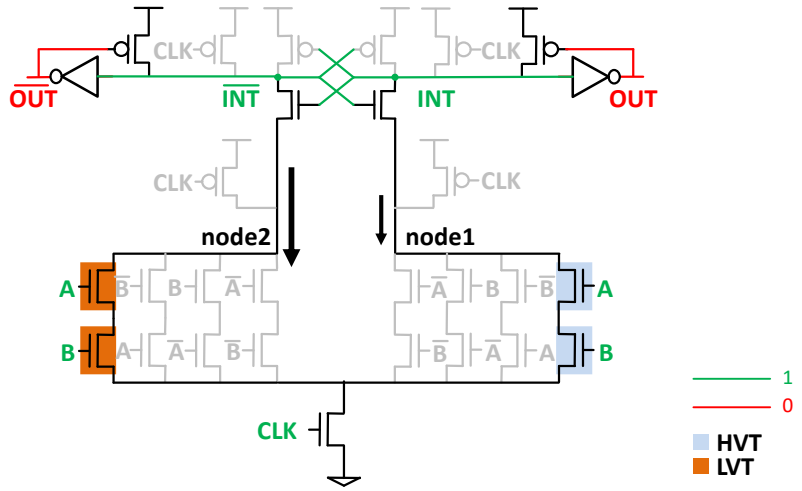
- Internal nodes are charged to 1
- Output nodes are pulled down to 0

TVD Operation: Evaluate



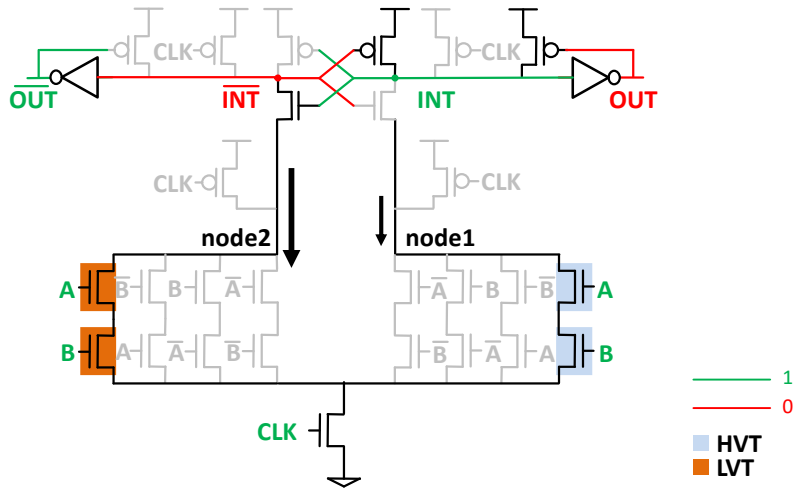
- Inputs AB = 11
- Left and right legs will start pulling current

TVD Operation: Evaluate



- Inputs AB = 11
- LVT gates pull more current compared to HVT gates

TVD Operation: Evaluate

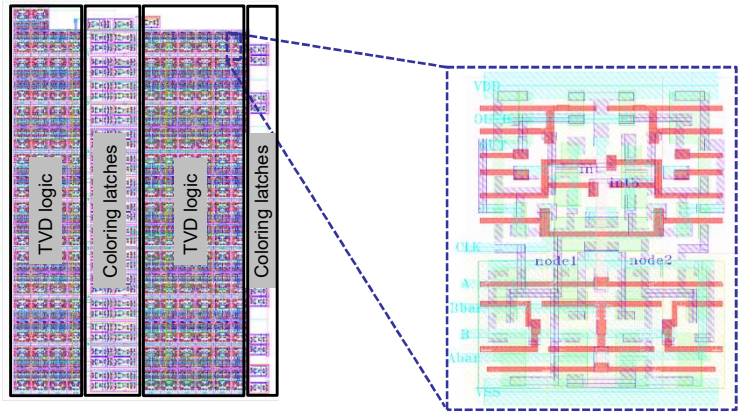


- Inputs AB = 11
- $\overline{\text{INT}}$ is discharged to 0, $\overline{\text{OUT}}$ is pulled up to 1

TVD Camouflaging Advantages

- **Security not reliant on limited RE resolution**
  - V_{TH} to set logic function
  - Identical layout
- **Fully CMOS logic process compatible**
  - No special layers, masks, or DRC waivers needed
- **Robust against PVT variations and noise**
- **Low side-channel emissions**
  - Due to differential structure and homogeneity

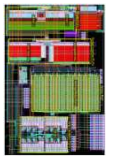
Example 16b Adder Layout

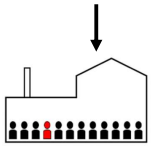


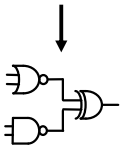
- **16b adder with 100% gate replacement**
- **Homogenous grids of TVD logic gates**
- **Latches between stages to color the logic**

Supply Chain Threats

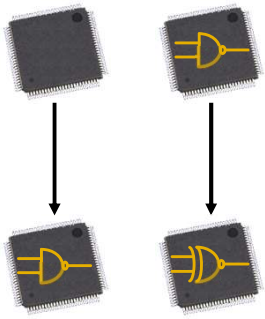
Untrusted Fabrication



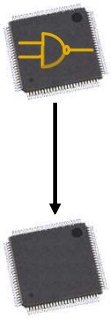




Programmable



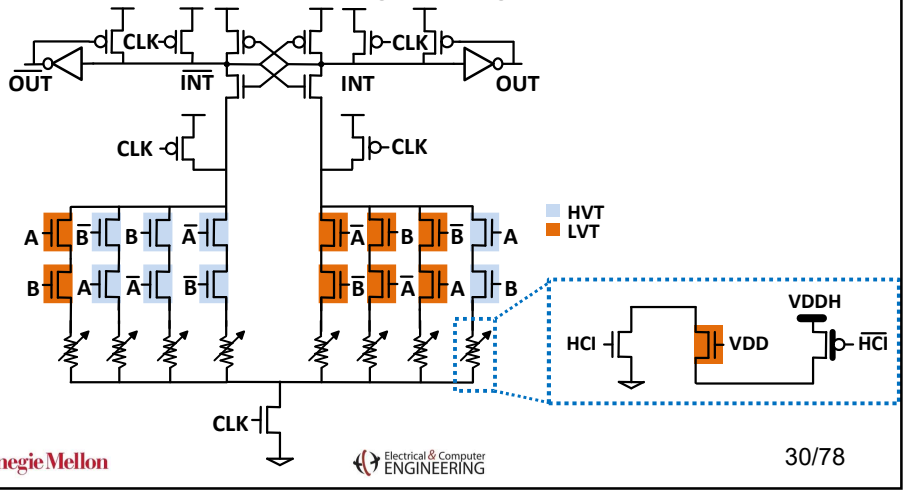
Erasable



Carnegie Mellon Electrical & Computer ENGINEERING 29/78

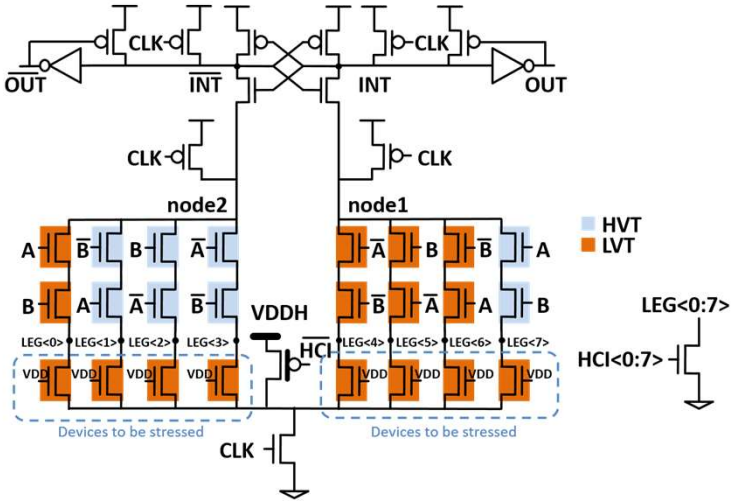
Supply Chain & RE Countermeasure

- Programmable TVD logic gate
- 3rd party fab does not have critical design info
- Resistant to reverse engineering



Carnegie Mellon Electrical & Computer ENGINEERING 30/78

Post-Manufacturing Programmed TVD Logic

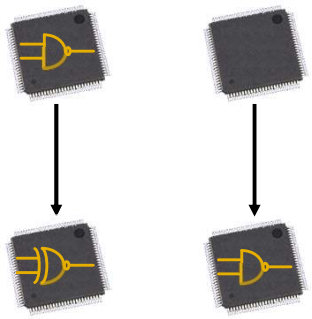


PMP-TVD Logic

- **Countermeasure against untrusted fabrication**
  - Fab does not have logic gate Boolean function
- **Differential dynamic amplifying gate**
  - Two phases: pre-charge and evaluate
- **Logic function set by V_{TH} implant**
  - Identical layout except V_{TH} masks
- **Operation is similar to TVD logic**

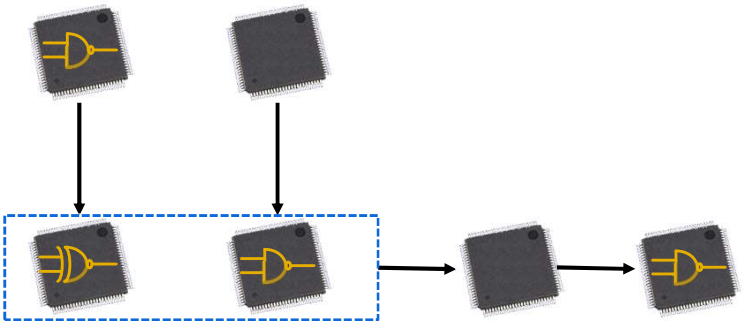
PMP-TVD Logic

- **Programming options**
  - Preprogrammed
  - Blank

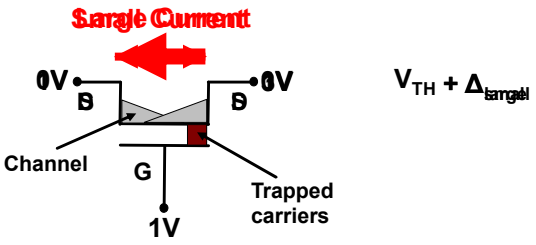


PMP-TVD Logic

- **Hot-carrier injection (HCI) programming**
  - Programmable
    - Adding/changing functionality
  - Erasable
    - Reversing the effects of HCI



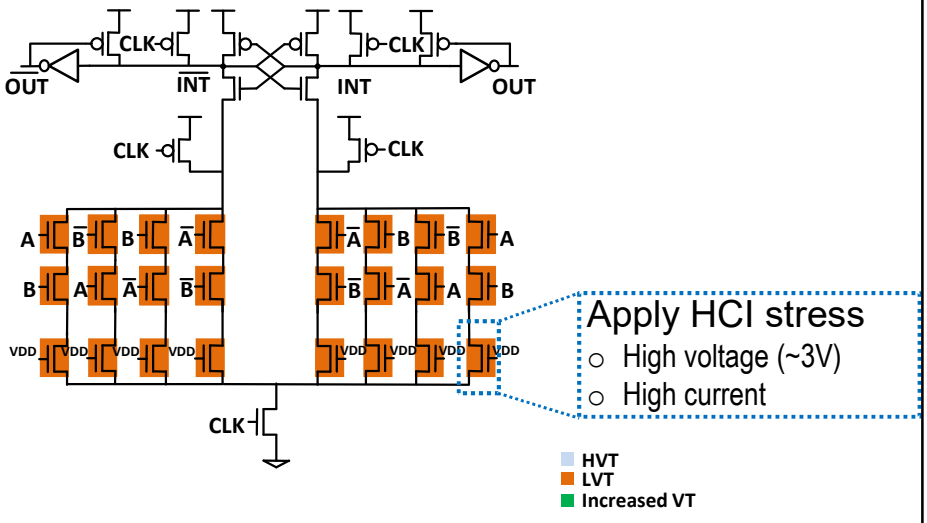
Hot-Carrier Injection (HCI)



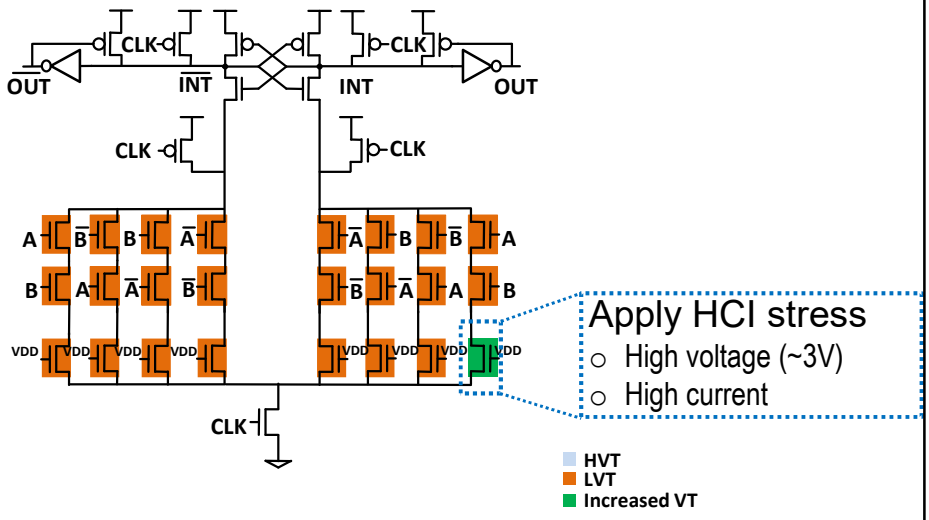
One-time Post-HCI stress

- Charge carriers to be trapped in gate dielectric
- V_{TH} of a transistor may be altered

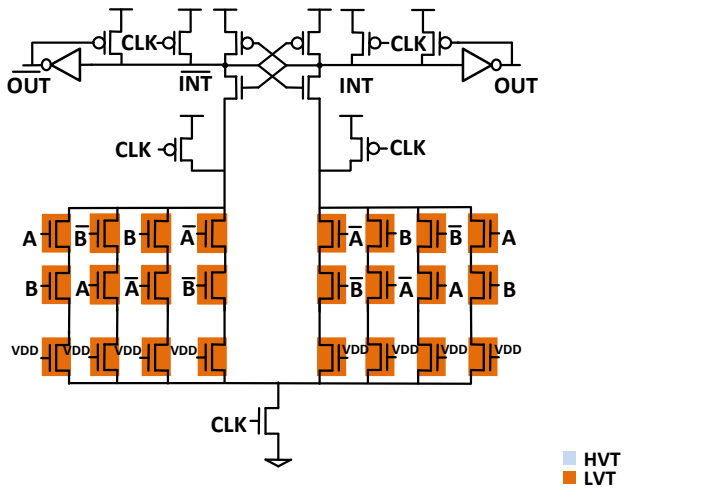
PMP-TVD Gate Programming



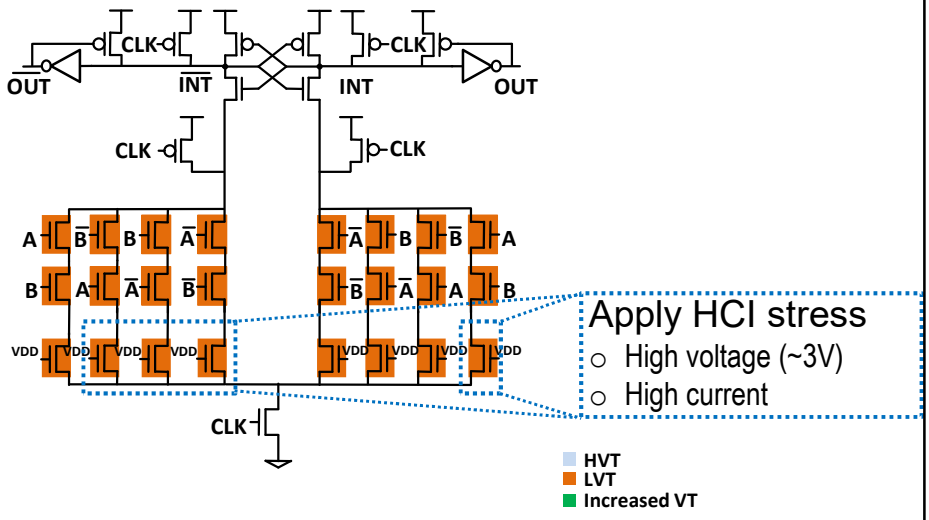
PMP-TVD Gate Programming



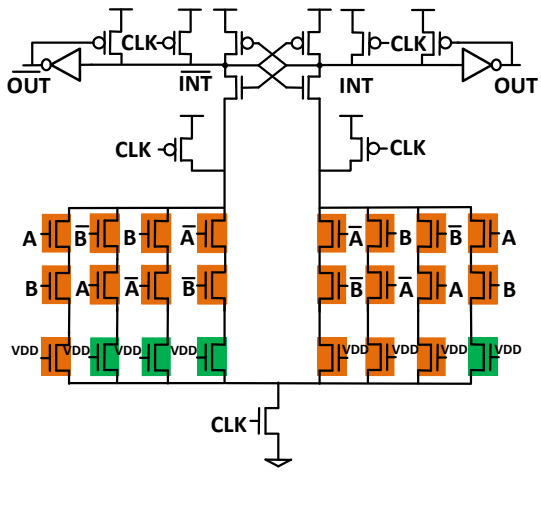
Blank PMP-TVD Gate Programming



Blank PMP-TVD Gate Programming

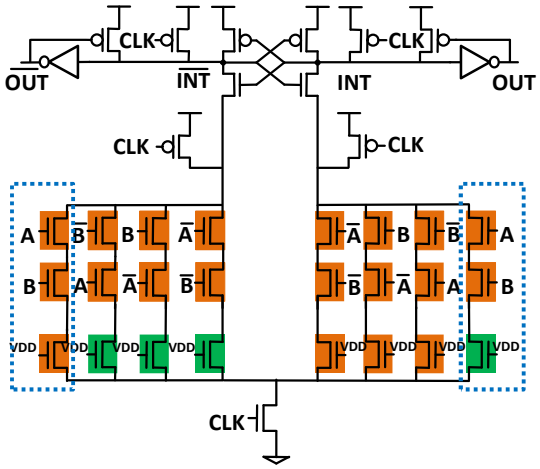


Blank PMP-TVD Gate Programming



A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

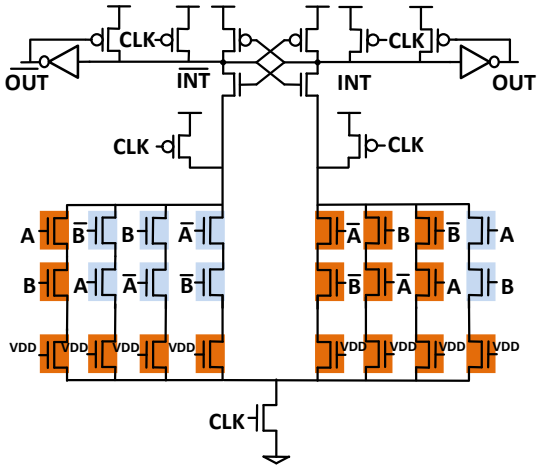
Blank PMP-TVD Gate Programming



A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

HVT
LVT
Increased VT

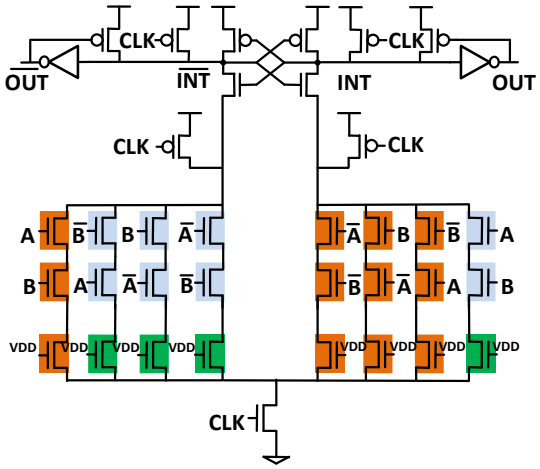
Preprogrammed PMP-TVD Gate Programming



A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

HVT
LVT
Increased VT

Preprogrammed PMP-TVD Gate Programming

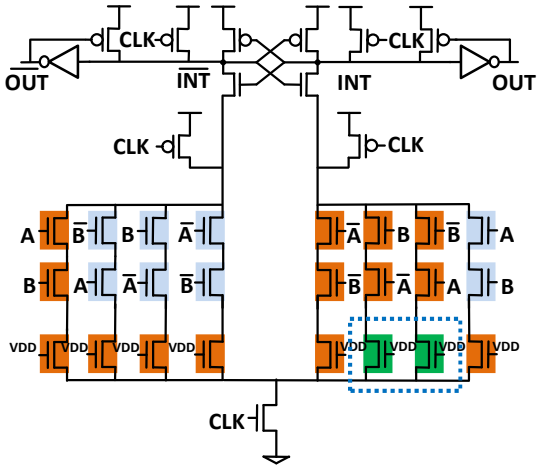


A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

Boost performance

HVT
LVT
Increased VT

Preprogrammed PMP-TVD Gate Programming

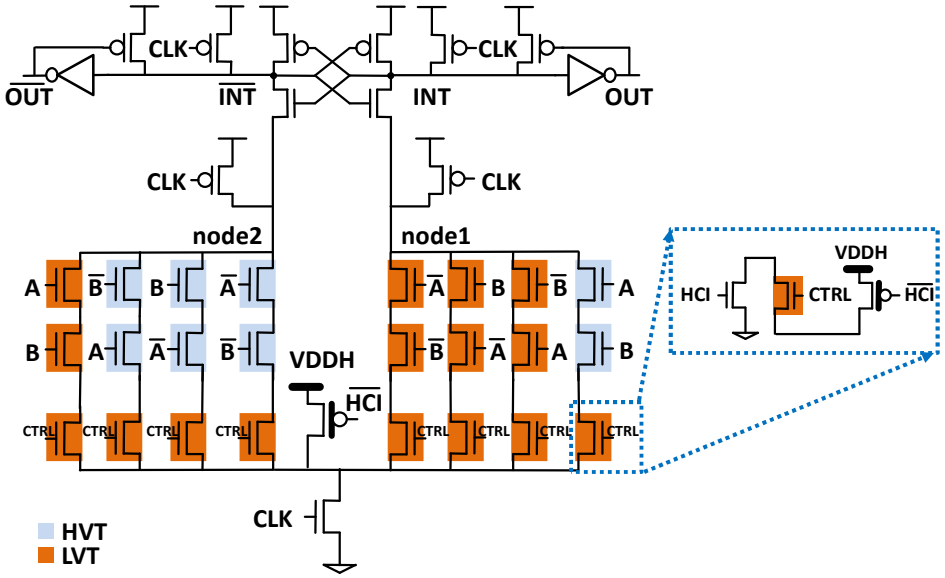


A	B	NOR (OUT)	OR ($\overline{OUT}$)
0	0	1	0
1	0	0	1
0	1	0	1
1	1	0	1

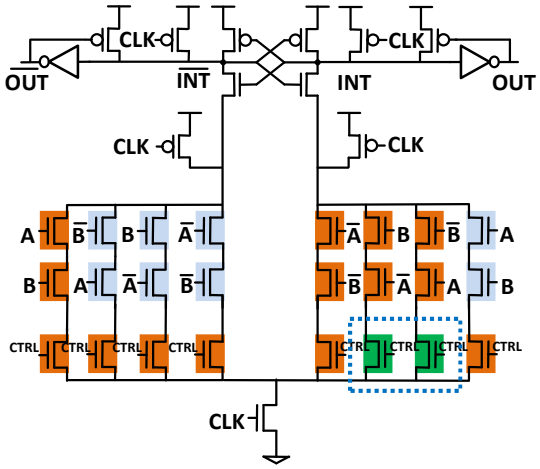
Change function

HVT
LVT
Increased VT

HCI Re-programmability



Erasing by Reversing HCI

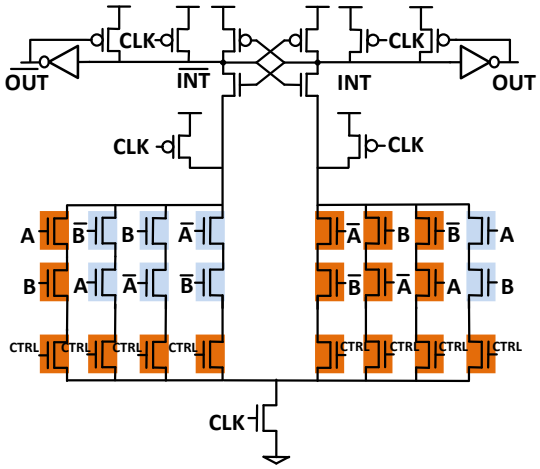


A	B	NOR (OUT)	OR ($\overline{OUT}$)
0	0	1	0
1	0	0	1
0	1	0	1
1	1	0	1

Change function

HVT
LVT
Increased VT

Erasing by Reversing HCI (cont.)

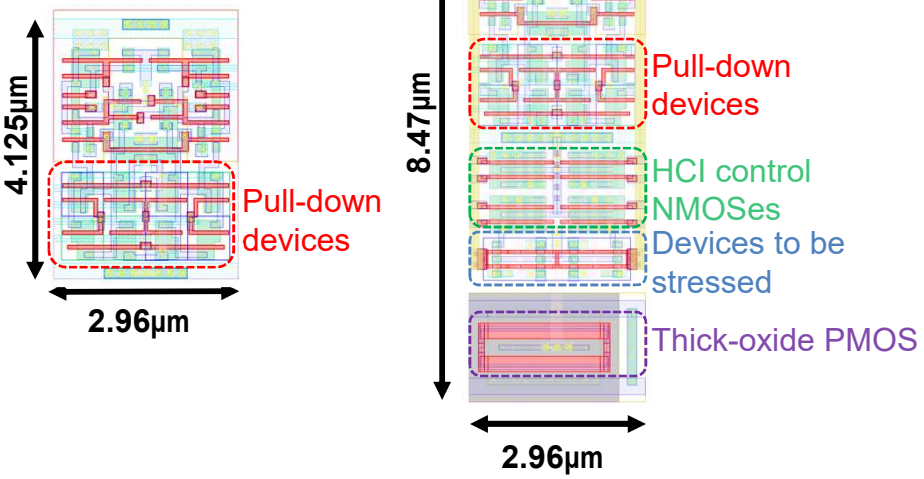


A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

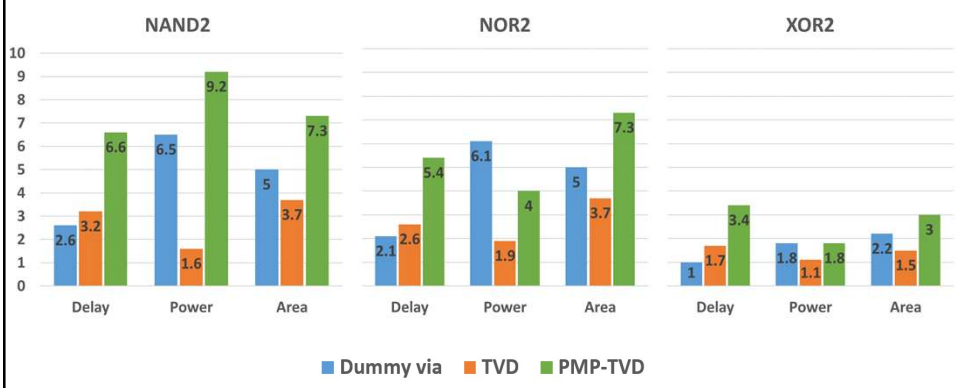
HCI effects are reversed

HVT
LVT
Increased VT

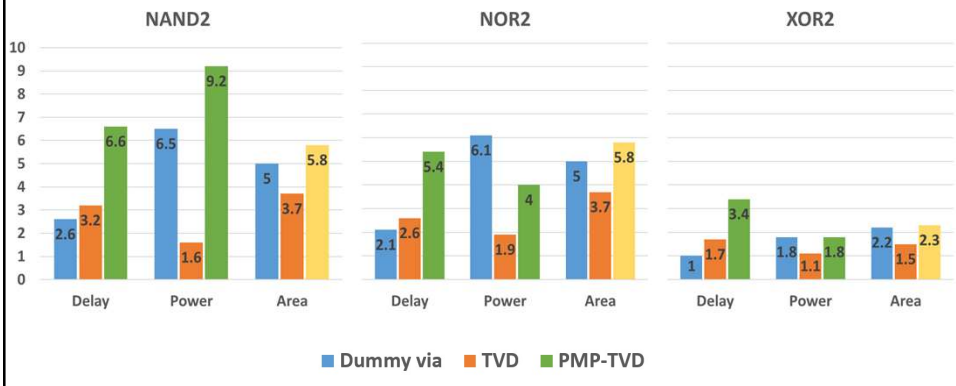
2-input TVD vs PMP-TVD (65nm)



Single Gate Overhead Comparison



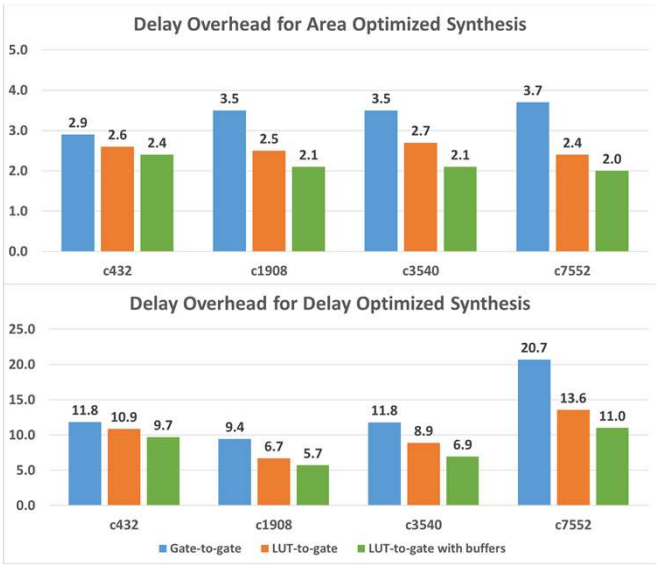
Single Gate Overhead Comparison



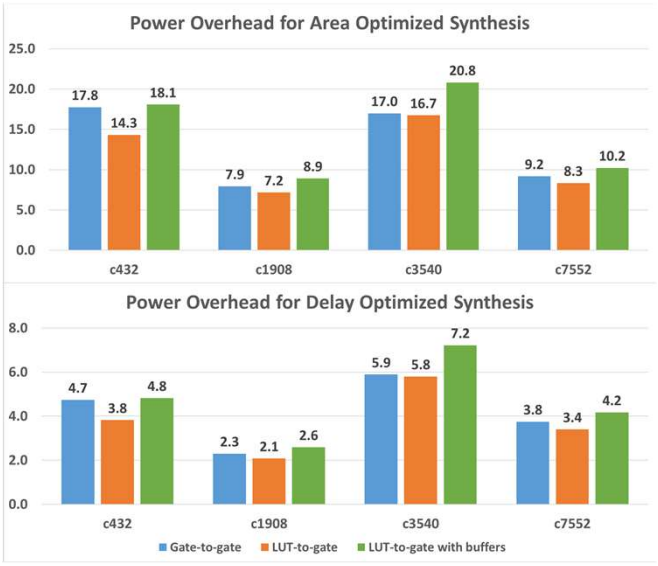
Overhead Analysis

- **ISCAS85 benchmark circuits**
  - c432, c1908, c3540, c7552
- **Design optimization points**
  - Area optimized
  - Delay optimized
- **Replacement strategies with 100% camouflaging**
  - Gate-to-gate
  - LUT-to-gate
  - LUT-to-gate with buffers

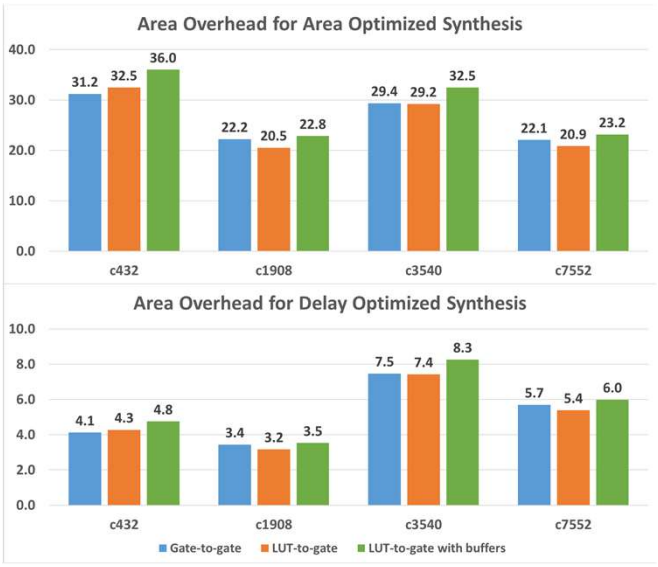
Delay Overhead



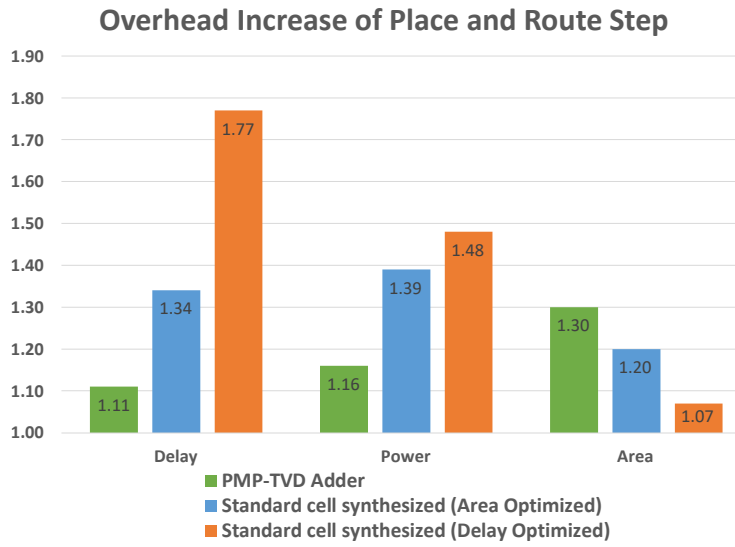
Power Overhead



Area Overhead



PnR Overhead



Security Evaluation

- **Untrusted fabrication**
  - Concealment of the logic function from the fab
  - HCI programming
- **Reverse engineering**
  - IC de-camouflaging
  - Deciphering the obfuscated design with camouflaged gates
  - SAT-based attacks[1]

[1] Massad et al., NDSS'15

Security Evaluation

- **PMP-TVD gates are fully camouflaged**
  - SAT attacks are ineffective against large scale camouflaging
  - n-input PMP-TVD gate → $2^{\wedge(2^{\wedge}n)}$ possible functionalities
- **LUT-based designs are resilient against SAT attacks**
  - Resilient with replacing only:
    - 5% with LUT2
    - 3.5% with LUT3
    - 1.6% with LUT4
- **Advantage over other reconfigurable designs:**
  - Embedded and distributed secret configuration

PMP-TVD Advantages

Security Comparison

	Dummy via[1]	TVD	PMP-TVD
Low side-channel Leakage		●	●
Untrusted Fab			●
Reverse Engineering	◐	●	●
Erasable/Programmable			●

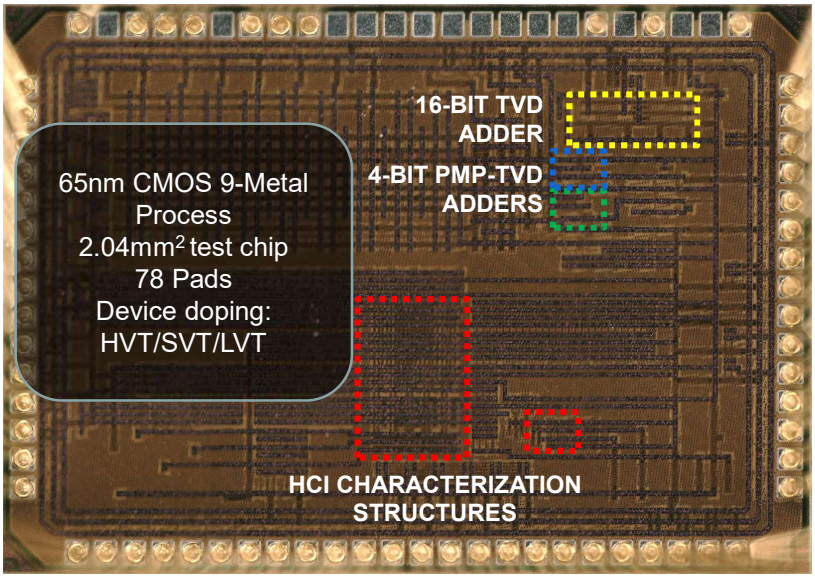
- **Security**
  - High resistance to reverse engineering
  - Concealment of logic function from fab
  - Embedded and distributed secret information
  - Erasable / Programmable
  - Low side-channel leakage
- **VLSI**
  - Fully CMOS logic process compatible
  - Fast programming time
  - High programming reliability and permanence

[1] Rajendran et al., CCS'13

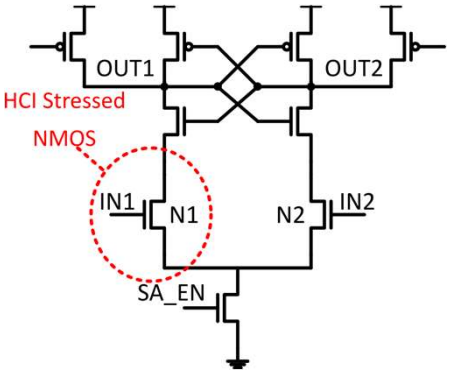
Testchips

- **Two prototype testchips in**
  - 65nm CMOS process
  - 28nm CMOS process
- **Implemented structures:**
  - 4-bit PMP-TVD adder/blank (65nm)
    - 2-input PMP-TVD gates
  - 16-bit TVD adder (65nm)
  - HCI characterization array (65nm)
  - 16-bit PMP-TVD adder/subtractor/XOR/blank (28nm)
    - 2- and 3- input PMP-TVD gates

Testchip Die Shot (65nm)

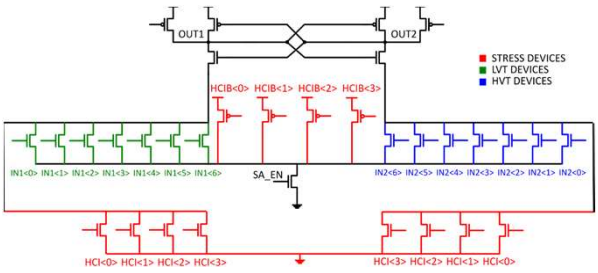


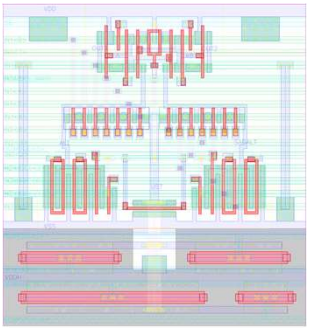
HCI Characterization



- Sense amplifier with intentional bias
- HCI flips offset after a known time
- One-way transform
- Single HCI stress current and voltage levels

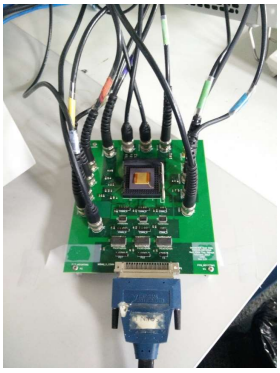
Modular Binary Aging Element





- 7 legs on either side
- 4 thick oxide HCI stress devices
- 693 possible configurations

HCI Characterization Methodology



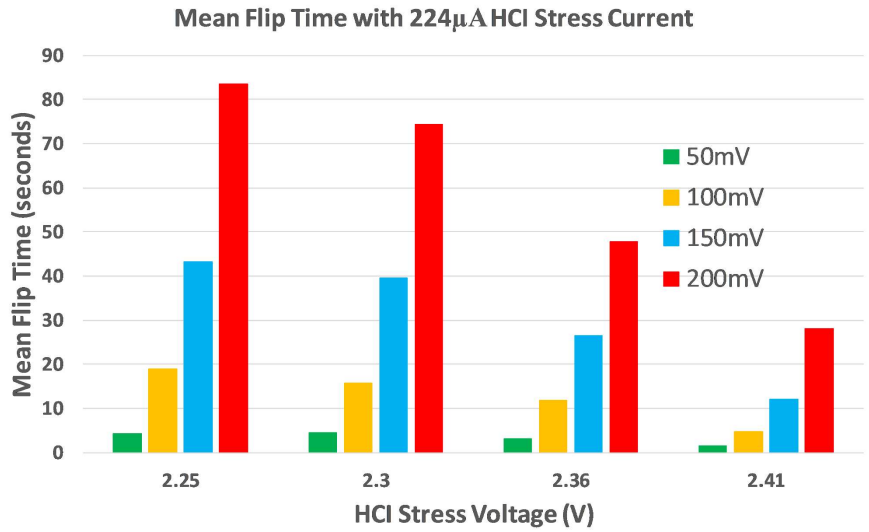
- **Methodology**
  - 1V Core voltage
  - 2.5V Stress voltage
  - Room temperature
- **Tests**
  - Input sweep before stress for initial input offset measurement
  - Stress/check cycle until output flips
    - Stress for a certain time
    - Input sweep for input reference offset

Results: Mean Flip Time

Stress Configuration	92µA and 1.67V	94.3µA and 2.05V	167µA and 1.68V
Stressed Device Width (nm)	Mean (hour)	Mean (hour)	Mean (hour)
200	86.76	1.19	7.06
400	101.79	1.2	7.85
600	117.63	1.42	9.0

- **Increasing device size requires longer stress**
- **Flip time decreases with increasing stress voltage/current**
- **Increasing stress voltage is more effective**

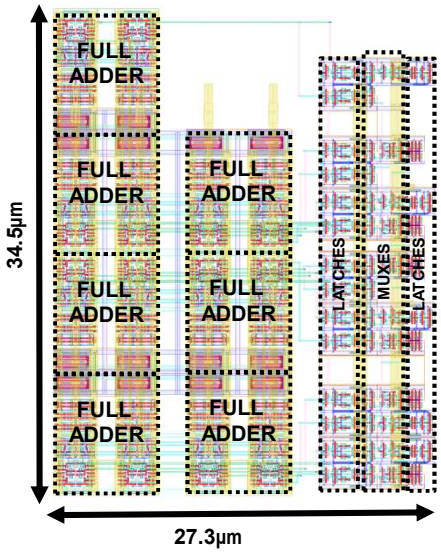
Results: Mean Flip Time (cont.)



PMP-TVD 4-bit Adder Implementation

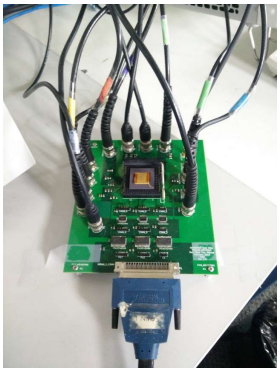
4-bit carry select adders:

- **Pipelined**
- **Two phases:**
  - Precharge
  - Evaluate
- **2-input PMP-TVD gates**
  - Preprogrammed
  - Blank

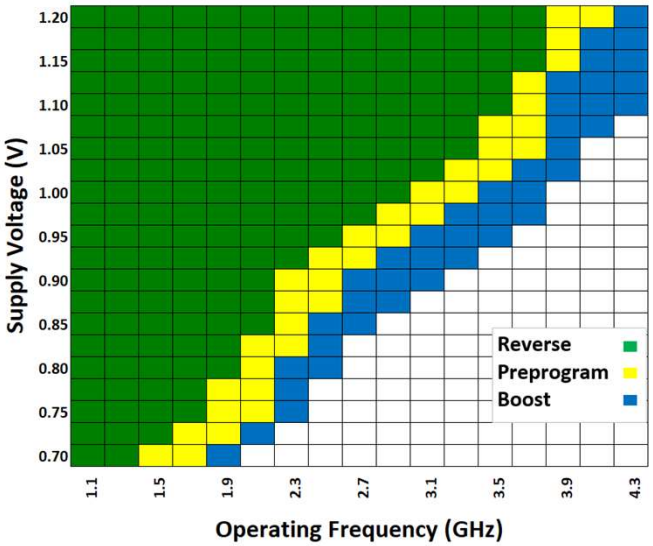


PMP-TVD Testing Methodology

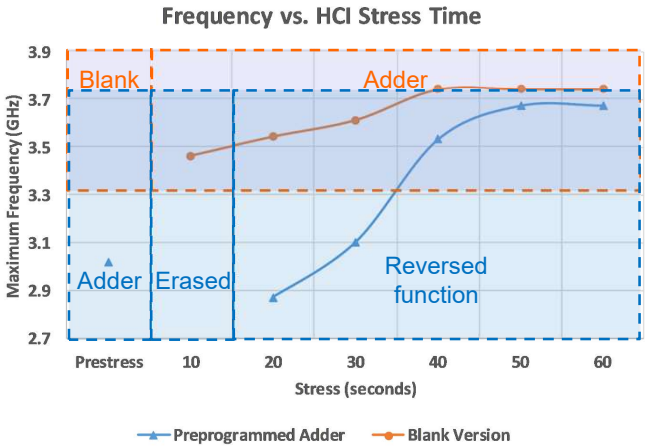
- **Methodology**
  - 1V Core voltage
  - 3V Stress voltage
  - 60 seconds of stress time
  - Room temperature
  - Supply Voltage: 0.7-1.2V
- **Tests**
  - Preprogrammed initial performance
  - Preprogrammed → Boosted
  - Preprogrammed → Reversed
  - Blank → Program



Shmoo Results (65nm)

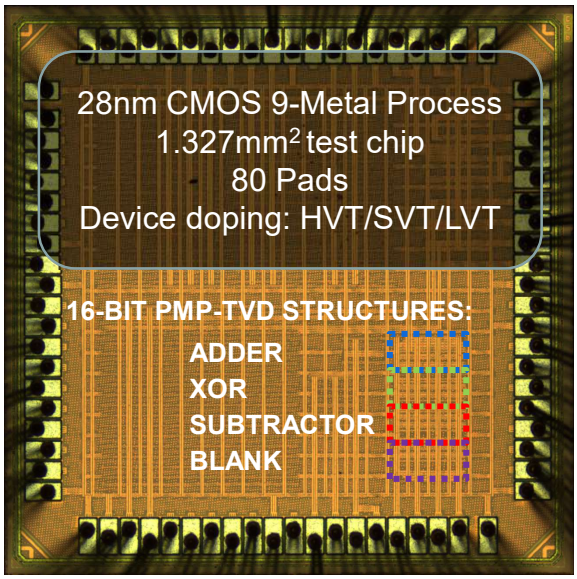


HCI Programming (65nm)



- **HCI programming permanence**
  - Baked the testchip at 125°C for 48 hours in two 24-hour steps

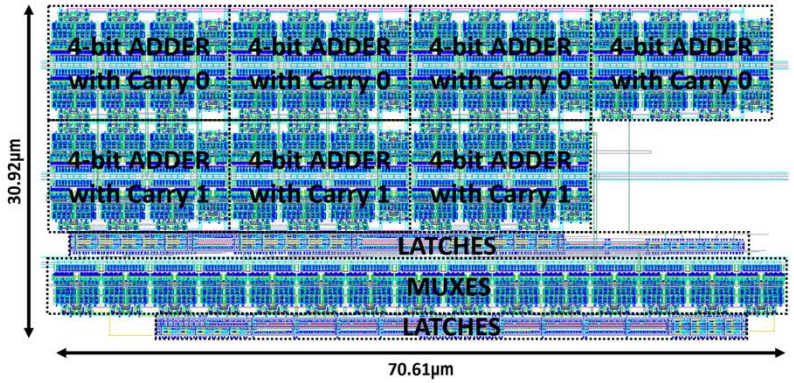
Testchip Die Shot (28nm)



PMP-TVD 16-bit Adder Implementation

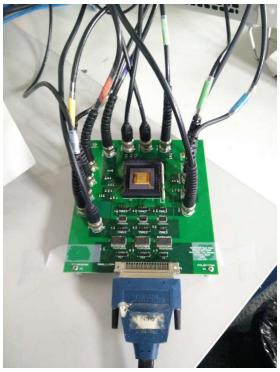
16-bit pipelined carry select adder:

- Two phases: Pre-charge and evaluate
- 2- and 3- input PMP-TVD gates

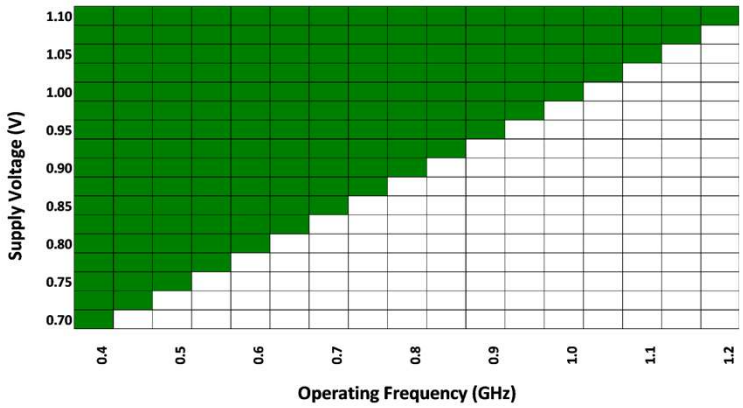


PMP-TVD Testing Methodology

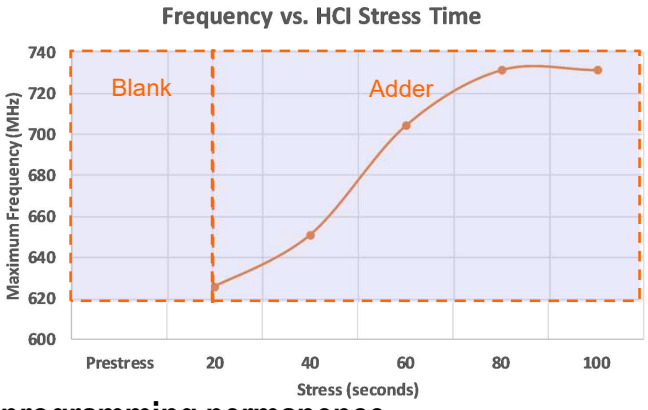
- **Methodology**
  - 0.9V Core voltage
  - 3V Stress voltage
  - 100 seconds of stress time
  - Room temperature
  - Supply Voltage: 0.7-1.1V
- **Tests**
  - Preprogrammed initial performance
  - Preprogrammed → Boosted
  - Preprogrammed → Reversed
  - Blank → Program → **Reprogram**



Shmoo Results (28nm)



HCI Programming(28nm)



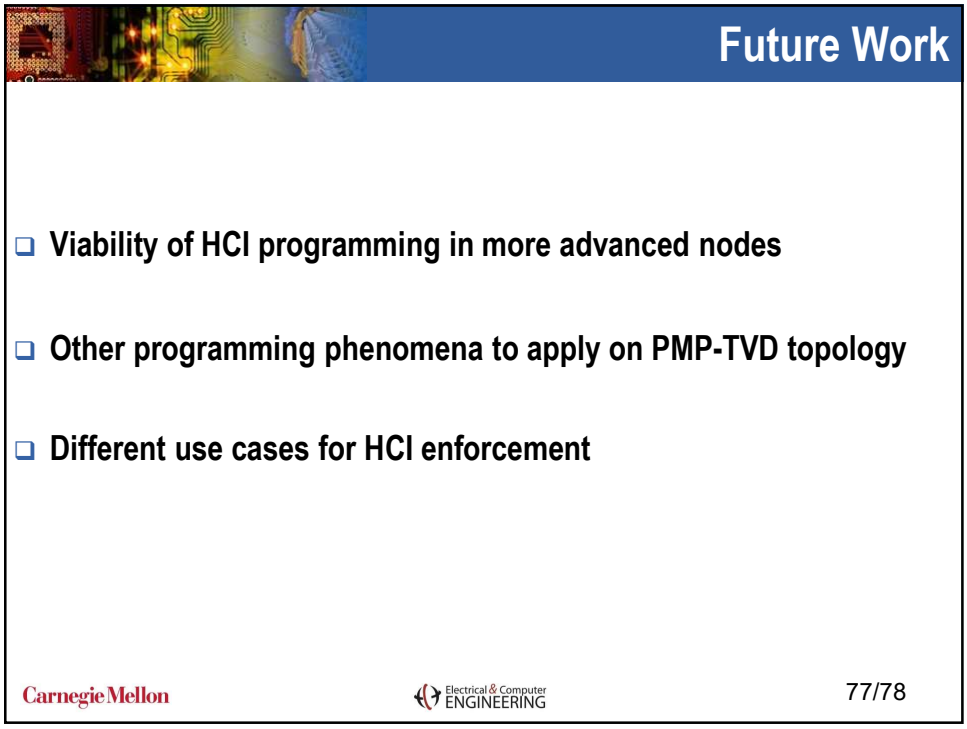
- **HCI programming permanence**
  - Baked the testchip at 130°C for 72 hours in three 24-hour steps
- **HCI reprogramming**
  - 2 write/erase cycles

Measurement Results: Summary

- Applicable in 65nm and 28nm CMOS processes
- Functionality can be enhanced, altered, or erased
- Programming retention after high temperature stress
- HCI reprogramming

Conclusions

- One-size-fits-all solution does not exist
  - Identify vulnerabilities
- Post-manufacturing Programmed Threshold Voltage Defined Logic
  - Secure camouflaging logic family
  - Fully CMOS logic process compatible
- Significant security benefits during manufacturing and deployment
  - Concealment of logic function from fab
  - Distributed and embedded secret information
  - Resilient against SAT-based attacks
  - Low side-channel leakage


Future Work
Viability of HCI programming in more advanced nodes
Other programming phenomena to apply on PMP-TVD topology
Different use cases for HCI enforcement
Carnegie Mellon
Electrical & Computer ENGINEERING
77/78

7.6 A Secure Camouflaged Logic Family Using Post-Manufacturing Programming with a 3.6GHz Adder Prototype in 65nm CMOS at 1V Nominal V_{DD}

Nail Etkin Can Akkaya, Burak Erbagci, Ken Mai

Carnegie Mellon University, Pittsburgh, PA

With the continued globalization of the IC manufacturing supply chain, securing that supply chain is becoming increasingly difficult and this opens the door to a myriad of security threats such as unauthorized production, counterfeiting, IP theft, and hardware Trojan Horses. A parallel and related threat is posed by advanced reverse engineering capabilities, such that even chips manufactured at the most advanced technology nodes can be de-layered, imaged, and analyzed [1]. While various manufacturing methodologies and camouflaged gates have been proposed, none fully address these threats, especially in combination. To address these concerns, we use post-manufacturing programmable camouflaged logic topology to simultaneously obscure the design IP from the manufacturer as well as combat reverse engineering. The basis of the design is a threshold-voltage-defined (TVD) logic gate topology that solely uses different threshold voltage implants to determine the logic gate function [2]. Every gate has an identical physical layout and is post-manufacturing programmed with different threshold voltages for different Boolean functions using intentional directed hot-carrier injection (HCI). Similar intentional HCI techniques have previously been used to enhance SRAM margins, boost PUF reliability, and build TRNGs [3][4]. The design is fully compatible with standard CMOS logic processes, requiring no special layers, structures, or process steps.

Figure 7.6.1 shows our post-manufacturing programmed threshold voltage defined (PMP-TVD) gate which is a pre-charged differential structure with an embedded cross-coupled inverter positive feedback amplifier similar to that used in sense-amplifier-based logic (SABL) [5]. The inputs (A and B) select one branch on each of the left and right sides of the gate, and based on which side pulls more current, the amplifier structure locks to one of the output states. The logic function is post-manufacturing programmed into the gates via intentional directed HCI on the final device in the three NMOS stack leg. A PMP-TVD gate can either be "pre-programmed" with a particular logic function or "blank" (i.e., with no manufactured logic function, nominally balanced like a traditional sense amplifier). Pre-programmed gates use a mixture of HVT and LVT devices in the legs to set the logic function and allow for simpler post-manufacturing testing. Blank gates use all LVT devices and must be HCI programmed before use.

Before logic function programming, all gates are put in reset mode (CLK=0), so the differential outputs of all the gates are 0, turning off all the input pull-down stacks. The bottom stress NMOSes of some legs are turned on (via HCI<0:7>) and the center thick-oxide PMOS is turned on (HCI_bar=0). The boosted V_{DDH} (3V) is applied and the selected stress NMOS devices see the HCI current in the opposite direction of the normal current flow, which results in maximizing the Vt increase of those NMOSes. During normal evaluation, the legs with the stressed NMOSes pull less current than their un-stressed counterparts on the opposite side. Thus, a blank gate can be programmed, a pre-programmed gate can be over-written (different logic function programmed in) or boosted for higher performance (reinforce pre-programmed function), or a gate function can be erased (e.g., for an erase on tamper detection security feature).

The testchip (Fig. 7.6.7) contained three prototype structures: (1) a pipelined 4b carry-select adder using 2-input pre-programmed PMP-TVD gates, (2) a pipelined 4b carry-select adder using 2-input blank PMP-TVD gates, and (3) a 16b carry select adder using 2- and 3- input fixed TVD gates (i.e., no HCI programming devices). In the 4b adders (Fig. 7.6.2), the sum and carry generators are PMP-TVD gates; the MUXes and the latches are standard CMOS gates. Like other dynamic logic families, PMP-TVD gates have 2 phases of operation (precharge and evaluate), so the adders are split into two phases. The first phase consists of the carry and sum generators, and the second phase consists of the carry selection MUXes, with the data values latched in between. The chips were manufactured in a 9-metal layer 65nm bulk CMOS process with a 1V nominal V_{DD}.

Using HCI stress, the pre-programmed PMP-TVD gates can either be "boosted" (HCI stress is used to reinforce the pre-programmed logic function) or "reversed" (HCI stress is used to program in a different logic function than pre-programmed). Fig. 7.6.3 shows the Shmoo plots for the pre-programmed adder design under no stress (baseline), 60 seconds reverse function stress from baseline, and 60 seconds boost stress from baseline. The 60 second reverse function stress fully alters the logic function of the pre-programmed gates. The stress voltage is 3V, resulting in a current density and voltage drop per leg of 18.4mA/μm² and 2.67V.

The pre-programmed 4b adder operates between 1.8-4.08GHz with 0.35-2.15mW power consumption at a supply range of 0.7-1.2V. At nominal 1V $_{VDD}$, it operates at 3.21GHz with 1.14mW power consumption with 13% leakage power. After the same chip is HCI stressed for adder configuration boosting, the operating range became 1.87-4.3GHz with the upper range limited by test structures. After HCI stress, the blank version achieves a similar performance with the same range of operating frequency. Another 4b pre-programmed adder is HCI stressed to reverse the functionality. After the stress, the new function operates between 1.32-3.78GHz with 0.29-1.78mW power consumption at 0.7-1.2V supply. At nominal 1V V_{DD}, it operates at 2.89GHz with 0.96mW power consumption with 14% leakage. The 16b adder with fixed TVD gates operates between 474Mhz-1.21GHz (0.7-1.2V VDD) with a power consumption of 0.889-5.46mW. At nominal V_{DD}, the adder operates at 1.03GHz with a power consumption of 3.22mW with 8% leakage.

Figure 7.6.4 shows the operating frequency of the blank PMP-TVD design as a function of stress time. Even with 10 seconds of stress, the blank design is sufficiently programmed to function correctly as an adder. Further stress reinforces the programming and increases the performance. The blue line shows the efficacy of using stress to reverse a pre-programmed gate, requiring at least 20 seconds of stress before the pre-programmed function is overridden.

To test the permanence of the HCI programming, we baked a test chip at 125°C for 48 hours (in two 24 hour steps) in a temperature chamber. After the initial 24 hours, the structure's maximum frequency at nominal V_{DD} and room temperature decreased from a post-stress 3.74GHz to 3.52GHz. However, after the second 24 hours, the performance of the structure remained the same, showing a slight reversal from baking, but a plateauing and program retention under high temperature [3].

Figure 7.6.6 shows overhead and security comparisons of PMP-TVD gates compared to previously proposed camouflaged gates using dummy vias [6] and fixed TVD [2]. The dummy via design only addresses reverse engineering, and only partially so, since advanced reverse engineering can typically discern real from dummy vias. Fixed TVD gates more fully address reverse engineering and have low side-channel leakage due to their differential gate topology, but they do not address untrusted fab or have the ability to erase or re-program the logic function. PMP-TVD gates address both untrusted fab and reverse engineering threats, as well as having low side-channel leakage due to also having a differential gate topology.

Acknowledgements:
The authors would like to thank DARPA for funding in support of this work.

References:

[1] R. Torrance and D. James, "Reverse Engineering in the Semiconductor Industry," *CICC*, pp. 429-436, 2007.
[2] B. Erbagci, et al., "A Secure Camouflaged Threshold Voltage Defined Logic Family," *IEEE HOST*, pp. 229-235, 2016.
[3] M. Bhargava and K. Mai, "A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement," *CHES*, LNCS vol. 8086, pp. 90-106, 2013.
[4] K. Miyaji, et al., "A 6T SRAM with a Carrier-injection Scheme to Pinpoint and Repair Fails That Achieves 57% Faster Read and 31% Lower Read Energy," *ISSCC*, pp. 232-234, 2012.
[5] K. Tiri, et al., "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," *ESSCIRC*, pp. 403-406, 2002.
[6] J. Rajendran, et al., "Security Analysis of Integrated Circuit Camouflaging," *ACM CCS*, pp. 709-720, 2013.

 978-1-5090-4940-0/18/$31.00 ©2018 IEEE

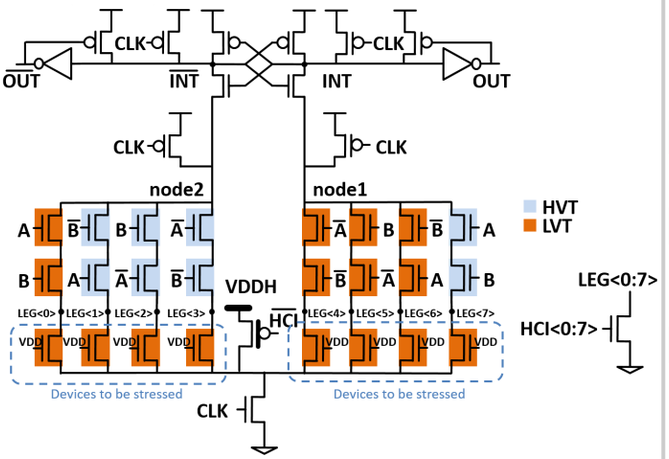


Figure 7.6.1: Schematic of a 2-input PMP-TVD logic gate pre-programmed as a NAND. The stress NMOSes used to program, boost, reverse, or erase the logic function are marked in the blue dashed lines.

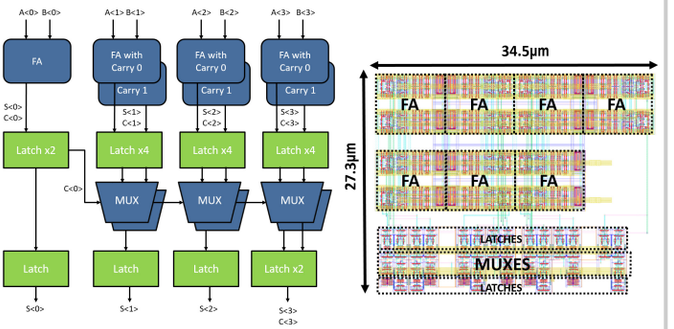


Figure 7.6.2: Structure and layout of the 4b PMP-TVD carry select adder.

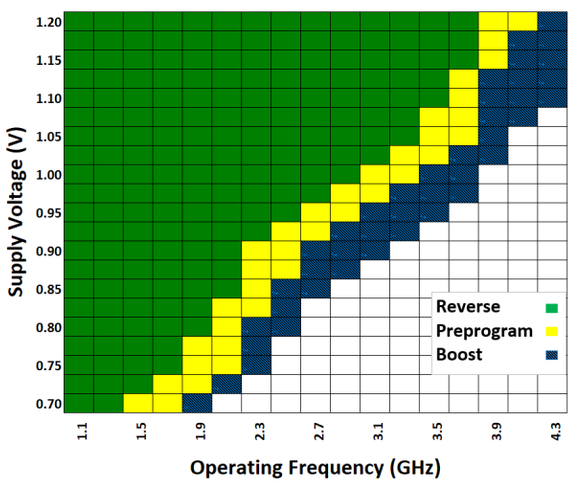


Figure 7.6.3: Shmoo plot at room temperature for the 4b PMP-TVD pre-programmed adder: pre-programmed baseline (yellow), 1 minute of reverse stress (green), and 1 minute of boost stress (blue).

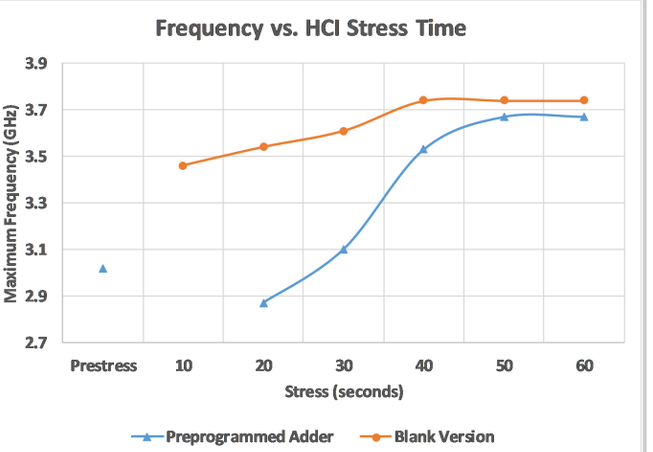


Figure 7.6.4: Frequency vs. HCI stress time plot of 4b blank PMP-TVD adder at 1V and room temperature (orange). Also, blue line shows stress time needed to reverse pre-programmed PMP-TVD adder (20 seconds) and subsequent boosting of the reverse function.

	4-bit PMP-TVD (pre-prog)	4-bit PMP-TVD (reverse)	4-bit PMP-TVD (boost)	4-bit PMP-TVD (blank)	16-bit TVD adder
Area (w/ test)	0.007mm²				0.029mm²
Area (core)	0.001mm²				0.003mm²
Freq. @ 1V	3.2GHz	2.9GHz	3.7GHz	3.6GHz	1.0GHz
Power @ 1V	1.14mW	0.96mW	1.09mW	1.09mW	3.22mW
Leakage @ 1V	0.15mW	0.14mW	0.14mW	0.14mW	0.26mW

Figure 7.6.5: Silicon results for 4-bit PMP-TVD (no stress), 4b PMP-TVD (60s reverse stress), 4b PMP-TVD (60s boost stress), 4b PMP-TVD (blank, 60s adder program), and 16b fixed TVD adder at 1V nominal V_{DD} and room temperature.

Overhead vs. Static CMOS Std. Cell

	Dummy via[6]			TVD[2]			PMP-TVD (This Work)		
	Power	Delay	Area	Power	Delay	Area	Power	Delay	Area
NAND	6.5X	2.6X	5X	1.6X	3.2X	3.7X	9.2X	6.6X	7.3X
NOR	6.1X	2.1X	5X	1.9X	2.6X	3.7X	4X	5.4X	7.3X
XOR	1.8X	1X	2.2X	1.1X	1.7X	1.5X	1.8X	3.4X	3X

Security Comparison

	Dummy via[6]	TVD[2]	PMP-TVD (This Work)
Low Side-channel Leakage		●	●
Untrusted Fab			●
Reverse Engineering	◐	●	●
Erasable/Programmable			●

Figure 7.6.6: Overhead comparison of dummy via [6], TVD [2], and PMP-TVD gates normalized to static CMOS standard cells. Also, security comparison of these gate types. Black dot indicates the extent that the gate type addresses the security threat (fully or partially).

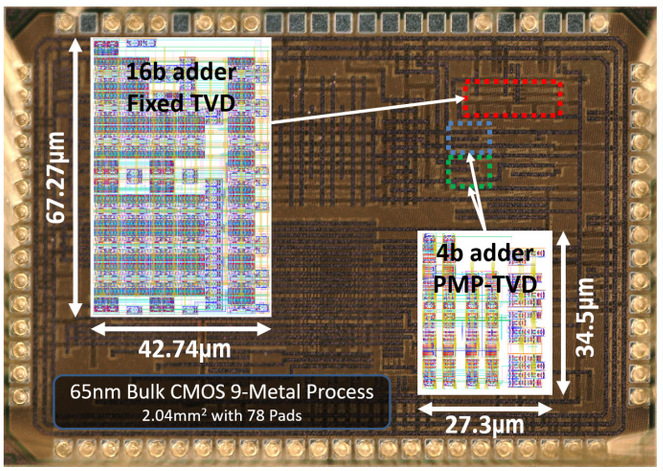


Figure 7.6.7: Die shot of the test chip. 16b TVD adder (red), 4b PMP-TVD adder (green) and 4b PMP-TVD blank structure (blue) are highlighted.

978-1-5090-4940-0/18/$31.00 ©2018 IEEE

A Secure Camouflaged Logic Family Using Post-Manufacturing Programming with a 3.6GHz Adder Prototype in 65nm CMOS at 1V Nominal V_{DD}

Nail Etkin Can Akkaya, Burak Erbagci, Ken Mai

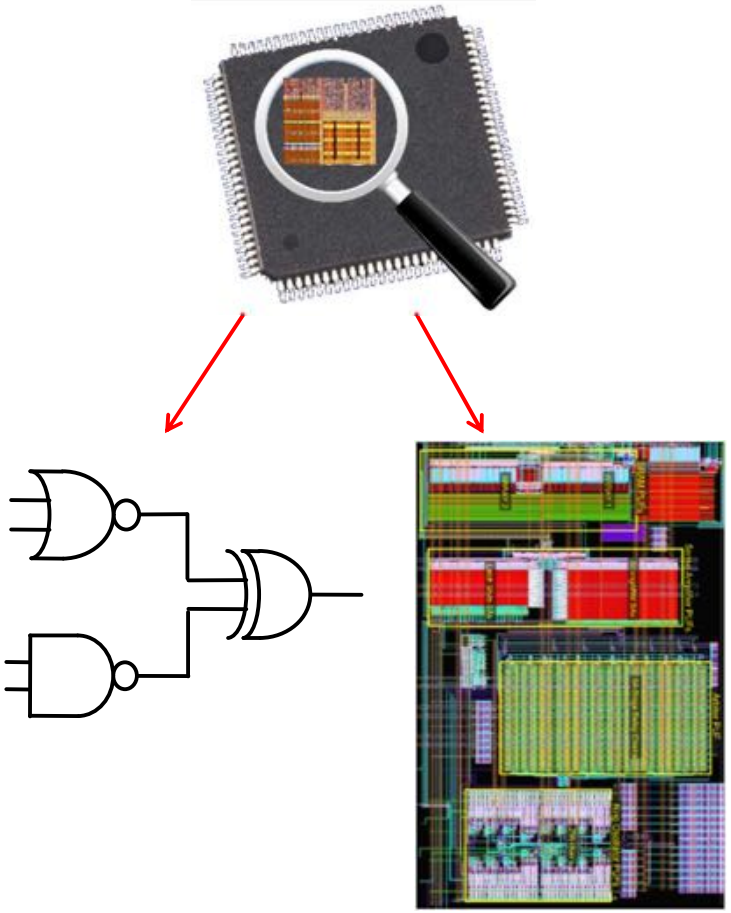
Carnegie Mellon University, USA

Supply Chain and Reverse Engineering Threats

“VAX – when you care to steal the very best”

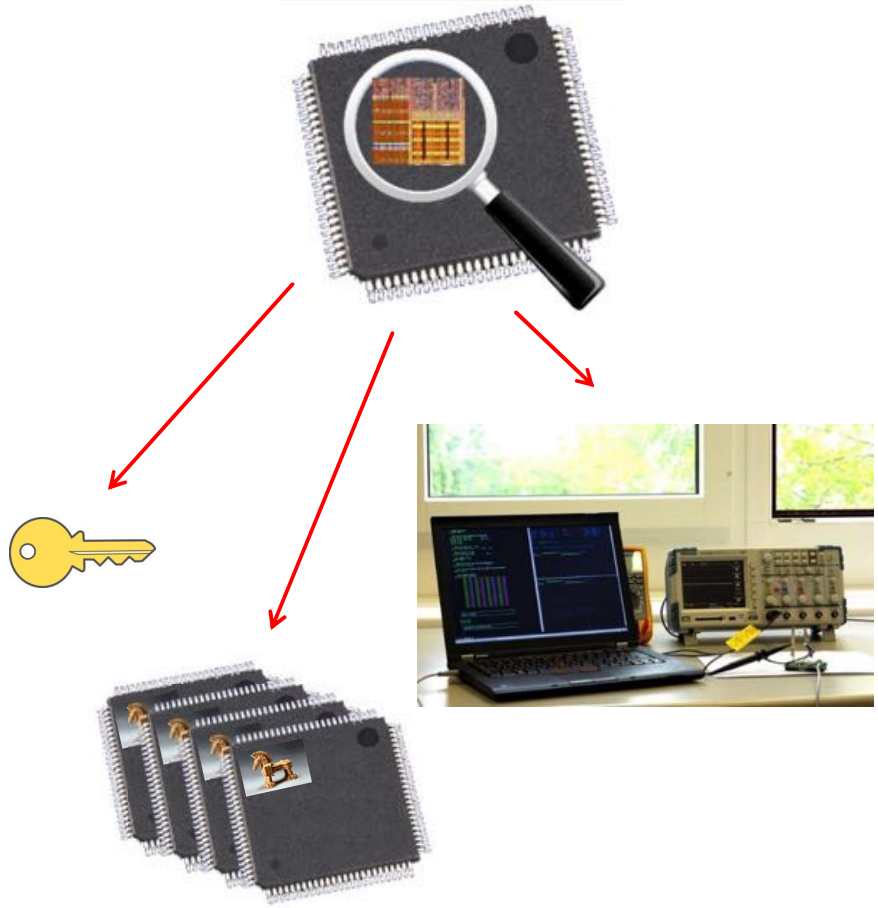
Reverse Engineering Goals

- Reverse engineer wants to learn
  - Functionality
  - Internal structure
  - Manufacturing process details
- Uses for the extracted information
  - Steal intellectual property and secrets
  - Create clones or insert trojans
  - Enhance other attacks

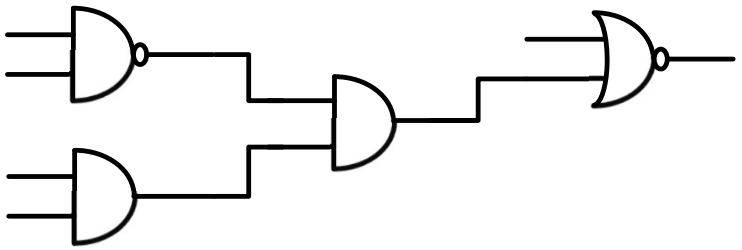


Reverse Engineering Goals

- Reverse engineer wants to learn
  - Functionality
  - Internal structure
  - Manufacturing Process Details
- Uses for the extracted information
  - Steal intellectual property and secrets
  - Create clones or insert trojans
  - Enhance other attacks

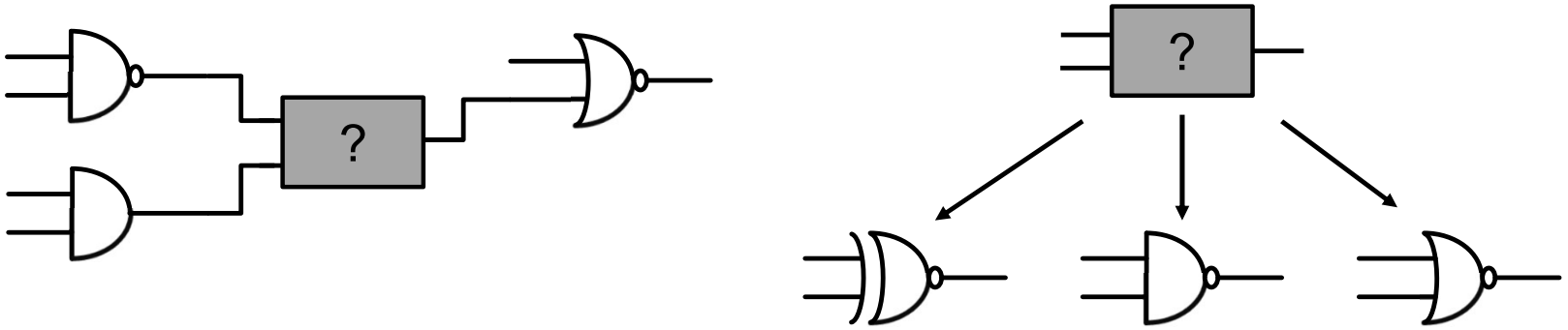


Camouflaged Gates



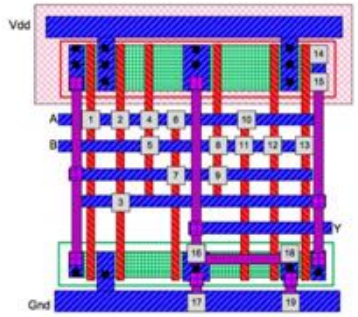
- Hide logical function of gate from attacker
- Use look-alike gates
  - Very similar layouts
  - Different Boolean function
- Replace some gates with camouflaged ones

Camouflaged Gates

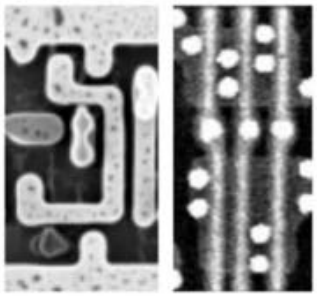


- Hide logical function of gate from attacker
- Use look-alike gates
  - Very similar layouts
  - Different Boolean function
- Replace some gates with camouflaged ones

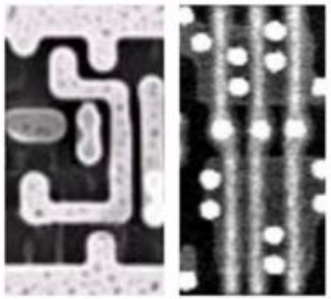
Issues with Current Camouflaged Gates



Dummy via[1]



AND2 gate[2]

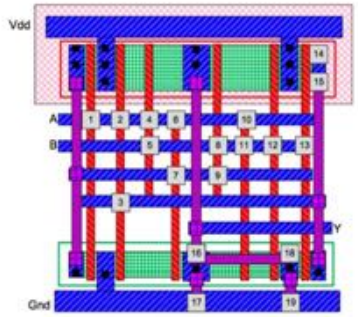


AND2 look-alike gate[2]

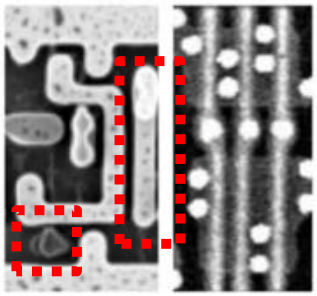
- Security relies on limited reverse engineering resolution
  - Dummy contact detectable with careful de-processing
  - Look-alike gates may be discernable
- Incompatibility with standard process and tools
  - Additional mask layers and process steps
  - DRC waivers and non-standard structures

[1] Rajendran et al., CCS'13
[2] Syphermedia

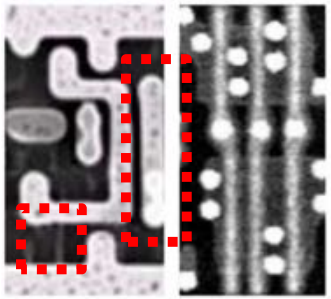
Issues with Current Camouflaged Gates



Dummy via[1]



AND2 gate[2]

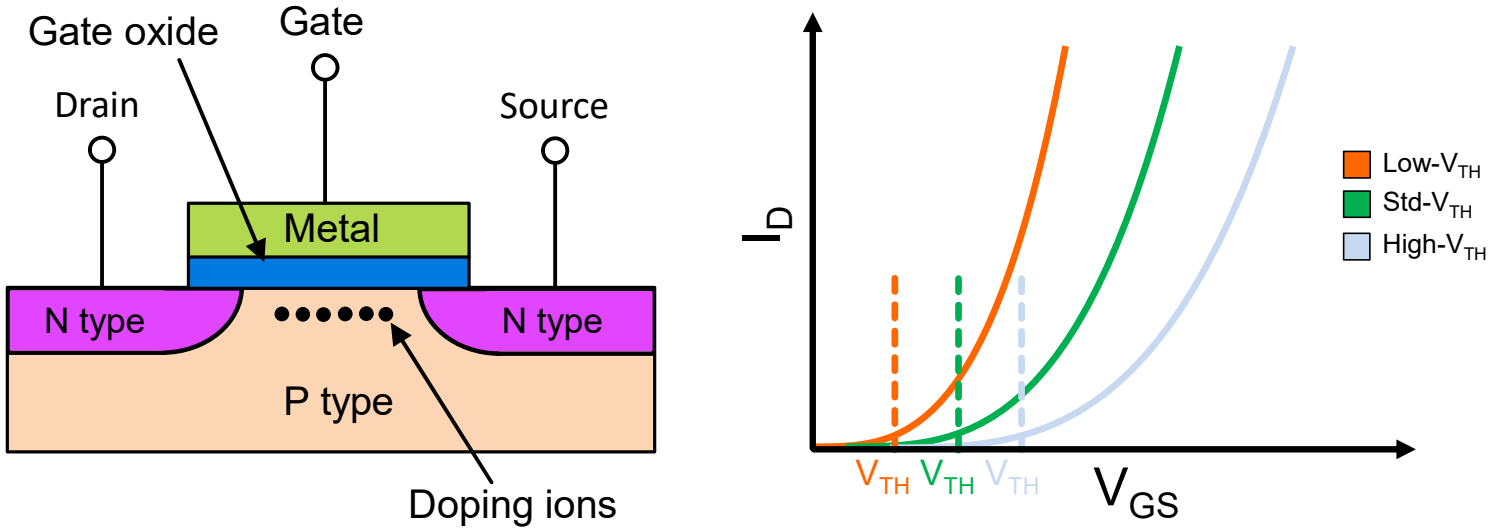


AND2 look-alike gate[2]

- Security relies on limited reverse engineering resolution
  - Dummy contact detectable with careful de-processing
  - Look-alike gates may be discernable
- Incompatibility with standard process and tools
  - Additional mask layers and process steps
  - DRC waivers and non-standard structures

[1] Rajendran et al., CCS'13
[2] Syphermedia

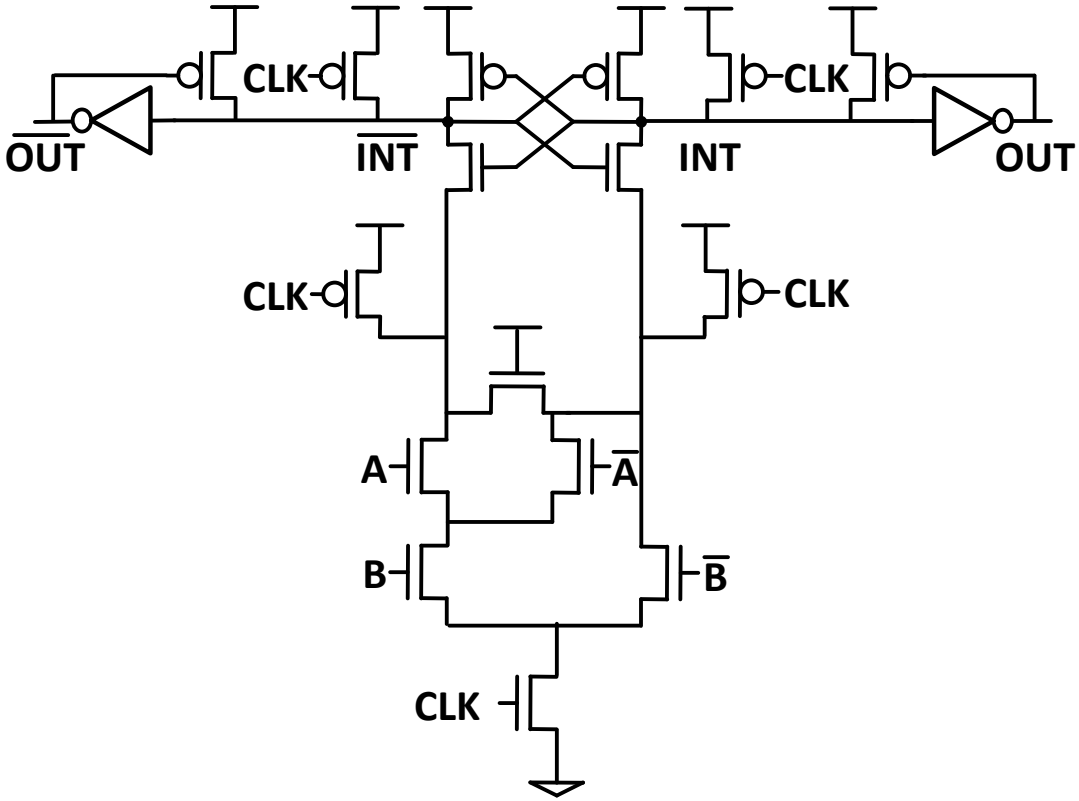
Threshold Voltage Defined (TVD) Logic



- Today's processes offer multiple transistor V_{TH}'s
- Devices differ only in # ions implanted in the channel
- Allow designers to trade-off speed and power

Sense-Amplifier Based Logic

- Dual-rail dynamic logic
- Two phases
  - Precharge
  - Evaluate

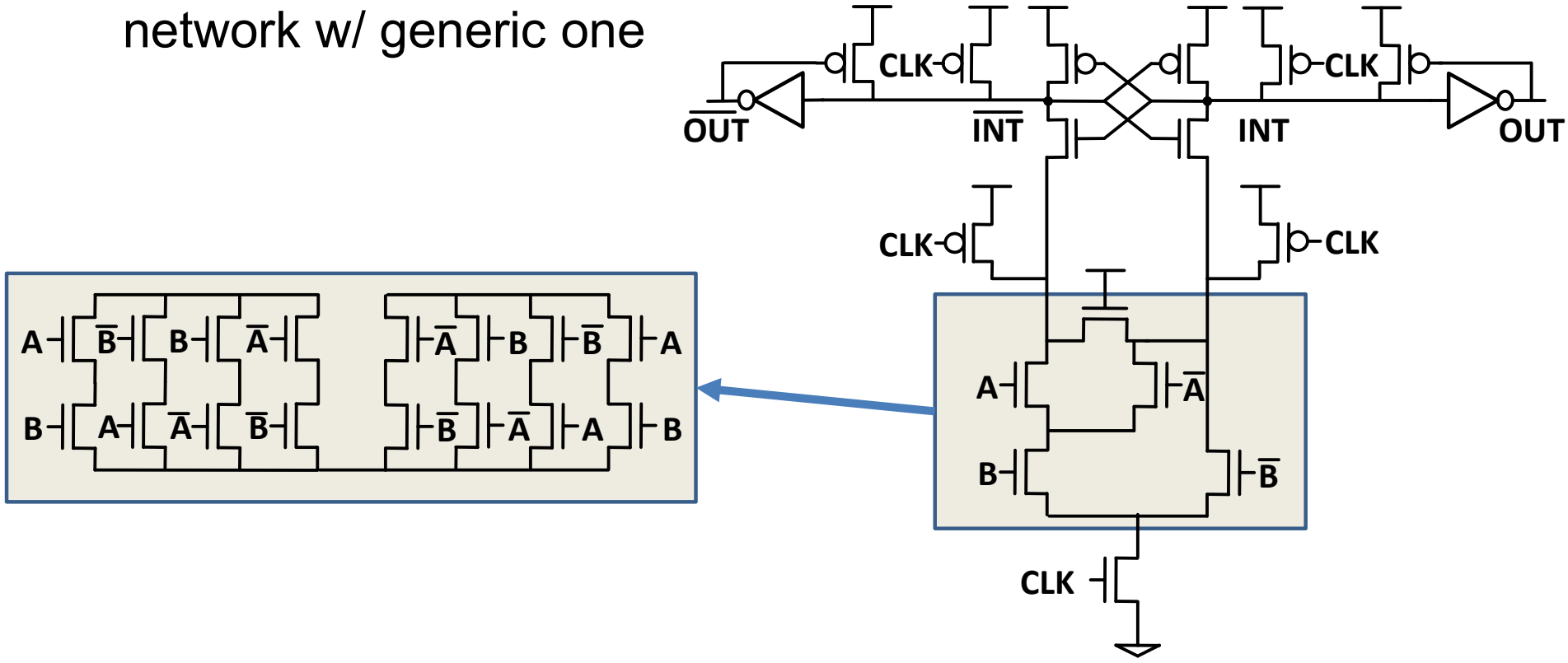


A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

[1] Tiri et al., ESSCIRC'02

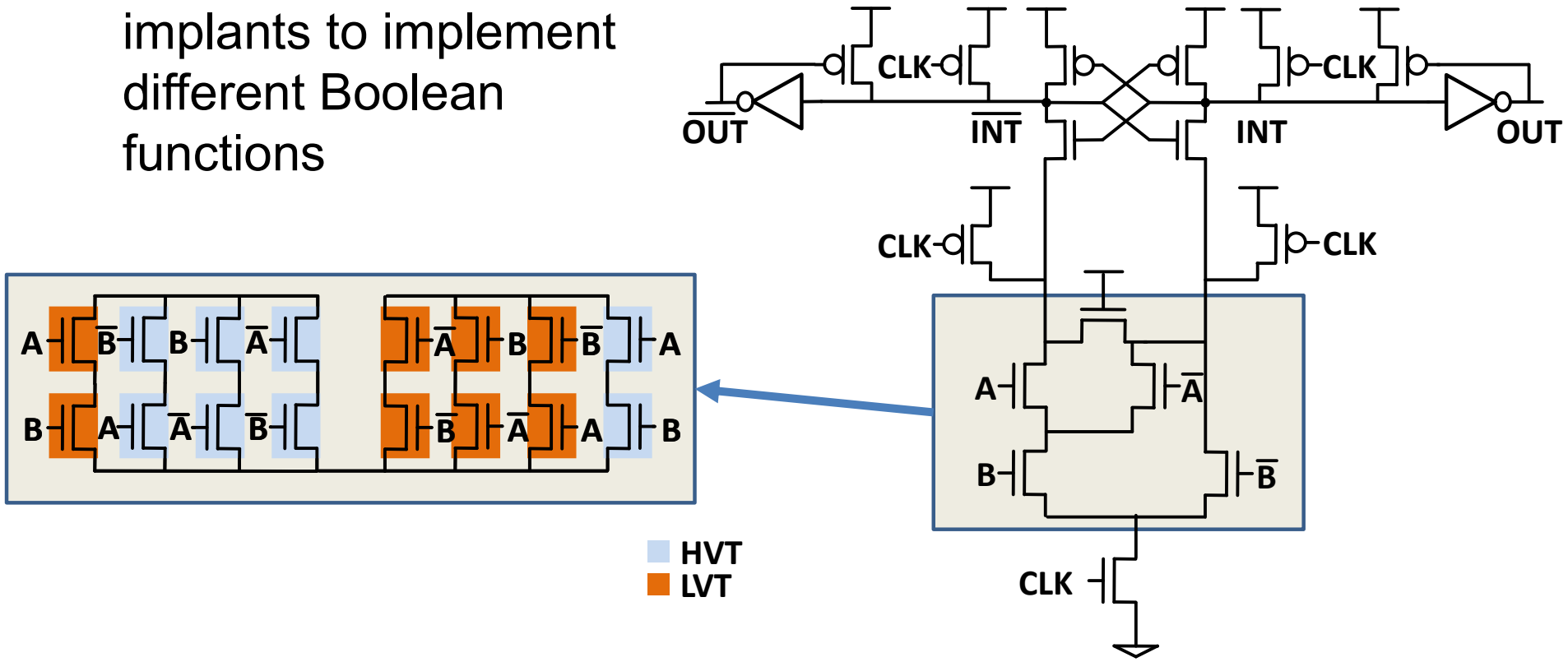
Threshold Voltage Defined (TVD) Logic

- Replace the pull-down network w/ generic one



Threshold Voltage Defined (TVD) Logic

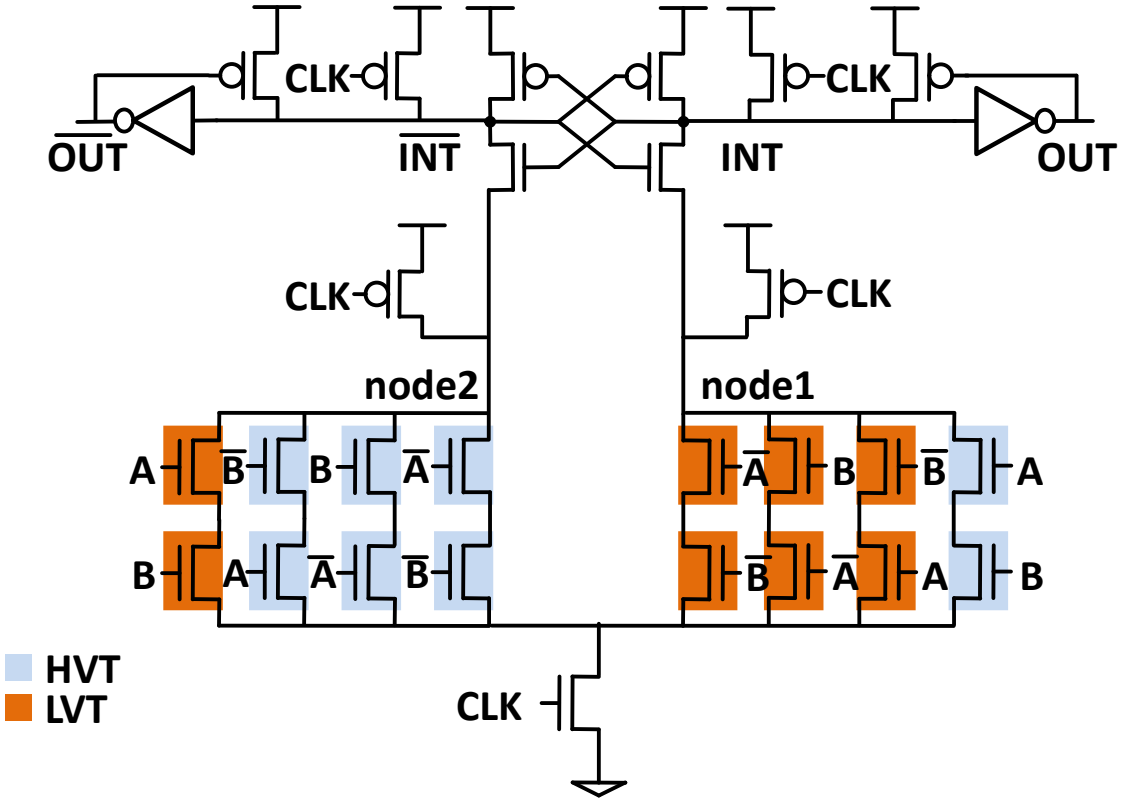
- Use different V_{TH} implants to implement different Boolean functions



Threshold Voltage Defined (TVD) Logic

- Generic differential pull-down network
- Both branches conduct briefly
- ΔI is amplified
- Different V_{TH} implants

A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

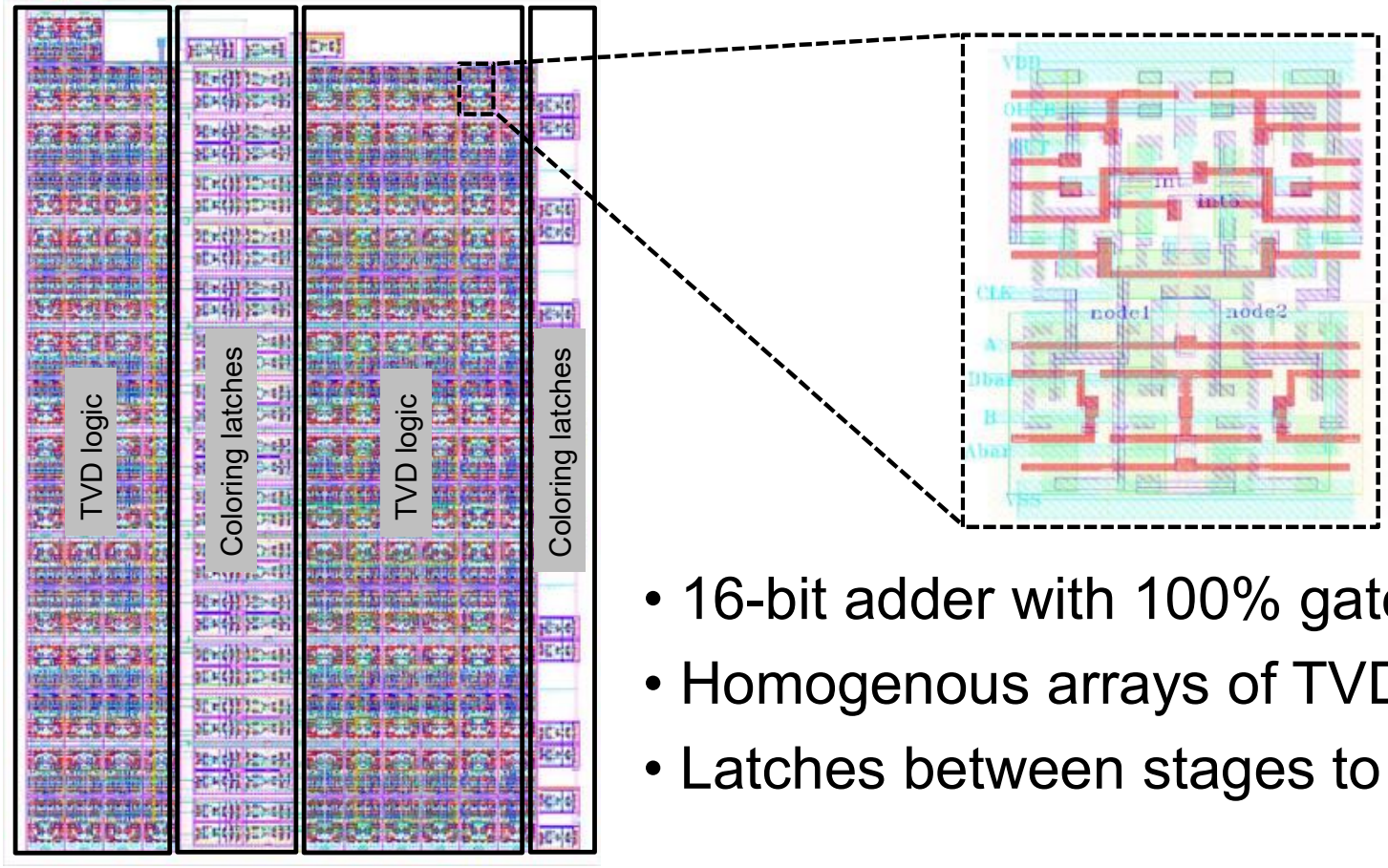


[1] Erbagci et al., HOST'16

TVD Camouflaging Advantages

- Security not reliant on limited reverse engineering resolution
  - Different V_{TH} implants to set logic function
  - Identical layout
- Fully CMOS logic process compatible
  - No special layers, masks, or DRC waivers needed
- Low side-channel emissions
  - Due to differential structure and homogeneity

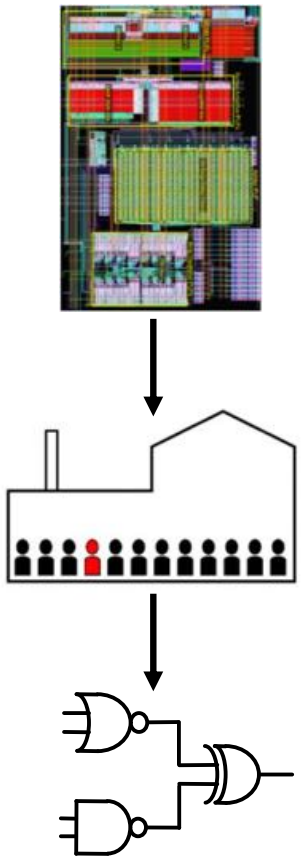
Example 16-bit Adder Layout



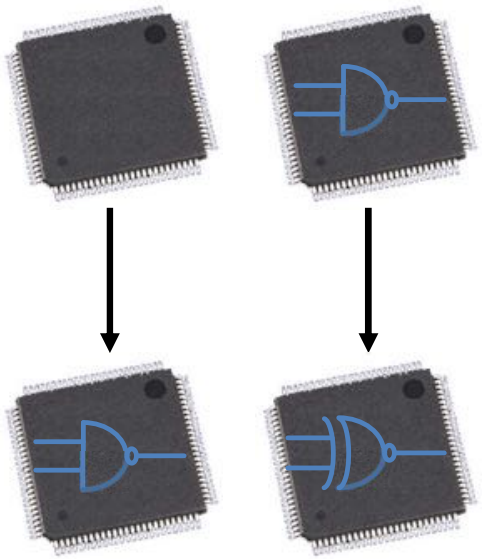
- 16-bit adder with 100% gate replacement
- Homogenous arrays of TVD logic gates
- Latches between stages to color logic

Supply Chain Security Issues

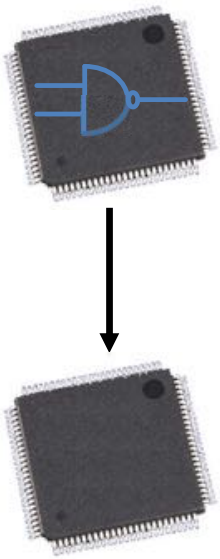
Untrusted Fabrication



Programmable

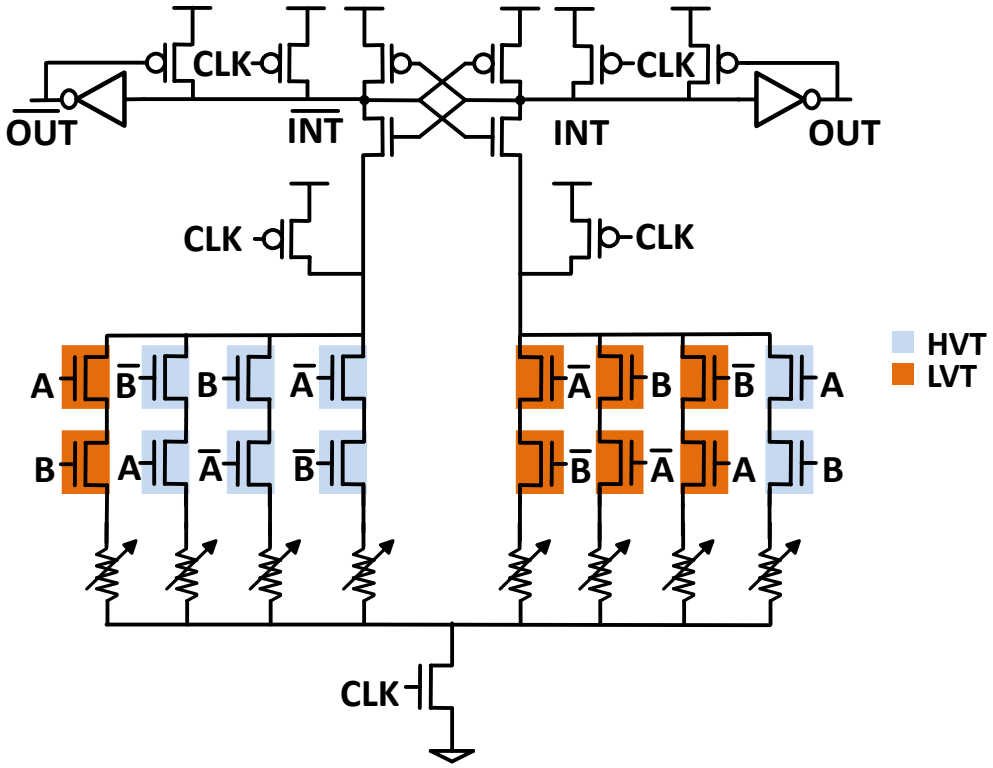


Erasable



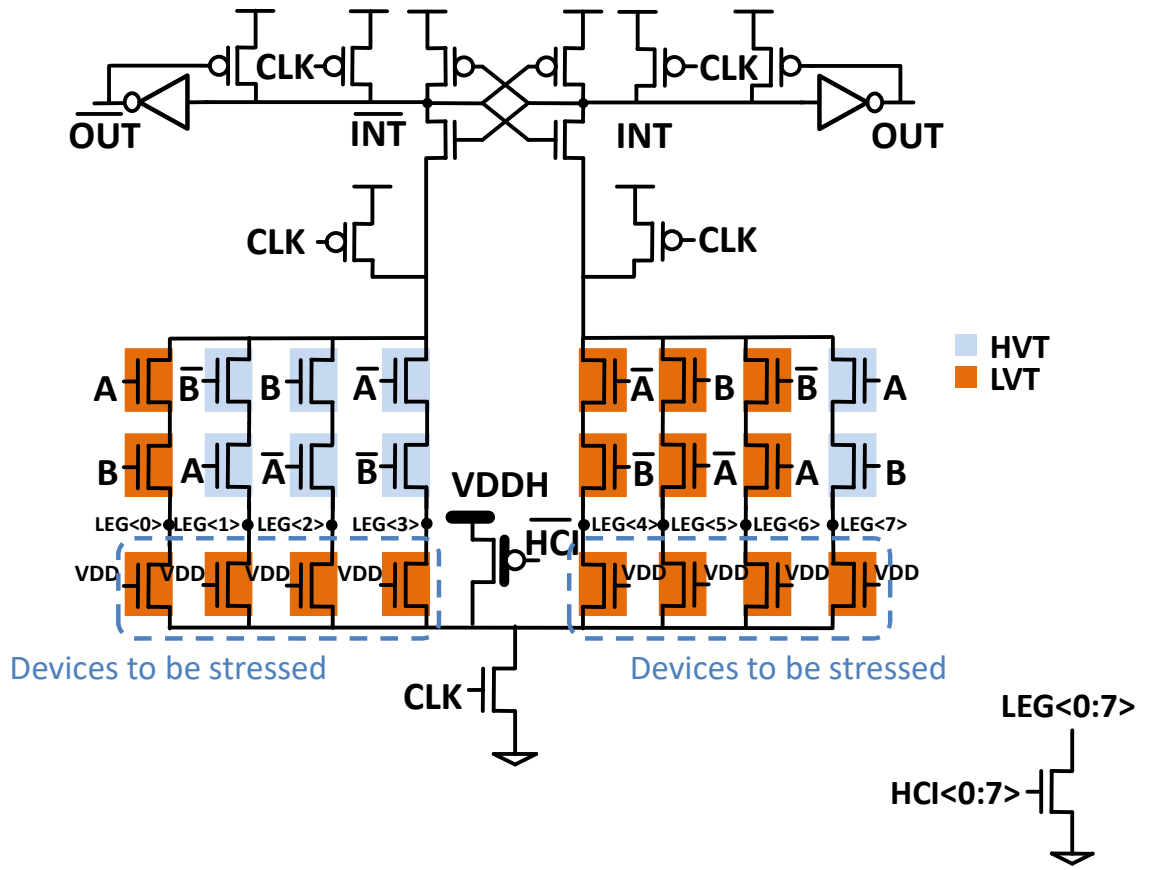
Post-Manufacturing Programmed TVD Logic

- Countermeasure against untrusted fabrication
  - Fab does not have logic gate Boolean function
- Hot-carrier injection programming
  - Programmable
  - Erasable
- Programming options
  - Preprogrammed
  - Blank

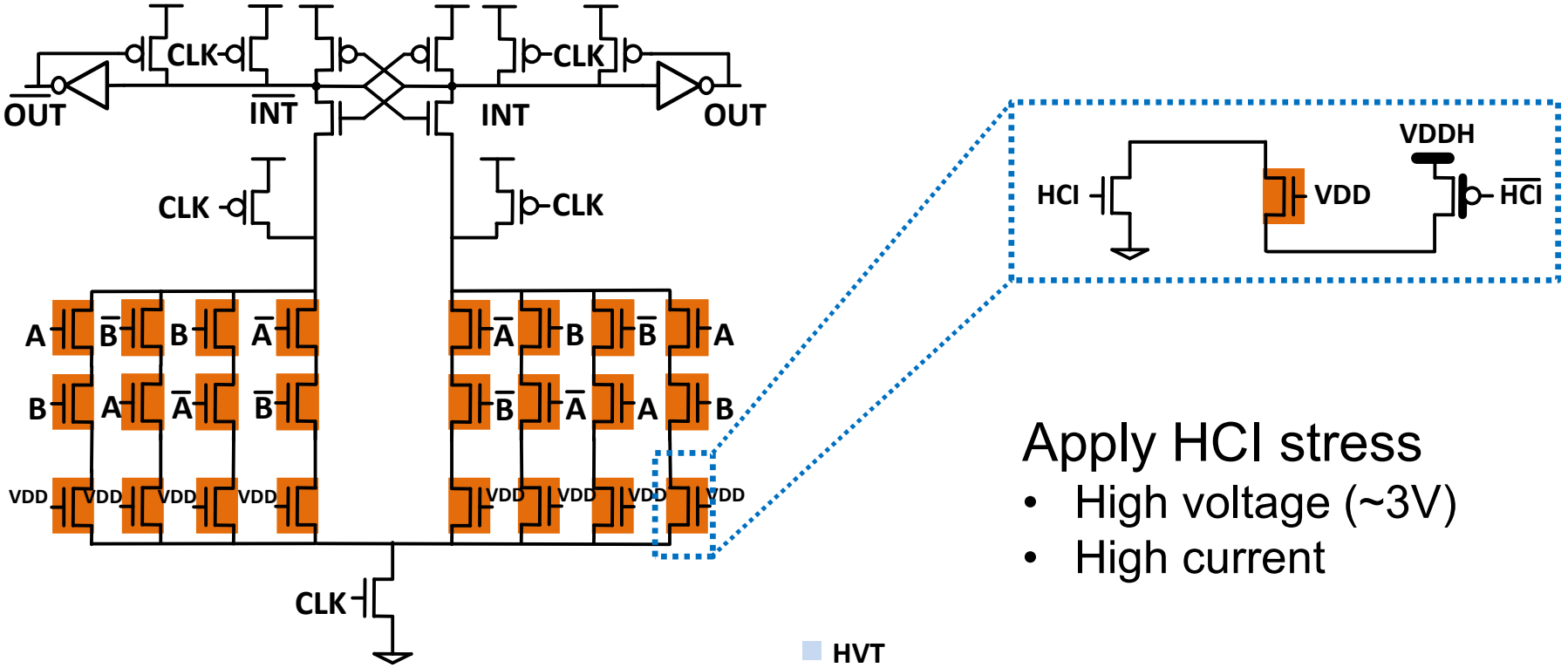


Post-Manufacturing Programmed TVD Logic

- Countermeasure against untrusted fabrication
  - Fab does not have logic gate Boolean function
- Hot-carrier injection programming
  - Programmable
  - Erasable
- Programming options
  - Preprogrammed
  - Blank



Blank PMP-TVD Logic Gate Programming

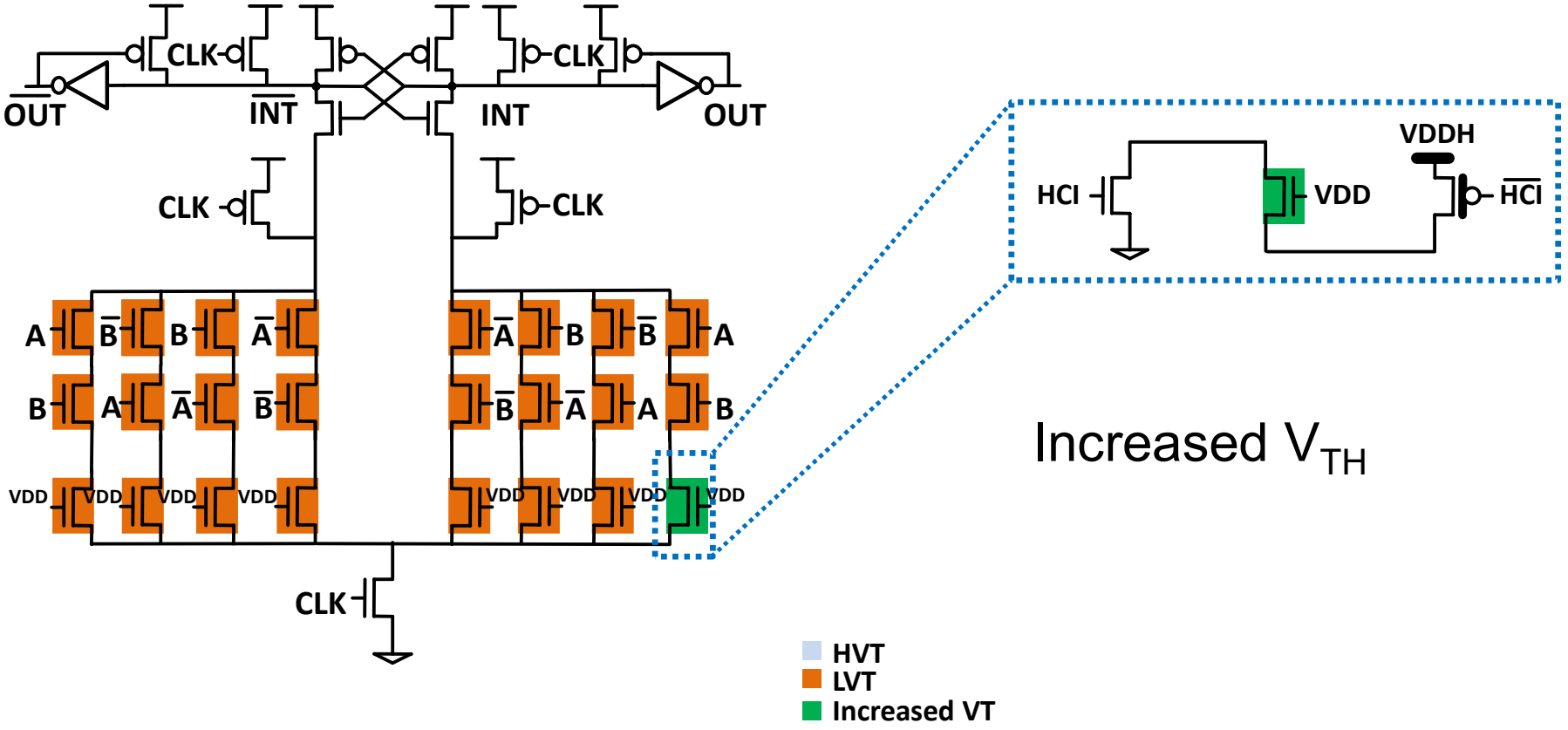


Apply HCI stress

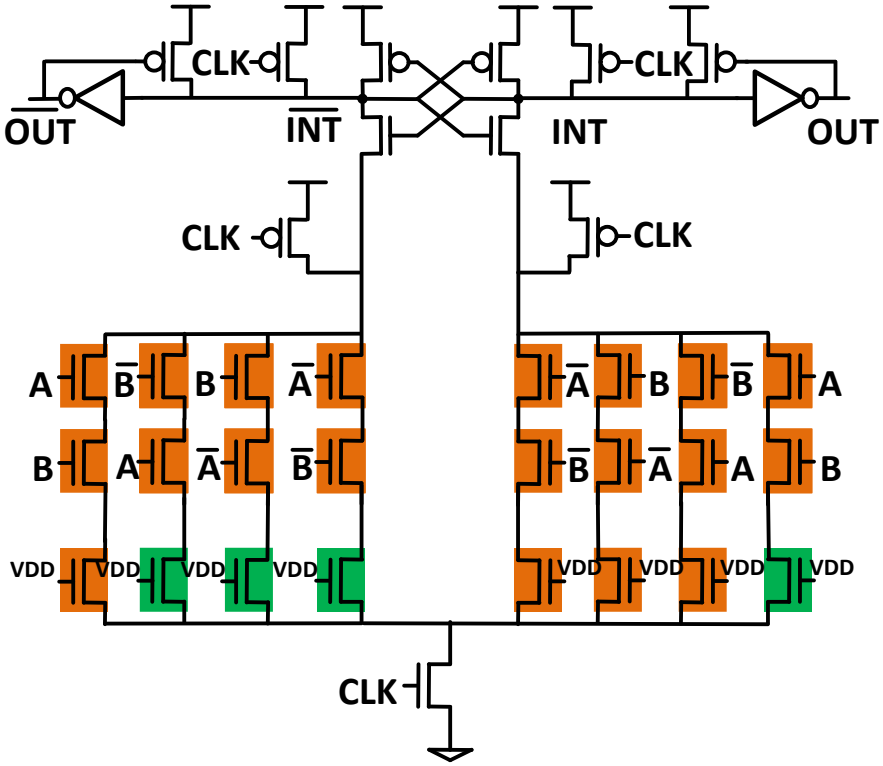
- High voltage (~3V)
- High current

HVT
LVT
Increased VT

Blank PMP-TVD Logic Gate Programming



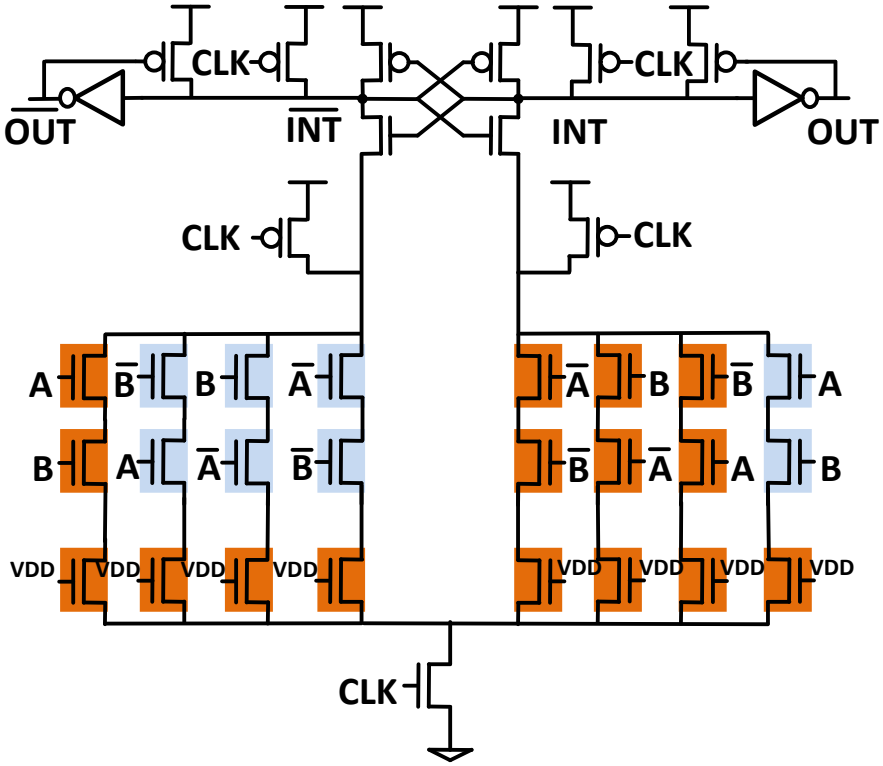
Blank PMP-TVD Logic Gate Programming



A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

HVT
LVT
Increased VT

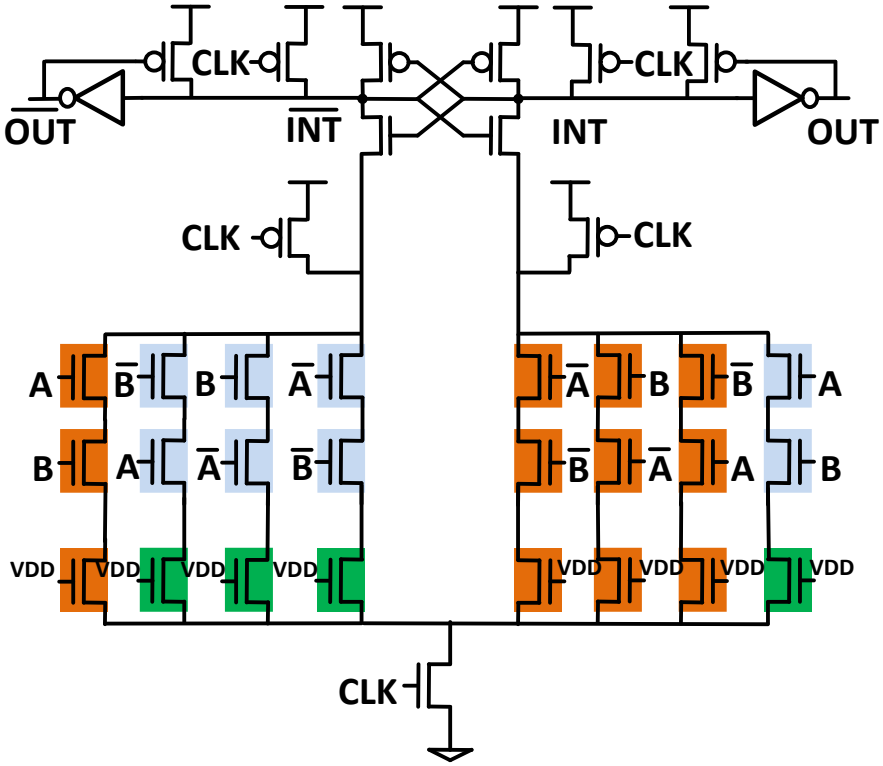
Preprogrammed PMP-TVD Logic Gate Programming



A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

HVT
LVT
Increased VT

Preprogrammed PMP-TVD Logic Gate Programming

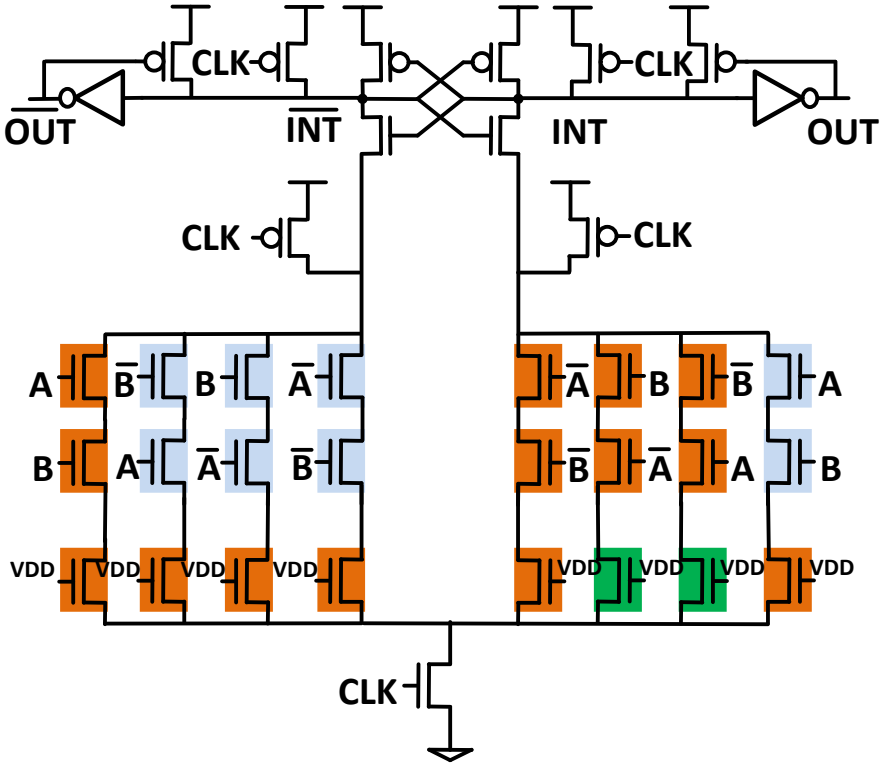


A	B	NAND (OUT)	AND ($\overline{OUT}$)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	0	1

Boost performance

HVT
LVT
Increased VT

Preprogrammed PMP-TVD Logic Gate Programming



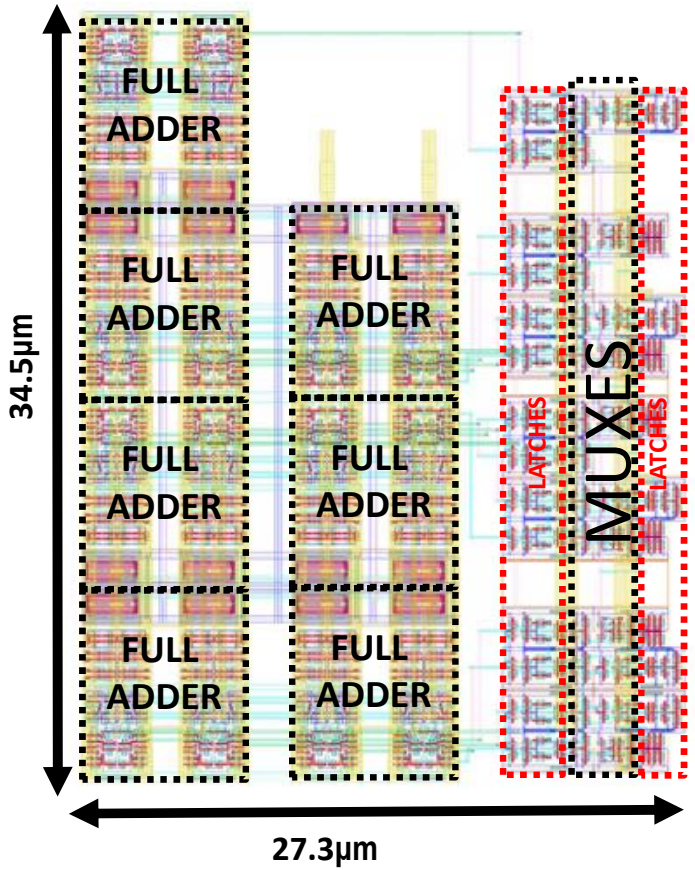
A	B	NOR (OUT)	OR ($\overline{OUT}$)
0	0	1	0
1	0	0	1
0	1	0	1
1	1	0	1

Change function

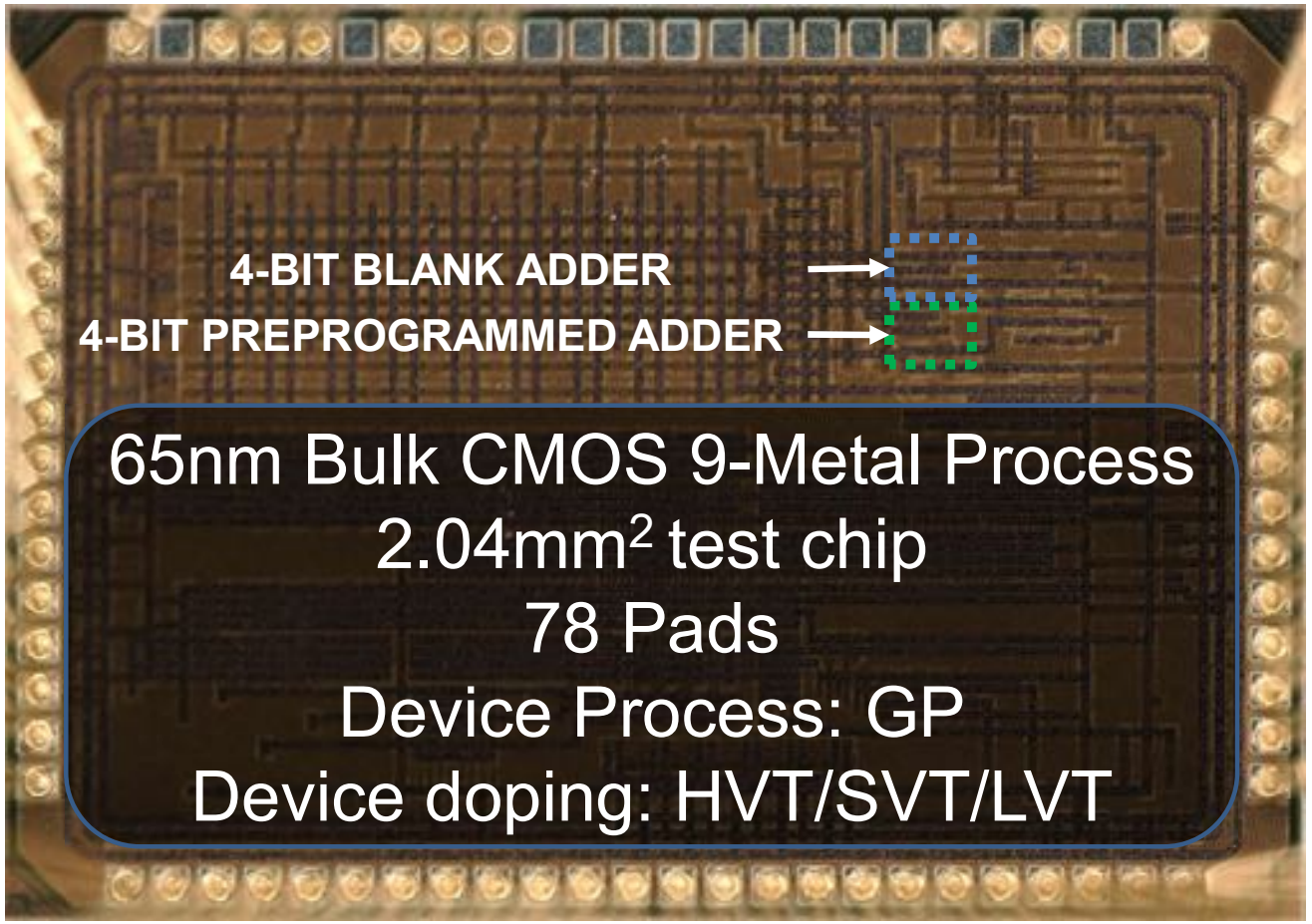
HVT
LVT
Increased VT

PMP-TVD Adder Designs

- 4-bit carry select adders
  - Pipelined
  - Two phase dynamic
  - 2-input PMP-TVD gates
- Adder versions
  - Preprogrammed
  - Blank



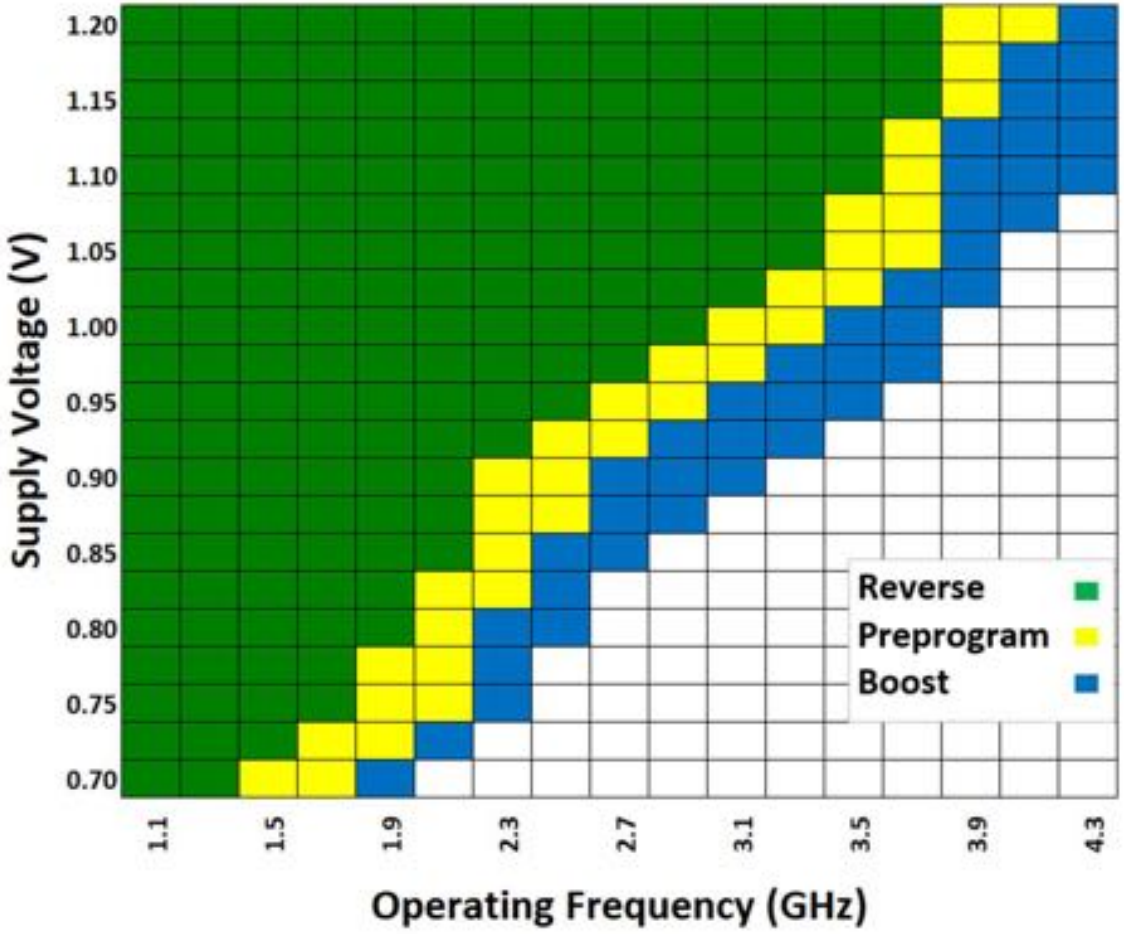
Testchip Die Shot



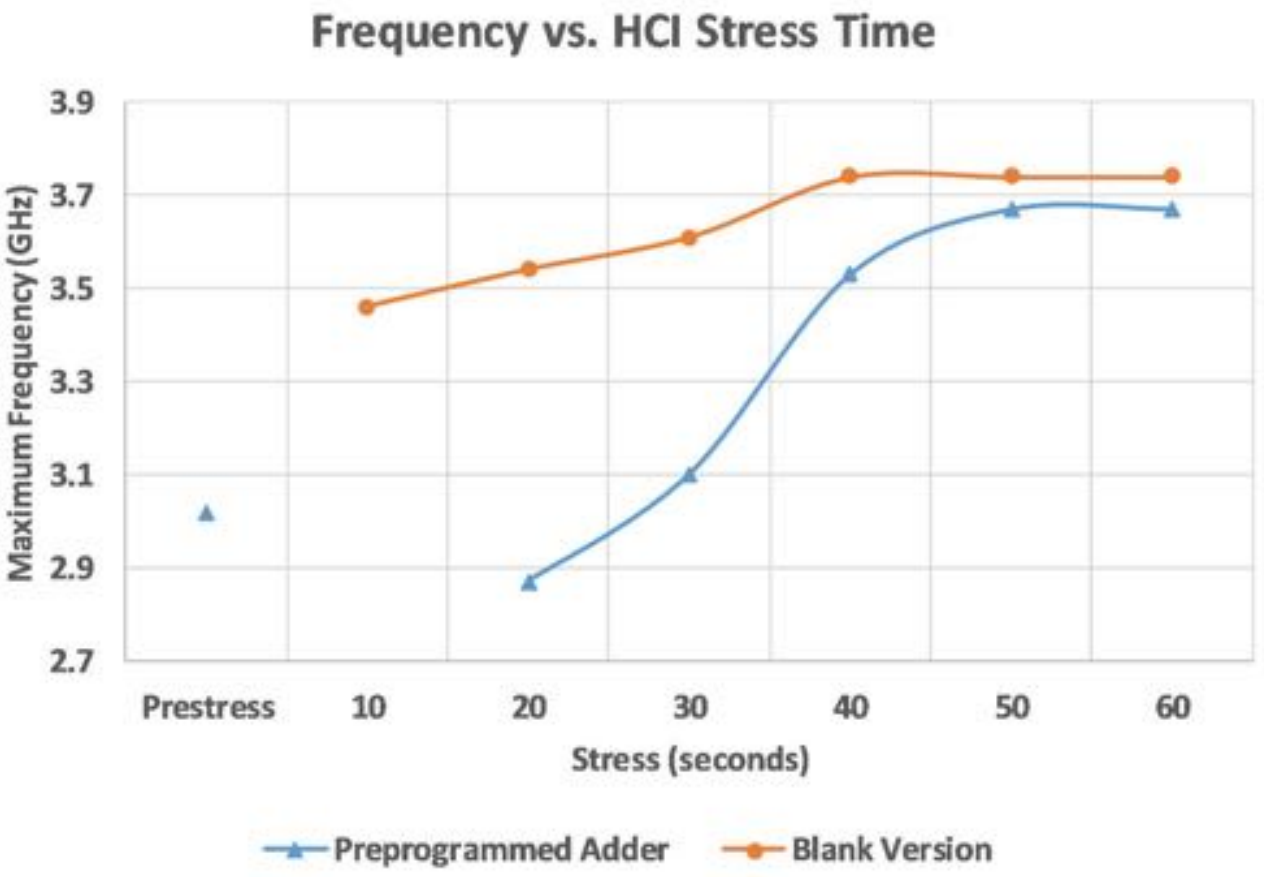
Testing Methodology

- Methodology
  - 1V core voltage
  - 3V stress voltage
  - 60 seconds of stress time
  - Supply Voltage: 0.7-1.2V
  - Room temperature
- Tests
  - Preprogrammed initial performance
  - Preprogrammed → Boosted
  - Preprogrammed → Reversed
  - Blank → Programmed

PMP-TVD Preprogrammed Adder Shmoo

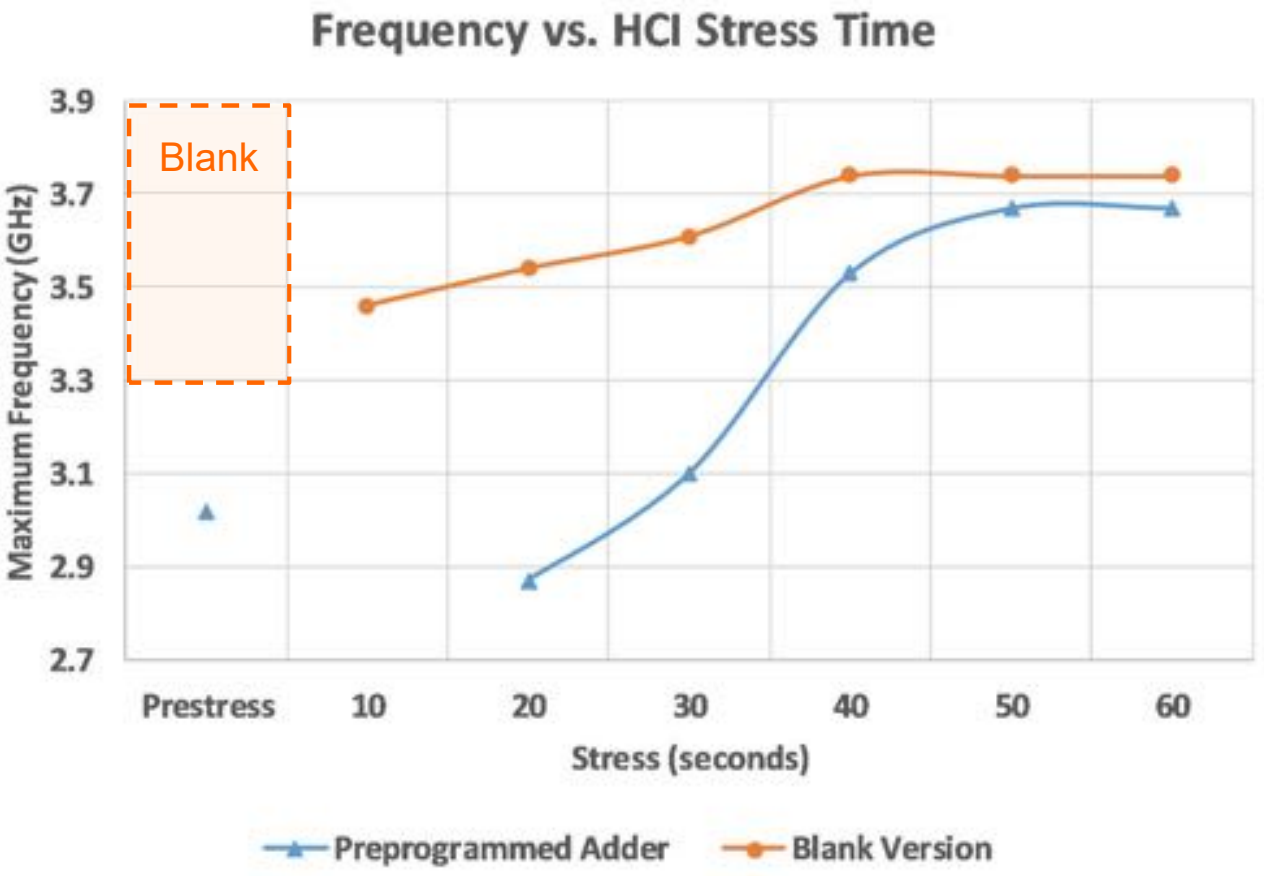


Stress Time vs Performance



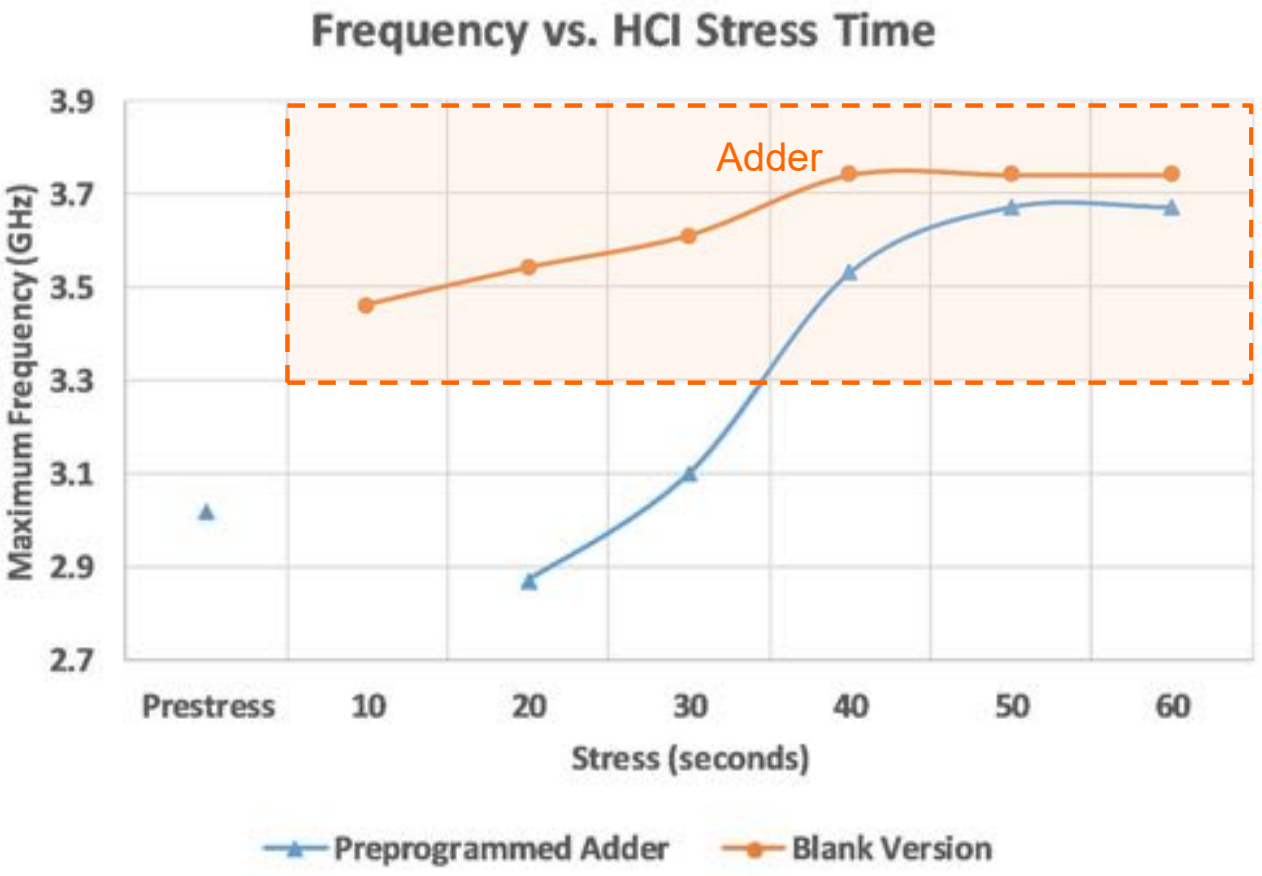
- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Stress Time vs Performance



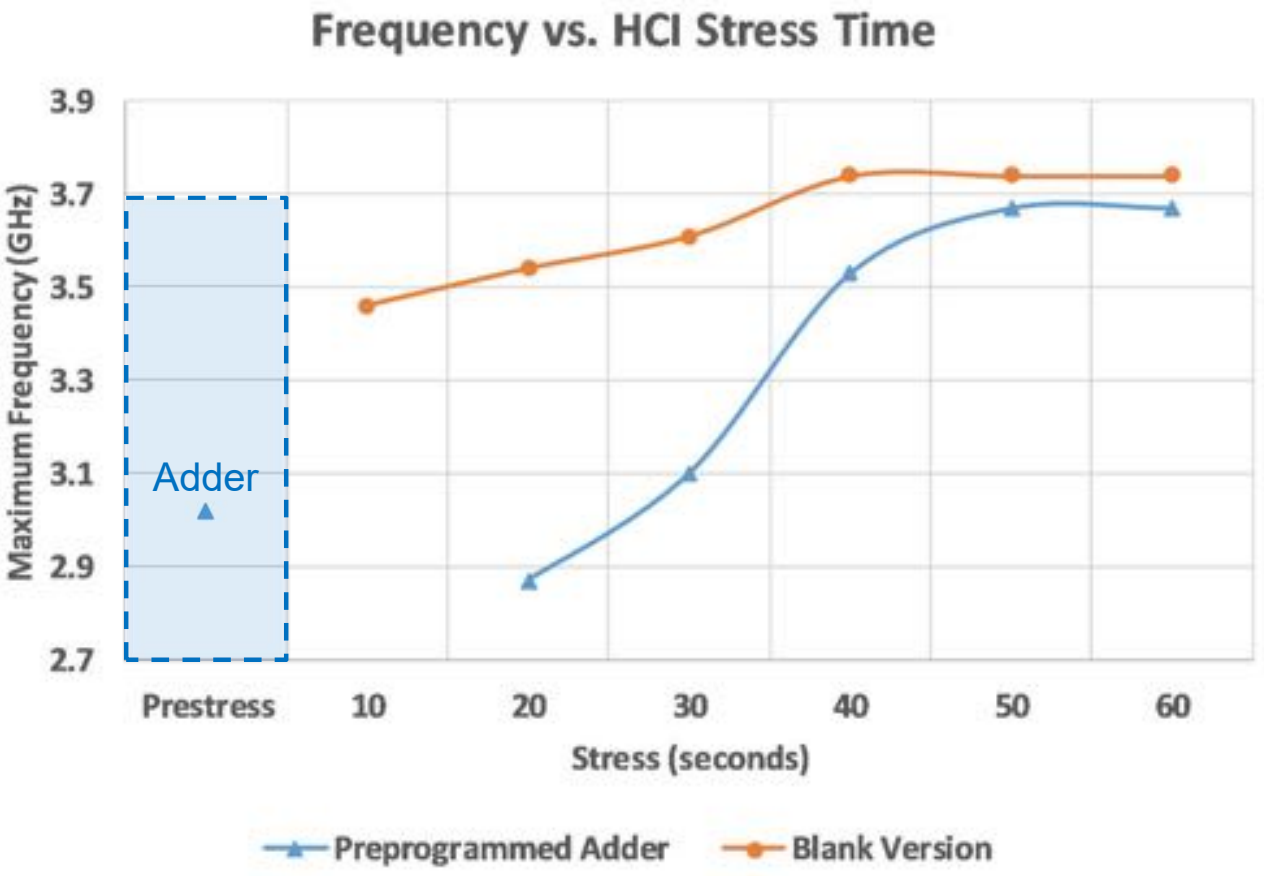
- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Stress Time vs Performance



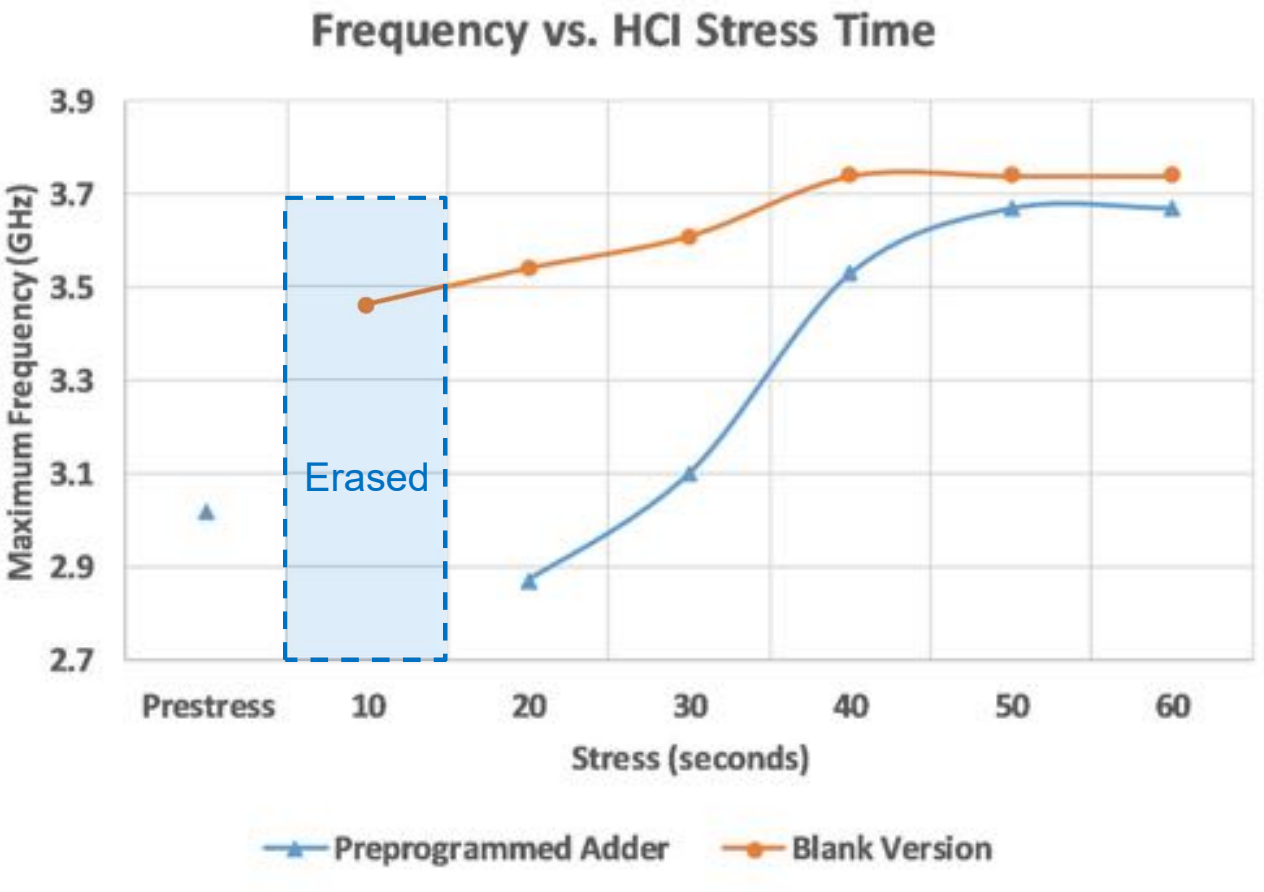
- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Stress Time vs Performance



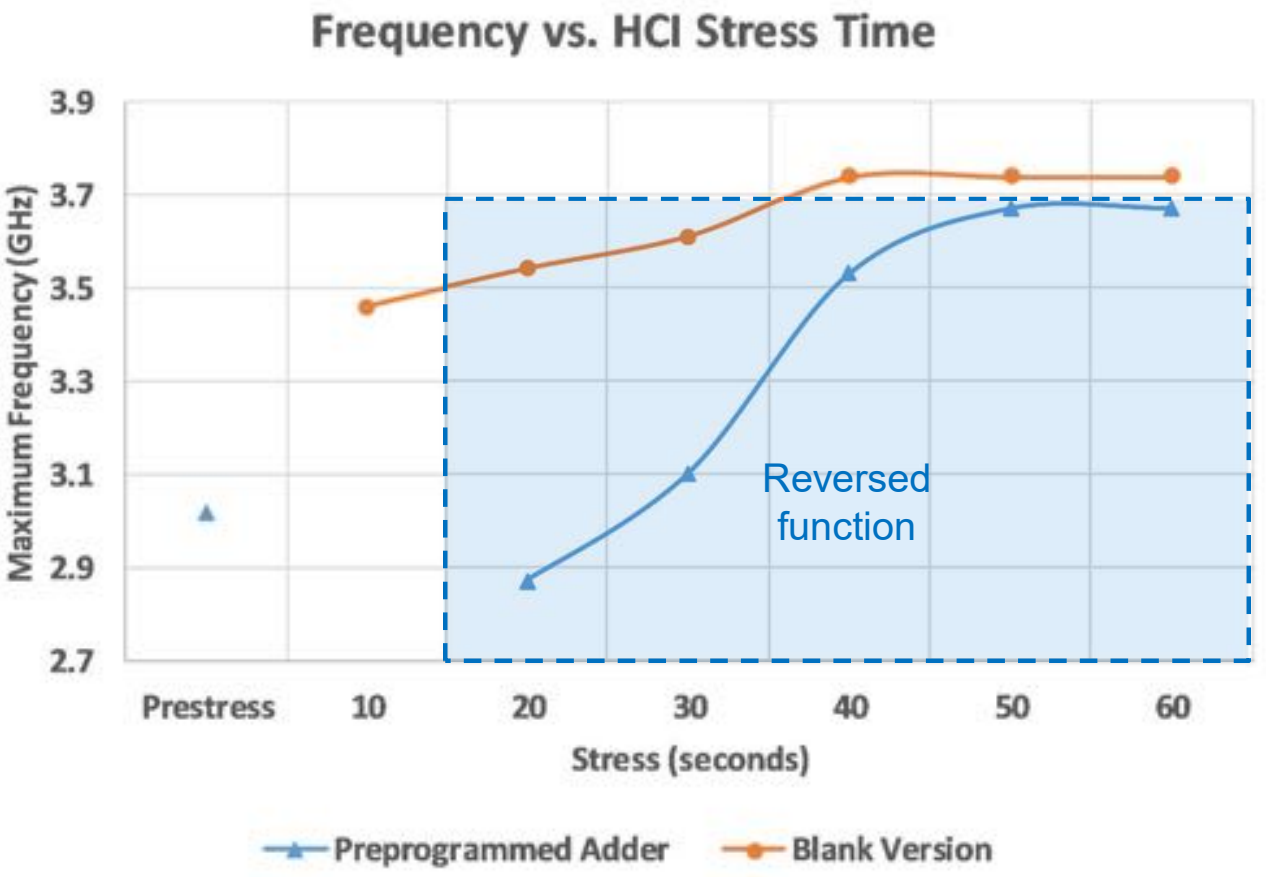
- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Stress Time vs Performance



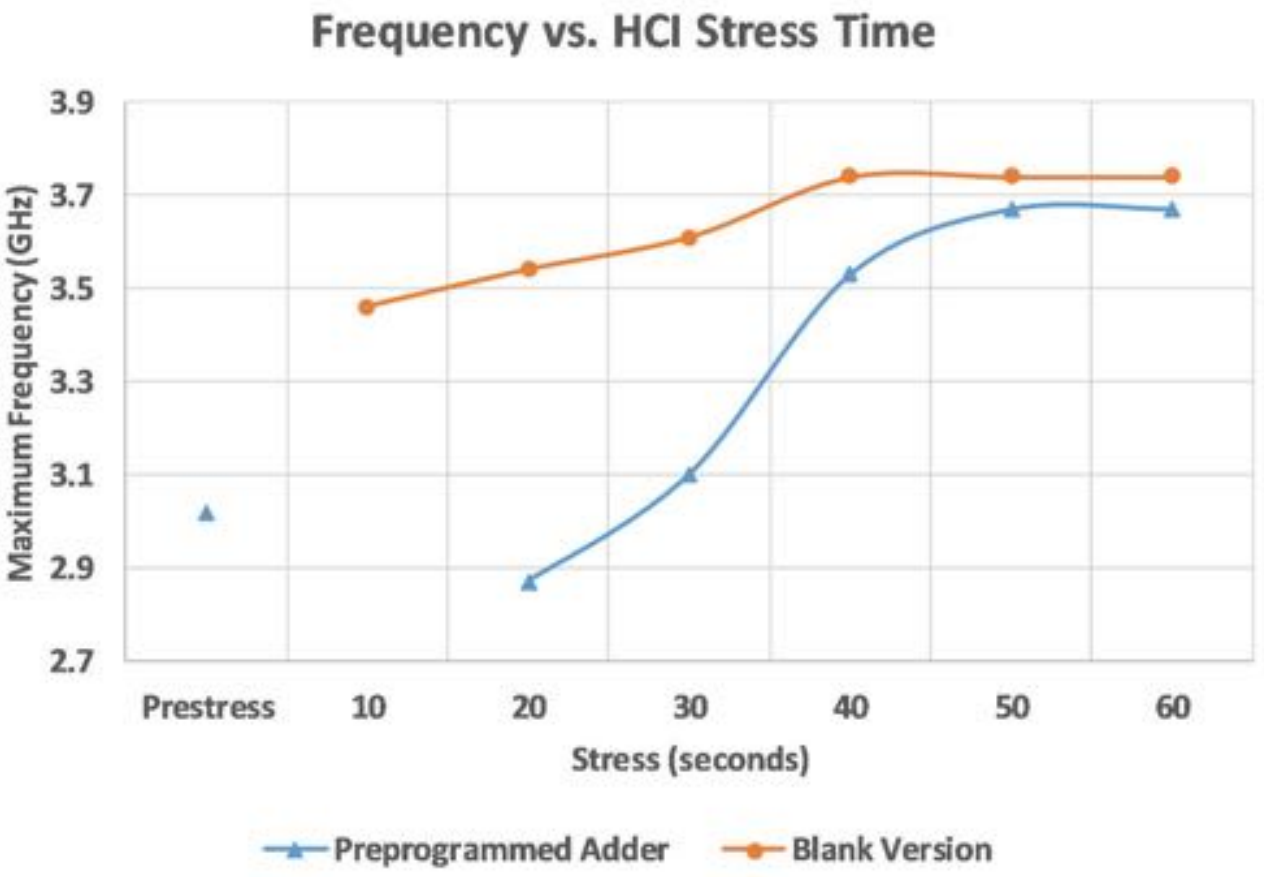
- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Stress Time vs Performance



- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Stress Time vs Performance



- **Boost** blank version
- **Reverse** preprogrammed version
- **Permanence** Baked at 125°C

Overhead and Security Comparison

Overhead vs. Static CMOS Std. Cell

	Power			Delay			Area		
	NAND	**NOR**	**XOR**	**NAND**	**NOR**	**XOR**	**NAND**	**NOR**	**XOR**
Dummy via[1]	6.5X	6.1X	1.8X	2.6X	2.1X	1X	5X	5X	2.2X
TVD[2]	1.6X	1.9X	1.1X	3.2X	2.6X	1.7X	3.7X	3.7X	1.5X
PMP-TVD (This Work)	9.2X	4X	1.8X	6.6X	5.4X	3.4X	7.3X	7.3X	3X

Security Comparison

	Dummy via[1]	TVD[2]	PMP-TVD (This Work)
Low side-channel Leakage		●	●
Untrusted Fab			●
Reverse Engineering	◐	●	●
Erasable/Programmable			●

[1] Rajendran et al., CCS'13
[2] Erbagci et al., HOST'16

Overhead and Security Comparison

Overhead vs. Static CMOS Std. Cell

	Power			Delay			Area		
	NAND	**NOR**	**XOR**	**NAND**	**NOR**	**XOR**	**NAND**	**NOR**	**XOR**
Dummy via[1]	6.5X	6.1X	1.8X	2.6X	2.1X	1X	5X	5X	2.2X
TVD[2]	1.6X	1.9X	1.1X	3.2X	2.6X	1.7X	3.7X	3.7X	1.5X
PMP-TVD (This Work)	9.2X	4X	1.8X	6.6X	5.4X	3.4X	**5.8X**	**5.8X**	**2.3X**

Security Comparison

	Dummy via[1]	TVD[2]	PMP-TVD (This Work)
Low side-channel Leakage		●	●
Untrusted Fab			●
Reverse Engineering	◐	●	●
Erasable/Programmable			●

[1] Rajendran et al., CCS'13
[2] Erbagci et al., HOST'16

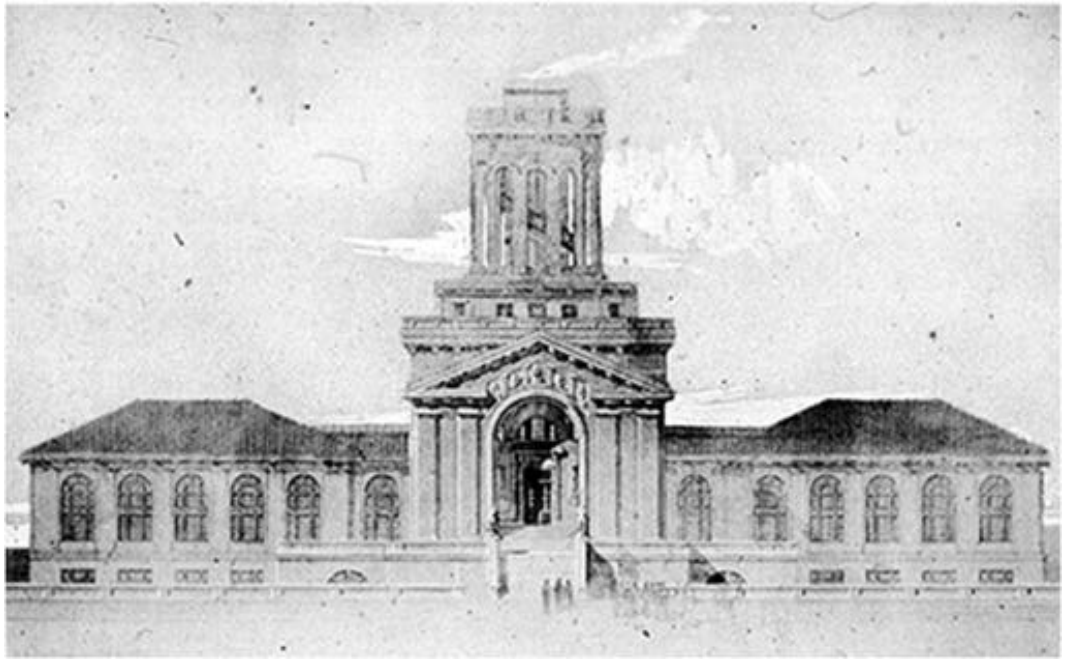
Conclusions

PMP-TVD Logic

- Security
  - Resistant to reverse engineering
  - Concealment of logic function from untrusted fab
  - Erasable / Programmable
  - Low side-channel leakage (power, timing)
- VLSI characteristics
  - Fully CMOS logic process compatible
  - Fast programming time and relatively low programming voltage
  - High programming reliability and permanence

Acknowledgements

The authors would like to thank DARPA for funding in support of this work.



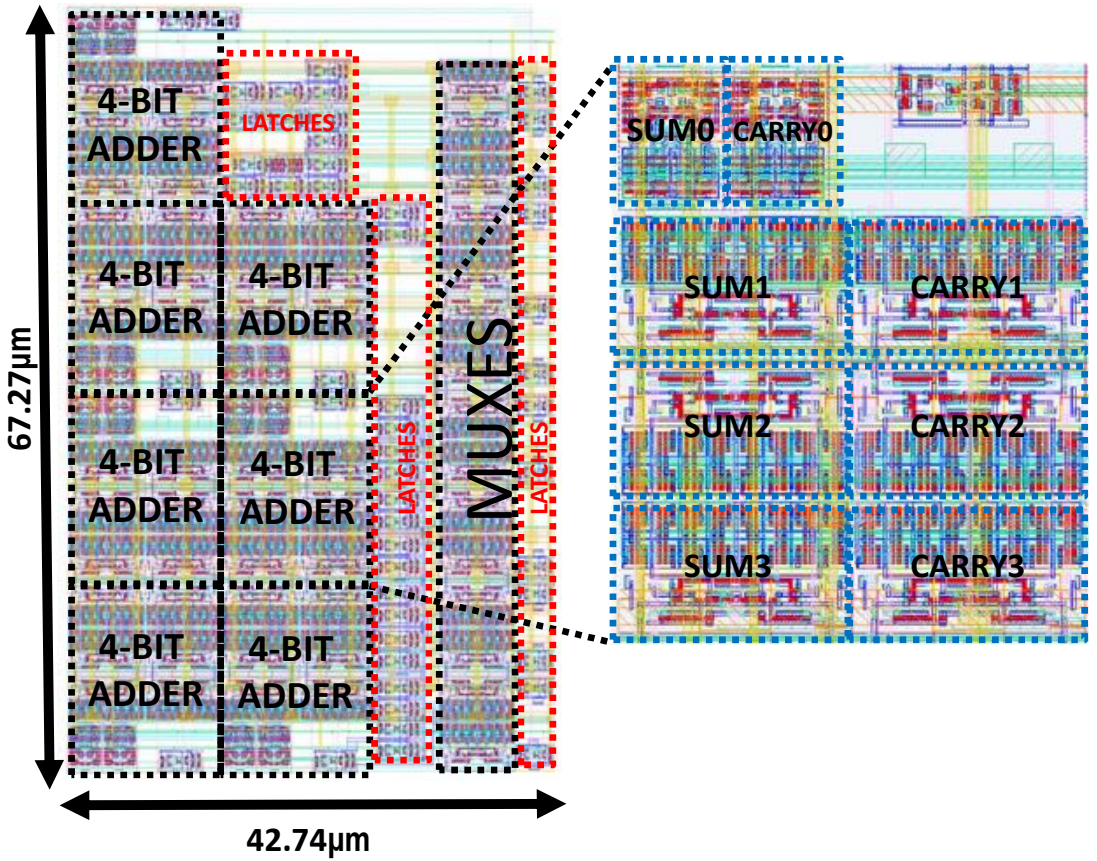
Thank you!

Results

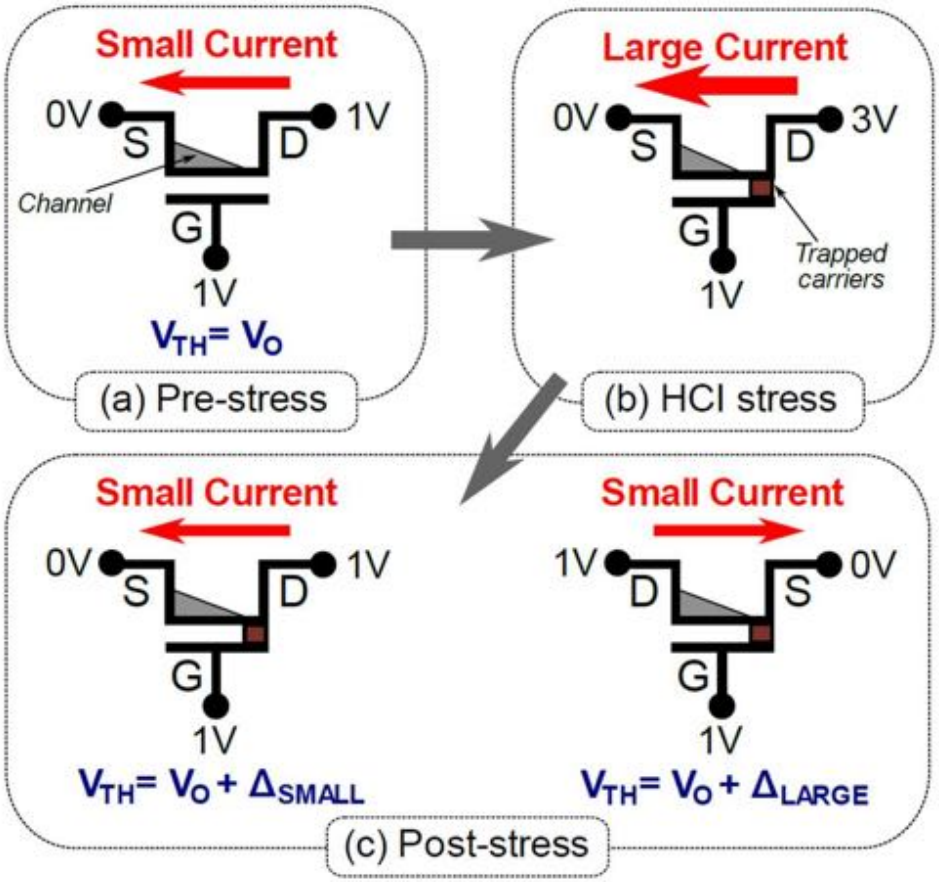
	4-bit PMP-TVD (pre-prog)	4-bit PMP-TVD (reverse)	4-bit PMP-TVD (boost)	4-bit PMP-TVD (blank)	16-bit TVD adder
Area (w/ test)	$0.007mm^2$				$0.029mm^2$
Area (core)	$0.001mm^2$				$0.003mm^2$
Freq. @ 1V	3.2GHz	2.9GHz	3.7GHz	3.6GHz	1.0GHz
Power @ 1V	1.14mW	0.96mW	1.09mW	1.09mW	3.22mW
Leakage @ 1V	0.15mW	0.14mW	0.14mW	0.14mW	0.26mW

16-bit TVD Adder

- 16-bit carry select adder
  - Pipelined
  - Two phases dynamic
  - 2- and 3- input TVD gates

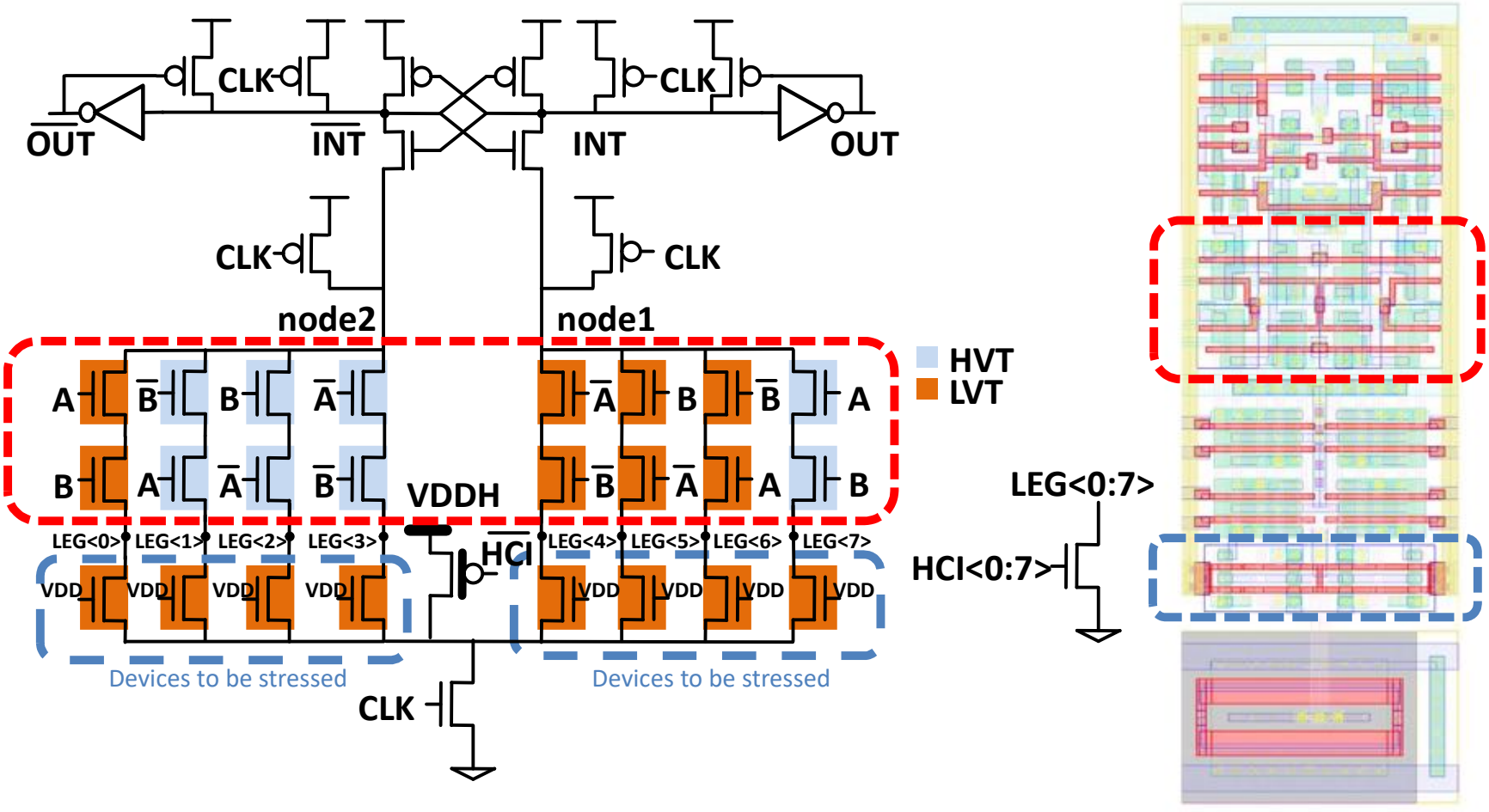


Hot-Carrier Injection (HCI)



Bhargava et al., CHES'13

Post-Manufacturing Programmed Threshold Voltage Defined Logic



An Inherently Secure FPGA using PUF Hardware-Entanglement and Side-Channel Resistant Logic in 65nm Bulk CMOS

Burak Erbagci, Nail Etkin Can Akkaya, Cagri Erbagci, Ken Mai
Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA
{berbagci,nakkaya,cerbagci,kenmai}@ece.cmu.edu

***Abstract*—We present an inherently secure FPGA that uses PUF-based hardware-entanglement of the configuration data and a side-channel resistant, self-timed logic style. The 3.14mm x 2.47mm testchip is fabricated in 9-metal 65nm bulk CMOS, contains the secure 10x10 tile FPGA fabric (six 6-input LUTs each), and runs at 290MHz at nominal 1V VDD and room temperature. The 38,400 PUF bits exhibit high uniqueness, randomness, and a BER $< 8.1*10^{-12}$.**

I. Introduction

FPGAs are attractive for secure systems due to their inherent lack of design information in the base hardware, especially in untrusted fab scenarios. To protect critical design information, FPGA manufacturers have implemented bitstream encryption, but this leads to a point of vulnerability in the bitstream decryption unit which has been successfully attacked [1]. Further, the configuration information is stored in the clear in the fabric and is vulnerable to multiple forms of probing attacks. Additionally, the user design implemented on the FPGA can be vulnerable to side-channel attacks. It can be hardened against such attacks at the HDL level, but the area, power, and delay overheads are very high. Thus, we have implemented an inherently secure FPGA that uses Physical Unclonable Function (PUF) hardware-entanglement to conceal the configuration data and uses a side-channel secure logic style to protect the FPGA operation in-the-field with low overhead. These protection mechanisms operate in a virtually user-transparent fashion and do not require alteration of the normal HDL code.

Our FPGA never stores the configuration data in the clear, even at the lowest level of the hardware (Figure 1). Each SRAM configuration bit is paired with a PUF bit. The SRAM bits store a one-time pad (OTP) encrypted version of the true configuration bitstream, with the PUF response serving as the encryption codebook [2]. At manufacture time, the PUF response for each FPGA instance is read out via a secure scan chain and then the scan chain is permanently disabled. A number of researchers have proposed designs for secure scan chains previously. The user writes the application RTL as usual, but at the time of bitstream generation, the CAD tools one-time pad encrypt the plaintext bitstream with the PUF response, thus generating a die-unique configuration bitstream.

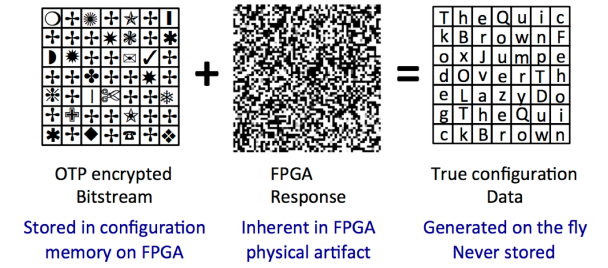


Fig. 1: Hardware-entanglement concept.

II. Hardware-Entangled Secure FPGA

A secure FPGA tile consists of three sub-blocks: Logic Cluster (LC), Connection Block (CB), and Switch Box (SB), as shown in Fig. 2. LC includes the programmable logic and a crossbar to route LC inputs to LUT inputs. CB selects and routes the corresponding channel wires to LC inputs, and SB is the programmable interconnect between the tiles. A multiplexer (MUX) is the basic building block of an FPGA tile. Each tile consists of clusters of different sized MUXes, whose sizes and numbers are dictated by the FPGA architecture parameters (Fig. 2).

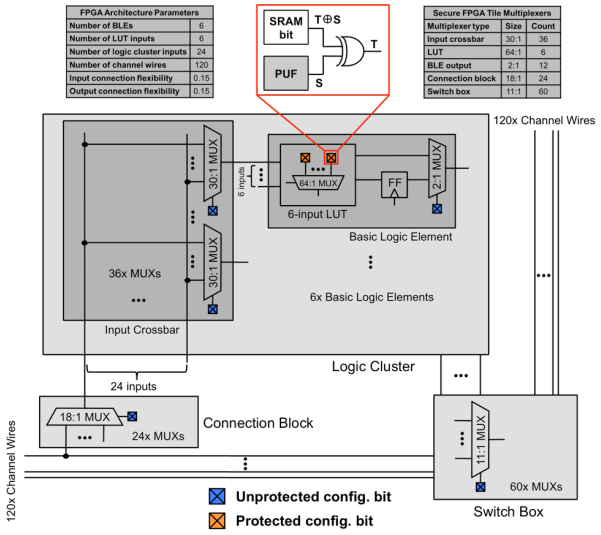
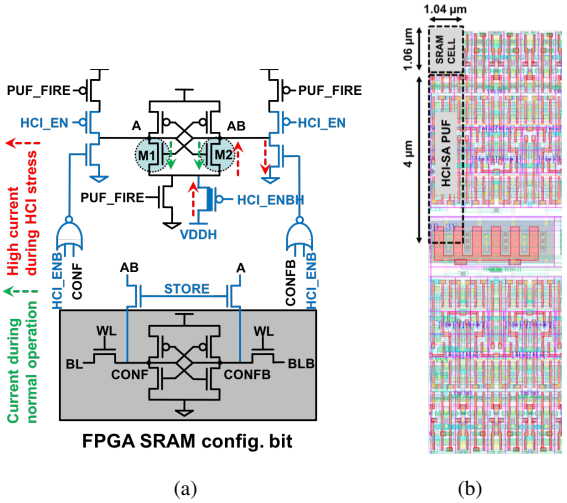


Fig. 2: Hardware-entangled secure FPGA tile.

A. Hardware-entanglement using PUFs

The core FPGA design remains the same, with only changes required in the configuration bits. This design requires a compact, fast, energy-efficient PUF capable of reliably generating a large number of response bits. We use a bi-stable PUF based around sense-amplifiers (SA) with response reinforcement via intentional directed device aging for high reliability (Fig. 3). PUF bits use hot-carrier injection (HCI) to achieve high reliability without needing inefficient ECC blocks and helper data storage [3]. For compactness, we use a latch-style SA and re-use the FPGA SRAM configuration bit to store golden response during the reinforcement phase. The HCI support circuits are shared among every two PUF bits to amortize the area overhead.



(a) (b)

Fig. 3: Compact, fast, and energy efficient PUF design that uses HCI-based response reinforcement for high reliability [3] (a) schematic (b) layout

B. Side-channel Resistant FPGA Fabric

For resistance to side-channel attacks, we use Post-Charged Dynamic Logic with Self-Timed Discharge (PCDL-STD) as seen in Fig. 4. The differential dual-rail logic style ensures low power side-channel emissions. The gate has three-phases of operation: evaluate, self-timed discharge, and post-charge.

During evaluate, the gate fires when an input pulse arrives and one of the internal output nodes is discharged. Then, during self-timed discharge, the remaining internal output node is discharged. During post-charge, both internal nodes are charged, and the gate is ready for the next evaluate cycle. The discharge phase, followed by evaluate, eliminates power side-channel emissions due to output loading imbalance, and because the discharge is self-timed, the gate is not vulnerable to clocking/control signal manipulation by an attacker.

III. Measured Results

The 3.14mm x 2.47mm testchip (Fig. 5) is fabricated on a 9-metal 65nm bulk CMOS process and contains the secure FPGA fabric, test and clocking infrastructure, and configuration control. The FPGA fabric consists of a 10x10 array

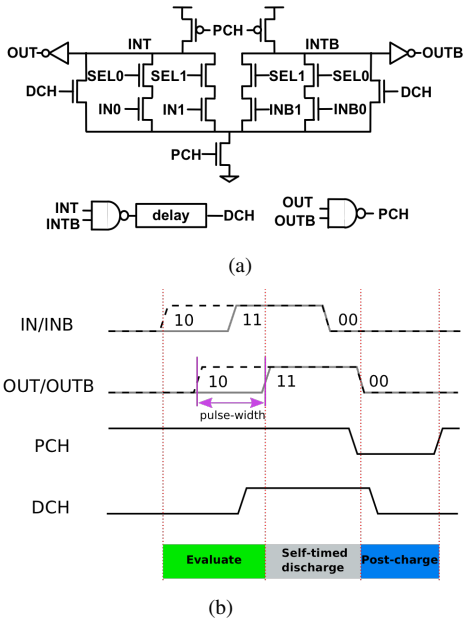


Fig. 4: A PCDL-STD 2:1 MUX (a) schematic (b) timing diagram. Sel0 =1 and Sel1=0, hence the first MUX input is selected at the output. The gate evaluates as soon as an input pulse arrives. Then, self-timed unconditional discharge phase ensures that both differential outputs switch. The gate resets after the discharge operation.

of tiles, each with a Logic Cluster (six 6-input LUTs), a Connection Block, and a Switch Box (Fig. 2). The interconnect has 120 channel wires spanning 4 LCs [2]. The testchip contains 38,400 PUF bits. The stress voltage is 3V, resulting in a current density and voltage drop in the corresponding transistor (i.e., M1 or M2) of 19.04 mA/μm^2 and 2.54V. We use a modified version of the University of Toronto's VTR tool chain [4] to generate the configuration bitstream from Verilog HDL.

PUF hardware-entanglement can be fired one-time at power-up to improve performance or activated on-the-fly for better security. Similarly, the wire discharge phase can be disabled for lower power (Table I). Based on architectural FPGA simulations and security evaluation, we only hardware-entangle the logic LUT configuration bits in the testchip, trading off security against VLSI overheads. But there is no fundamental barrier to hardware-entangling all the configuration bits.

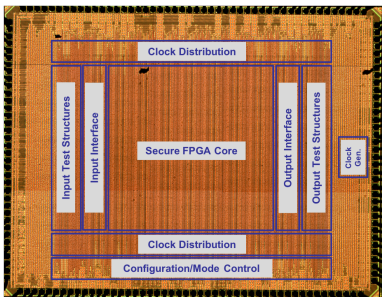


Fig. 5: Die microphotograph of 3.14 mm x 2.47 mm secure FPGA testchip in 65nm bulk CMOS. The chip has 170 I/O pads and consists of 10 x 10 (600 LUTs) secure FPGA tiles. There are a total of 38,400 PUF instances.

A. Benchmark Results

We use an AES S-Box security primitive (Fig. 7(b)) to benchmark the characteristics of the FPGA fabric. At nominal 1V VDD, with all security features enabled (i.e., PUFs fired on-the-fly, discharge enabled) the S-Box operates at 290 MHz and consumes 1.7 nJ/cycle. Switching to PUFs fired one-time, the frequency increases to 350MHz, since the PUF delay is removed from the logic evaluation forward path. At maximum, the FPGA operates at up to 490MHz at 1.3V and one-time PUF firing. The performance is commensurate with commercial FPGAs in the same technology. Disabling the discharge phase (WES=on) reduces the interconnect energy by 40%, but this only translates to an approximately 10% total energy savings due to the LUT and PUF energy overheads. Different modes of operations are summarized in Fig. 7.

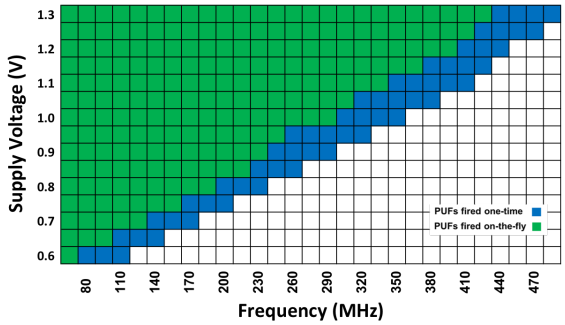
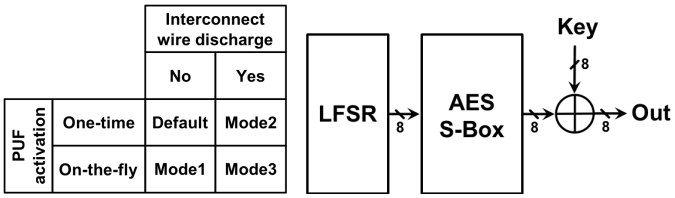


Fig. 6: Shmoo plot of secure FPGA. Green and blue areas represent the voltage-frequency points in which the chip is functional. In a temperature-stabilized environment of 27°C, the chip operates at 80-500 MHz across a supply range of 0.6-1.3V, respectively.

TABLE I: Secure FPGA silicon results

Mode	Default	Mode1	Mode2	Mode3
Area (mm^2, w/ test)	5.1			
Area (mm^2, core)	3.45			
Freq. @1V (MHz)	350	290	350	290
Energy @1V (nJ/cycle)	1.5	1.55	1.65	1.7
Power @1V (mW)	522	447	574	473
Leakage @1V (mW)	70			



(a) (b)

Fig. 7: (a) Secure FPGA operating modes (b) AES S-box benchmark circuit implemented on secure FPGA.

Table II shows the VLSI overhead comparisons of our secure FPGA against an HDL-level countermeasure against power side-channel attacks (D-WDDL [5]) using an unsecure static FPGA with the same design parameters. Results are normalized to a baseline unsecure static FPGA using unsecure HDL. Post-layout extracted simulation results are used in VTR flow to evaluate the VLSI overheads against D-WDDL.

TABLE II: VLSI overheads of secure FPGA against D-WDDL [5]

	Secure FPGA (This work)				D-WDDL [5]
	Default	Mode1	Mode2	Mode3	
Area	2x				4x
Delay	0.75x	0.9x	0.75x	0.9x	2x
Energy	3.2x	4x	4.2x	5x	7.7x

B. PUF Results

PUFs are evaluated on their uniqueness, randomness, and reliability. For uniqueness, Fig. 8 shows the pairwise Hamming distance of responses across 3 chips which is close to ideal with mean values around 8. With regards to randomness, the PUF response bits pass the NIST randomness tests with min. P value of 0.976.

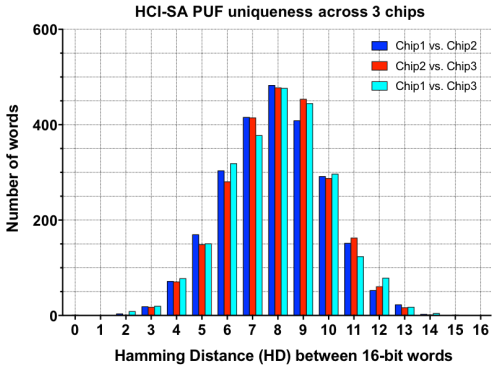


Fig. 8: Histogram of Hamming distance of 16-bit HCI-SA PUF response words from 3 chips. The pairwise HD of response bits from 3 chips is close to ideal (i.e., mean of 8) with means of 7.94, 8.02, and 7.96.

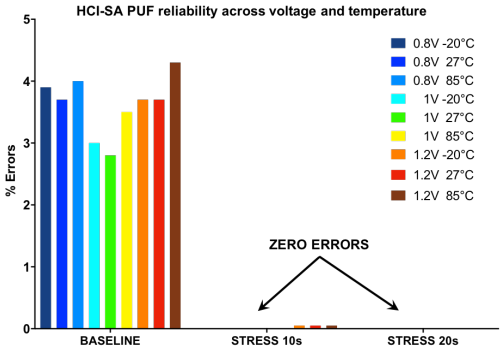


Fig. 9: Reliability of HCI-based PUFs shown as a percentage of errors across 100 evaluations at each voltage (0.8V, 1V, 1.2V) and temperature (-20°C, 27°C, 85°C) corner.

Our PUF reliability is evaluated in both small and large scale experimental tests. Fig. 9 shows the percentage of errors across 100 evaluations at each voltage (0.8V, 1V, 1.2V) and temperature (-20°C, 27°C, 85°C) corner. After 20s HCI stress time, there are no errors for any of the 38,400 PUF instances across all 100 evaluations for each voltage-temperature combination. We conduct the large-scale experiment at the worst-case corner (1.2V, 85°C). After 3,192,000 measurements at the

worst-case corner (133 days of continuous testing), no errors were observed. A conservative assumption that the very next measurement would be an error leads to a bit-error-rate (BER) $< 8.1*10^{-12}$, which is on par with the theoretical BER targeted by the ECC in the commercial PUFs and close to the reported BER of SRAMs at this technology node. High temperature and voltage experiments in [3], [6] have shown good HCI permanence across aging.

C. Security Analysis

We perform a DPA attack on the testchip on a custom test board with all de-coupling capacitors de-soldered and a 2Ω resistor in series with the core power supply for current measurement. We mount the DPA attack using the first 200 sample points in every clock cycle. As shown in Fig. 10, the extracted key values have very small correlations with the measured power variations and are random with no single outstanding value that dominates the other key guesses (Table III). Correlation analysis results for Mode1 (PUFs fired on-the-fly and no interconnect discharge) are shown in Table IV.

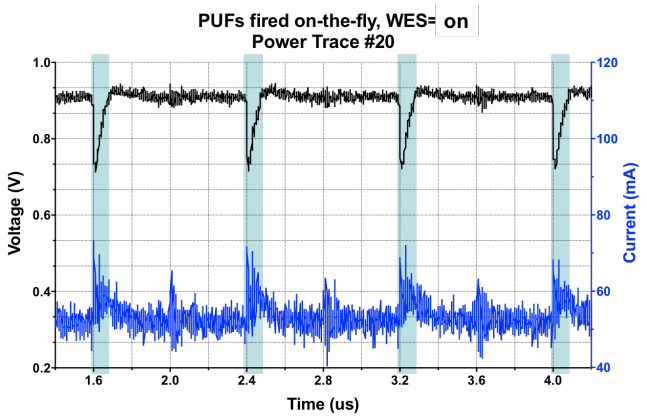


Fig. 10: Measured power trace for Mode1, where PUFs are fired on-the-fly and the interconnect discharge is turned off. The current (highlighted in blue) that is drawn by the secure fabric is measured through a 2Ω resistor in series with the supply power. 4 cycles in a 255-cycle period (i.e., all LFSR inputs) for the 20th power trace measurement are shown. The DUA evaluation windows are highlighted in light green.

TABLE III: Extracted key values for input bits for different modes

Mode	Bit[0]	Bit[1]	Bit[2]	Bit[3]	Bit[4]	Bit[5]	Bit[6]	Bit[7]
Default	110	3	2	121	41	4	101	95
Mode1	194	6	251	237	11	191	144	8
Mode2	12	196	2	181	215	170	221	94
Mode3	235	140	19	1	29	144	253	159

TABLE IV: Correlation analysis for Mode1 (PUFs fired on-the-fly, no interconnect discharge)

Correct key=174	Bit[0]	Bit[1]	Bit[2]	Bit[3]	Bit[4]	Bit[5]	Bit[6]	Bit[7]
Max. correlation	5.3e-2	6.1e-2	6.5e-2	6.2e-2	5.2e-2	6e-2	6.9e-2	7e-2
Min. correlation	3e-4	6e-5	2.4e-4	1.1e-4	7e-5	3e-5	1e-4	9e-5
Avg. correlation	1.6e-2	1.6e-2	1.5e-2	1.5e-2	1.6e-2	1.8e-2	1.6e-2	1.7e-2
Extracted key	194	6	251	237	11	191	144	8
Corr. of correct key	3.4e-2	1e-2	9e-4	5e-3	8e-3	2.2e-2	9e-3	3.4e-2
Rank of correct key	23	156	244	188	169	88	165	27

Table V summarizes the security evaluation of the secure FPGA compared to various countermeasures by FPGA vendors. Due to large number of PUF bits in secure FPGA, it is resistant to side-channel attacks (as there is no single point of attack) and direct probing attacks (as there are thousands of bits that would need to be non-destructively probed). Hardware-entanglement makes each configuration bitstream unique for each FPGA die. Thus, the compromise of one configuration bits does not pose a cloning or tampering threat to other configured FPGAs.

TABLE V: Security comparison summary of various countermeasures

Countermeasures	Attacks				Unique conf. per die
	Read-back	Rev. eng. /cloning	Side-channel	Direct probing	
Bitstream enc. [7]	✗	✓	✗	✗	✗
Bitstream auth. [8]	✗	✓	✗	✗	✗
Active defense [8]	✓	✓	✗	✗	✗
Flash FPGAs [7] [9]	✗	✓	✗	✓	✗
Secure FPGA	✓	✓	✓	✓	✓

IV. Conclusions

A secure FPGA concept is implemented in 65nm bulk CMOS. The bitstream is protected by hardware-entangling the configuration deep within the hardware with a secret, die-specific PUF response. Hence, the configuration data is stored encrypted at each level of hardware including the configuration storage on the FPGA. We also address the most common side-channel analysis (SCA) vulnerability, power-SCA, through use of a novel power-SCA resistant logic embedded within the fabric. Our prototype is the first-ever-reported FPGA that is designed specifically for secure operation. The secure FPGA performance is commensurate with commercial FPGAs in the same technology. We show that there are significant security benefits with secure FPGA and the corresponding overheads are much lower compared to existing countermeasures.

References

[1] S. Skorobogatov and W. C., "In the blink of an eye: There goes your AES key." *IACR Cryptology Archive*, 2012.

[2] B. Erbagci, M. Bhargava, R. Dondero, and K. Mai, "Deeply Hardware-entangled Reconfigurable Logic and Interconnect," in *International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Dec 2015, pp. 1–8.

[3] M. Bhargava and K. Mai, "A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement," in *Cryptographic Hardware and Embedded Systems (CHES)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 90–106.

[4] J. Luu *et al.*, "VTR 7.0: Next Generation Architecture and CAD System for FPGAs," *ACM Trans. Reconfigurable Technology and Systems (TRETS)*, vol. 7, no. 2, pp. 6:1–6:30, Jul. 2014. [Online]. Available: http://doi.acm.org/10.1145/2617593

[5] P. Yu and P. Schaumont, "Secure FPGA circuits using ontrolled placement and routing," in *IEEE/ACM/IFIP International Conference on Hardware/-Software Codesign and System Synthesis (CODES+ISSS)*, Sept 2007, pp. 45–50.

[6] N. E. C. Akkaya, B. Erbagci, and K. Mai, "A secure camouflaged logic family using post-manufacturing programming with a 3.6GHz adder prototype in 65nm CMOS at 1V nominal VDD," in *IEEE International Solid - State Circuits Conference - (ISSCC)*, Feb 2018, pp. 128–130.

[7] B. Badrignans, J. L. Danger, V. Fischer, G. Gogniat, and L. Torres, Eds., *Security Trends for FPGAS*. Springer, 2011.

[8] M. Smerdon, "Security Solutions Using Spartan-3 Generation FPGAs," 2008. [Online]. Available: https://www.xilinx.com/support/documentation/white_papers/wp266.pdf

[9] T. Huffmire, C. Irvine, T. D. Nguyen, T. Levin, R. Kastner, and T. Sherwood, Eds., *Handbook of FPGA Design Security*. Springer, 2010.

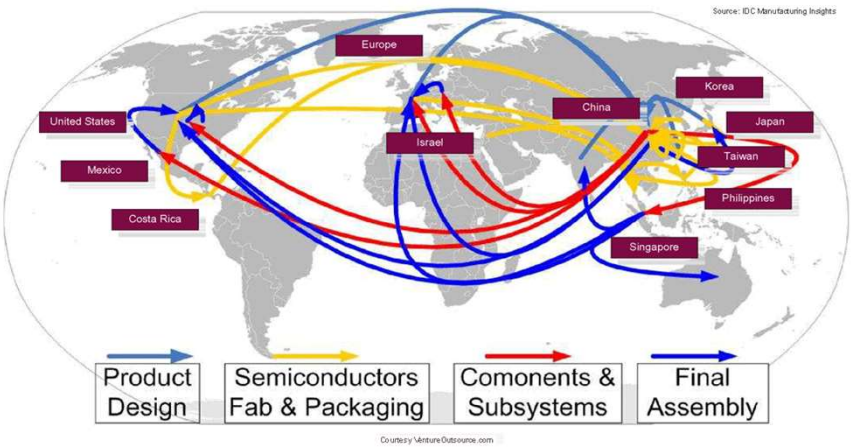
Carnegie Mellon University

Hardware Obfuscation via Designer-Directed Fine-Grained eFPGA Redaction

MAY 15, 2020

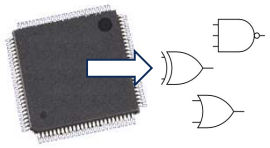
Ken Mai

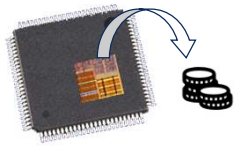
Electronic System Supply Chain



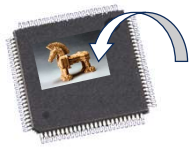
Supply Chain Threats

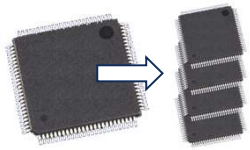
- Reverse engineering
  - Netlist extraction
  - IP piracy



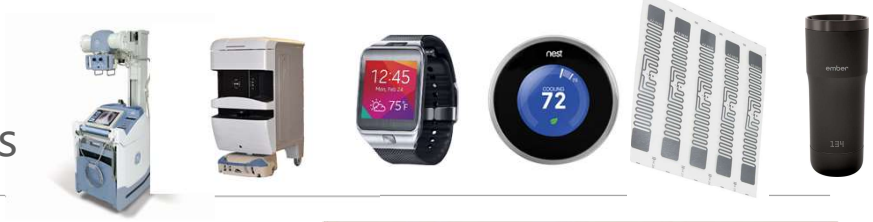


- Untrusted fabrication
  - Hardware trojans
  - Overproduction
  - IP piracy

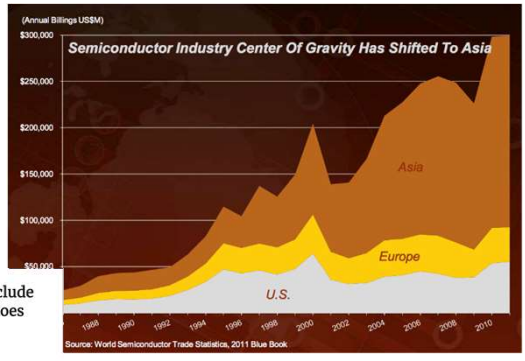




Drivers



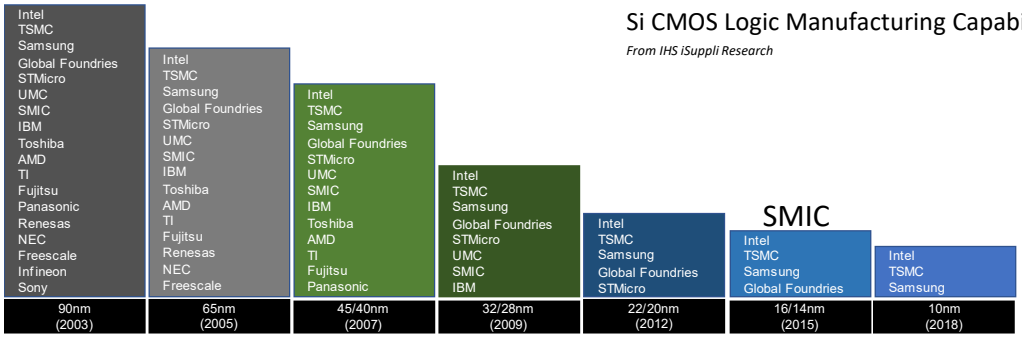
- Low cost
- High volume
- High-mix
- In-the-field fixes
- High-efficiency
- Security



Q: We manufacture integrated circuits (ICs) that are unique for defense articles and include programmable elements. Are these ICs described by USML Category XI(c)(1)? How does Note 3 to USML Category XI(c)(1) apply when the programmable elements are un-programmed?

A: An IC that is unique to a defense article is described in USML Category XI(c)(1). An IC that contains both programmable elements and non-programmable elements may only be treated as a Programmable Logic Device (PLD) when all of the non-programmable elements are common to an IC used in an item that is not a defense article. When these conditions are met, Note 3 to USML Category XI(c)(1) applies, and the IC is not controlled by USML Category XI(c)(1) so long as all of the programmable elements are un-programmed.

State of the Microelectronics Industry – Fabs



- Only 3 suppliers are committed to advancing to 10nm node and beyond
- Intel only US-owned/operated supplier committed to remaining at SOTA

New News …

TECH

Apple supplier TSMC to build a $12 billion chip factory in the U.S.

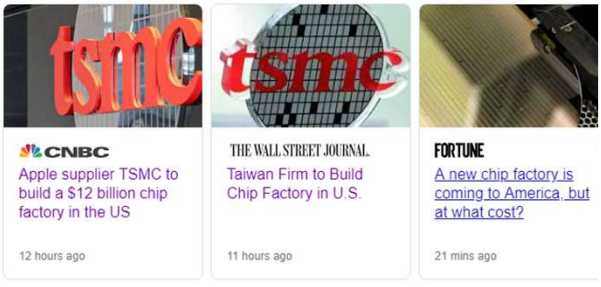
PUBLISHED THU, MAY 14 2020•10:21 PM EDT | UPDATED MOMENTS AGO

Arjun Kharpal

SHARE

KEY POINTS

- Taiwan Semiconductor Manufacturing Co (TMSC) said on Friday it will build a semiconductor facility in Arizona.
- Total spending on the project will be $12 billion with TSMC claiming it will directly create 1,600 jobs.
- TSMC's decision to build a new U.S. chip plant comes as President Donald Trump's administration continues to scrutinize the global technology supply chain upon which American firms rely on.



CNBC
Apple supplier TSMC to build a $12 billion chip factory in the US
12 hours ago

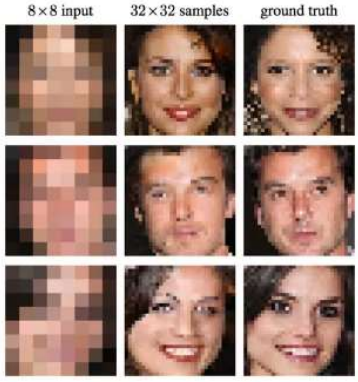
THE WALL STREET JOURNAL.
Taiwan Firm to Build Chip Factory in U.S.
11 hours ago

FORTUNE
A new chip factory is coming to America, but at what cost?
21 mins ago

Locking vs Obfuscation

Carnegie Mellon University

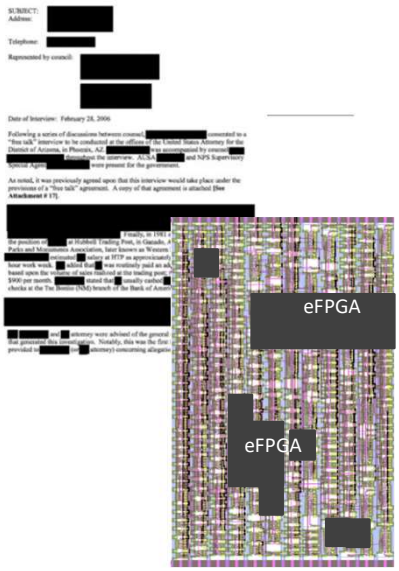
Obfuscation vs Redaction



Carnegie Mellon University

Redacted Hardware

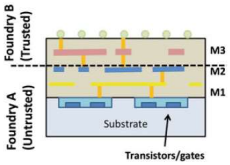
- Fine grained removal of sensitive information content
  - Countermeasure vs untrusted fab and reverse engineering
  - Can obfuscate any granularity from single gate to entire functional block
- Tight, fine-grained integration of eFPGA
  - Merged with regular standard cell PnR, not standalone eFPGA block
  - Allows for higher performance at power (PaP) than standalone eFPGA block
- Extreme logic locking …



Carnegie Mellon University

Countermeasures

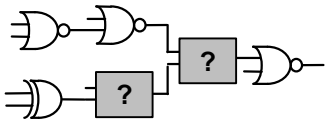
Split fabrication



Reverse engineering

Untrusted fabrication

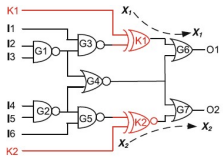
Gate camouflaging



Reverse engineering

Untrusted fabrication

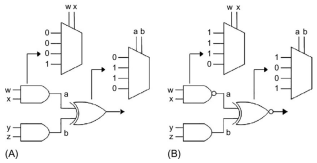
Logic locking



Reverse engineering

Untrusted fabrication

Reconfigurable logic

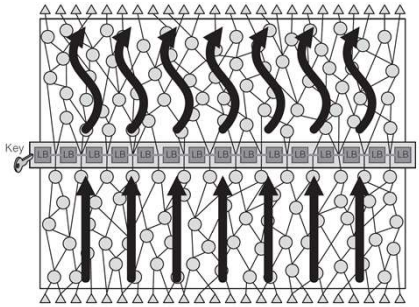


Reverse engineering

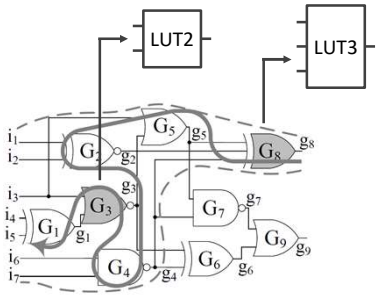
Untrusted fabrication

Carnegie Mellon University

Reconfigurability in Obfuscation

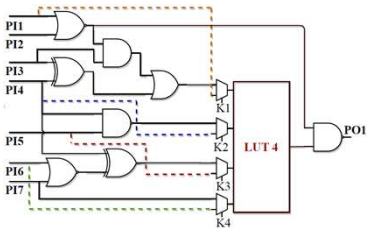


Reconfigurable barriers
(Baumgarten et al. 2010)

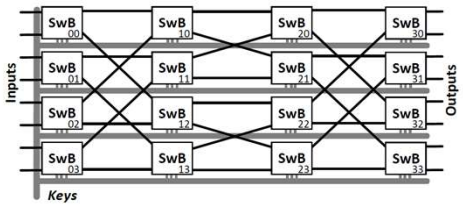


LUT-lock
(Kamali et al. 2018)

Reconfigurability in Obfuscation



Custom LUT based obfuscation
(Kolhe et al. 2018)

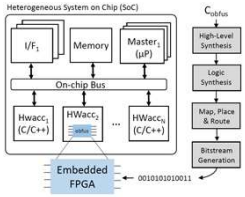


Full-lock
(Kamali et al. 2019)

FPGAs and Obfuscation

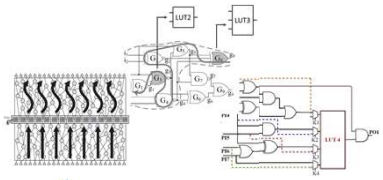
- Why not just use an FPGA?
  - Fully reconfigurable architecture (+)
  - Toolchain and IP support (+)
  - Targets the system instead of the critical IP (-)
  - High delay and area overheads (-)
- Embedded FPGAs are a potential solution.
  - Comparable level of security for critical IP (+)
  - More fine-grained (High-level blocks) (+)
  - Can't map gate-level structures (-)

A commercial FPGA chip

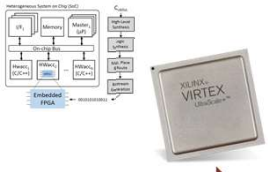


Hardware accelerator obfuscation (Hu et al. 2019)

Design Space

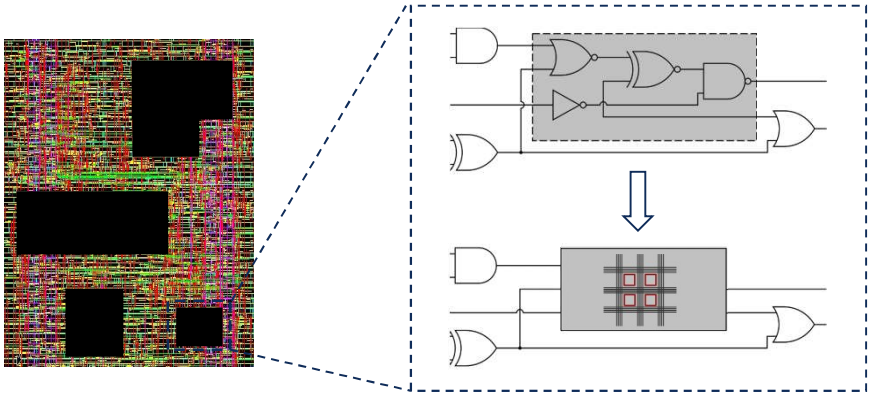


?



- Fine-grained integration
- Minimal delay, area overhead
- Fully concealed design intent
- Extensive toolchain support

eFPGA Redaction: Concept

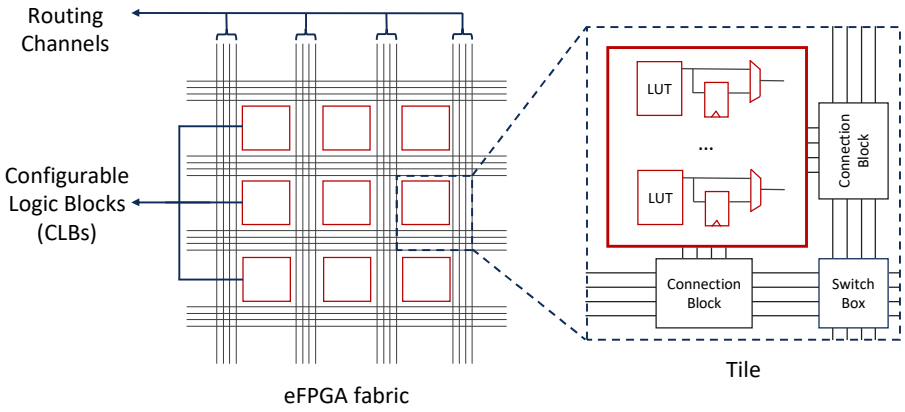


eFPGA Redaction: Flow

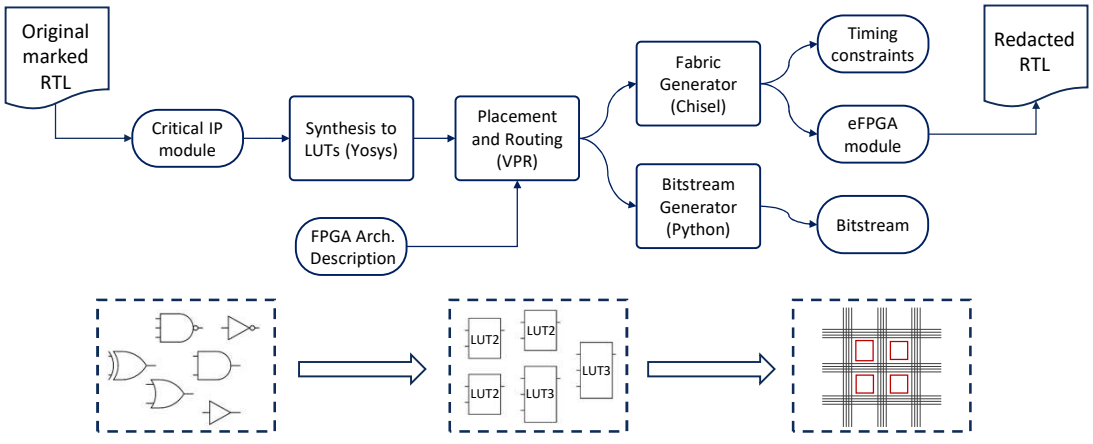
Original marked RTL | Redacted RTL | Layout

- Soft IP -> fully standard cell based design
  - Low floorplanning effort and seamless integration to the surrounding blocks
  - High flexibility in terms of size and architecture
  - No characterization necessary

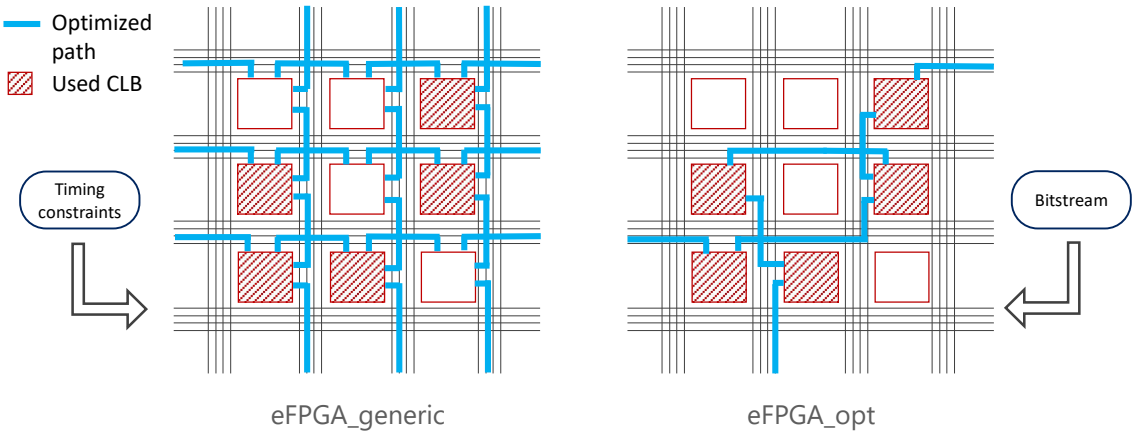
eFPGA Redaction: Soft eFPGA Fabric



eFPGA Redaction: Fabric Generation Flow

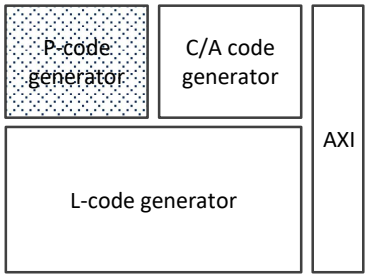


eFPGA Redaction: ASIC Timing Optimization



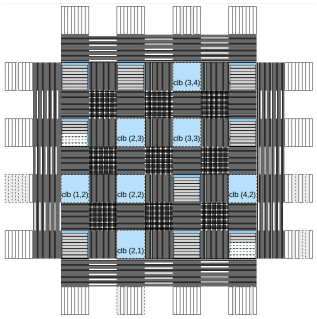
Test Circuit 1: GPS P-Code Generator

- MIT Lincoln Lab Common Evaluation Platform
- Generates C/A code, P-code and L-code
- P-code generator is obfuscated
  - Length of the code
  - Position of the LFSR taps
  - Initialization value of the LFSR



GPS core module diagram

GPS eFPGA Parameters

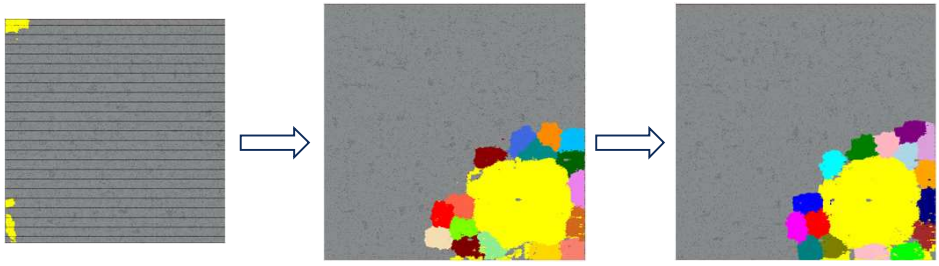


VPR implementation of the critical IP

Parameter	Value
Number of tiles	16 (4x4)
Channel width	44
Number of LUTs per CLB	8
LUT size	4
Crossbar connectivity	50%
Wire length	4
Switch block connectivity	3
Switch block type	Wilton
Input connectivity (Fc_{in})	0.2
Output connectivity (Fc_{out})	0.1

Architectural parameters

GPS Layout

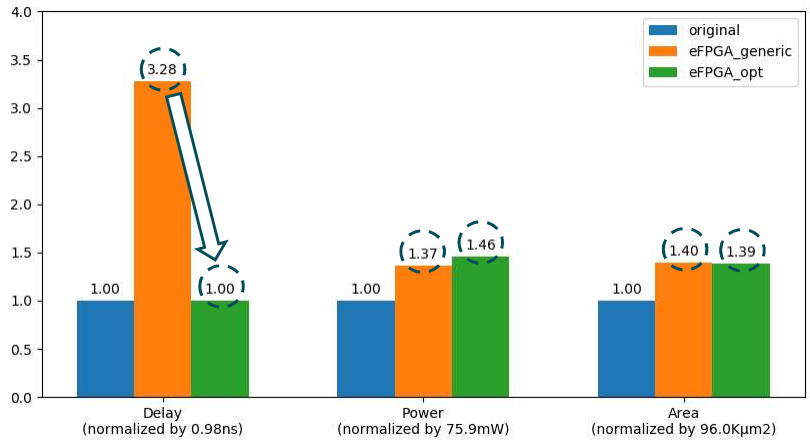


Original core ($0.096mm^2$)

eFPGA_generic ($0.134mm^2$)

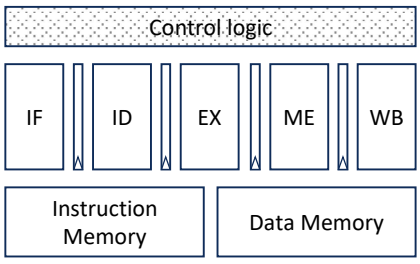
eFPGA_opt ($0.133mm^2$)

GPS VLSI Metrics



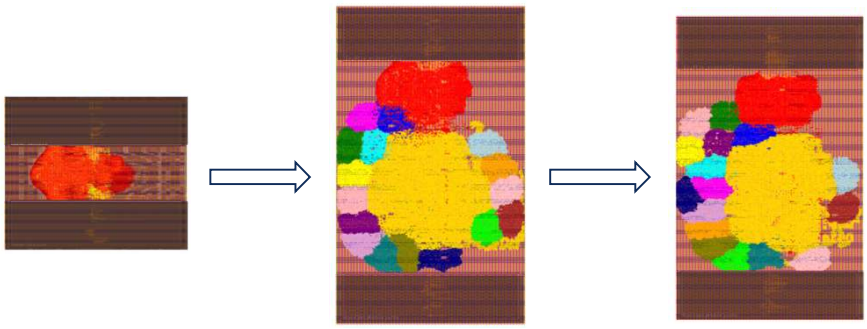
Test Circuit 2: RISC-V CPU

- RV32I architecture
- 5-stage pipelined
- 16 KB separate instruction and data memory
- Control logic obfuscated
  - Low percentage of the gates, and renders the entire CPU unusable



RISC-V CPU module diagram

RISC-V Layout

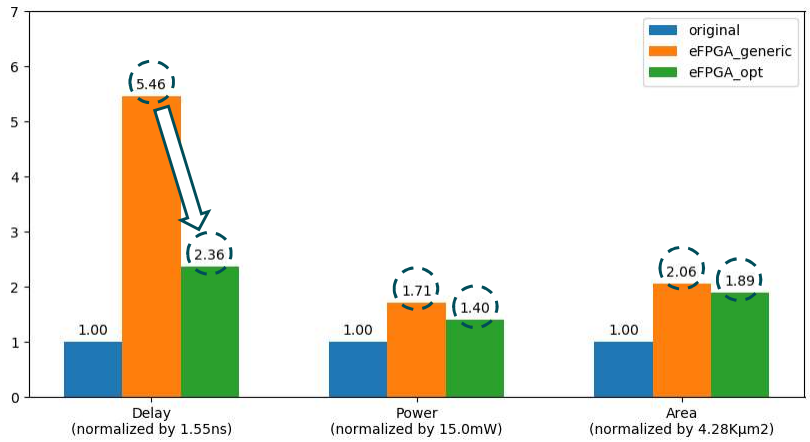


Original core
(4.28K μm²)

eFPGA_generic
(8.80K μm²)

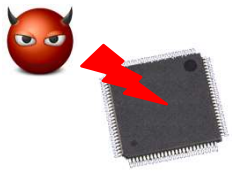
eFPGA_opt
(8.08 μm²)

RISC-V VLSI Metrics



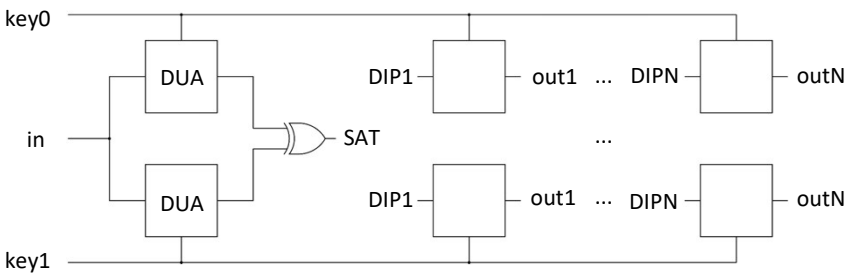
Security Analysis

- Attacker model:
  - Possesses full-chip netlist and layout
  - Has access to an unlocked design oracle
  - Can toggle eFPGA I/O through a scan chain



- Possible attacks:
  - Removal attack -> Not possible since LUTs implement the logic functionality
  - Direct probing -> Challenging due to sheer number of bits required to probe
  - SAT attack -> Mounted on redacted netlists

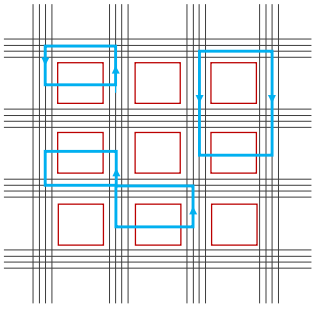
SAT Attack Setup



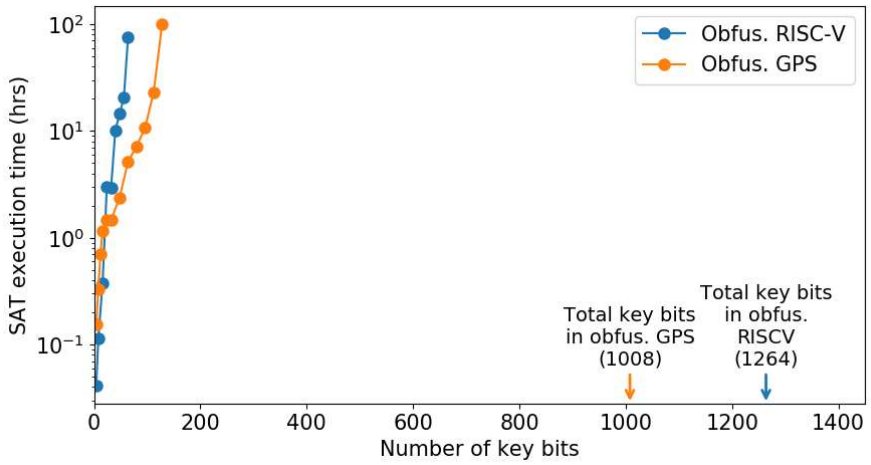
1. Find an input where SAT == 1
2. Save the distinguishing input and the golden output. Add a pair of constraint blocks
3. Repeat 1,2 until SAT can't be 1. Then, key0 = key1 = gold key

SAT Attack Results

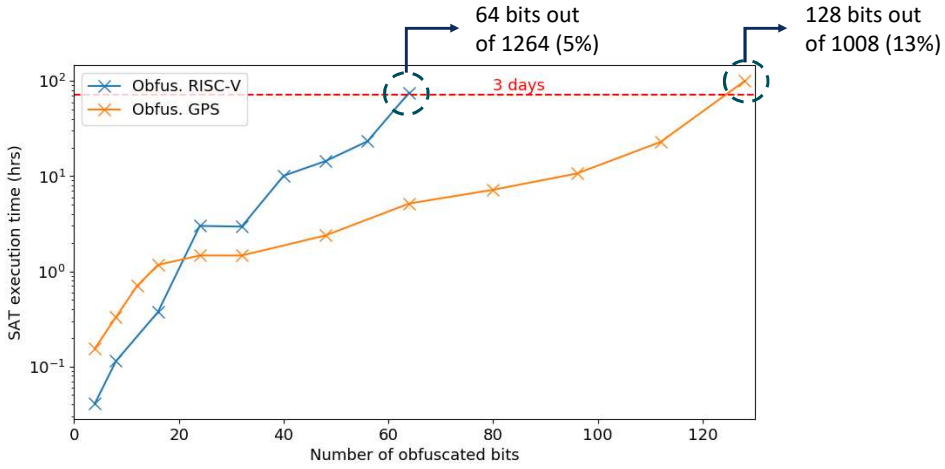
- SAT runs infinitely due to combinational loops
  - Assume that the attacker knows the routing keys
- Runtime is too long due to the large key space.
  - Assume that the attacker knows every configuration bit
  - Randomly select a utilized LUT
  - Make all its configuration bits unavailable to the attacker
  - Run SAT attack on the reduced key space
  - Make more LUTs unavailable until runtime > 3 days



SAT Attack Results



SAT Attack Results



Conclusion

- eFPGA redaction can provide routing and logic obfuscation in a fine-grained way.
- RISC-V & GPS achieved SAT-hardness with 5% and 13% of the key bits respectively.
- Bitstream-specific timing optimization techniques can be employed to reduce overhead greatly at the expense of routing information leakage.
- Further improvements can be made by exploring more diverse FPGA architectures and the ability to selectively hardwire key bits to reduce overhead.