IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 01-06

Obfuscating Dsp Circits via High Level Transformations

Angel Priya[1], S.Lakshmi[2]
1P.G Student, Dept Of ECE, Thirumalai Engineering Collage ,Kanchipuram
2Assistant Professor, Dept Of ECE, Thirumalai Engineering Collage ,Kanchipuram .

Abstract: *To Design Obfuscated Circuits For Digital Signal Processing (DSP) Applications Using High-Level Transformations, A Key-Based Obfuscating Finite-State Machine (FSM), And A Reconfigurator. The Goal Is To Design DSP Circuits That Are Harder To Reverse Engineer. High-Level Transformations Of Iterative Data-Flow Graphs Have Been Exploited For Area-Speed-Power Tradeoffs. This Is The First Attempt To Develop A Design Flow To Apply High-Level Transformations That Not Only Meet These Tradeoffs, But Also Simultaneously Obfuscate The Architectures Both Structurally And Functionally. Several Modes Of Operations Are Introduced For Obfuscation Where The Outputs Are Meaningful From A Signal Processing Point Of View, But Are Functionally Incorrect. The Latter Two Modes Are Meaningful, But Represent Functionally Incorrect Modes. Multiple Meaningful Modes Can Be Exploited To Reconfigure The Filter Order For Different Applications. A Correct Key Input To An FSM Activates A Reconfigurator. The Configure Data Controls Various Modes Of The Circuit Operation. Functional Obfuscation Is Accomplished By Requiring Use Of The Correct Initialization Key, And Configure Data. Wrong Initialization Key Fails To Enable There Configurator, And A Wrong Configure Data Activates Either A Meaningful But Nonfunctional Or Non-Meaningful Mode. Probability Of Activating The Correct Mode Is Significantly Reduced Leading To An Obfuscated DSP Circuit.*
Indexterms: *Digital Signal Processing (DSP), Functional Obfuscation, Hardware Security, High-Level Transformations, Intellectual Property (IP) Protection, Obfuscation, Reconfigurable Design, Structural Obfuscation.*

I. Introduction

The Problem Of Hardware Security Is A Serious Concern That Has Led To A Lot Of Work On Hardware Prevention Of Piracy And Intellectual Property (IP) [1], Which Can Be Broadly Classified Into Two Main Categories: 1) Authentication-Based Approach, Or 2) Obfuscation-Based Approach. Obfuscation-Based Approach [1] Is Of Interest In This Paper, Which Is A Technique That Transforms An Application Or A Design Into One That Is Functionally Equivalent To The Original But Is Significantly More Difficult To Reverse Engineer. Some Hardware Protection Methods Are Achieved By Altering The Human Readability Of The Hardware Description Language (HDL) Code, Or By Encrypting The Source Code Base Cryptographic Techniques. Recently, A Number Of Hardware Protection Schemes Have Been Proposed That Modify The Finite-State Machine (FSM) Representations To Obfuscate The Circuit's .However, To The Best Of Our Knowledge, No Obfuscation Based IP Protection Approach Has Been Proposed For DSP Circuits [1] In The Literature. This Paper, For The First Time, Presents Design Of Obfuscated DSP Circuits Via High-Level Transformations That Are Harder To Reverse Engineer. From This Standpoint Of View, A DSP Circuit Is More Secure, If It Is Harder For The Adversary To Discover Its Functionality. In Other Words, A High Level Of Security Is Achieved If The Functionality Of A DSP Circuit Is Designed To Be Hidden To The Adversary Our Goal Is To Design Obfuscated Circuits By Applying High-Level Transformations During The Design Phase. The Key Idea Of The Proposed Work Is To Generate Meaningful Design Variations By Exploiting High-Level Transformations [4]. A Critical Challenge For Nano Electronic Systems Is To Achieve Yield And Reliability. As VLSI Technology Scales Into The Nanometer Scale, Devices And Interconnects Are Subject To Increasingly Prevalent Defects And Significant Parametric Variations. Based On Photolithography, We Are Making Layout Features Of Smaller Dimensions Than The Wavelength Of The Light, Which Requires Increasingly Complex OPC And Other DFM Techniques [3] At Increasing Layout Area Cost. Future Nano Electronic Systems Are Expected To Be Based On Self-Assembly Manufacture Of Physical Structure, And Achieve. Reconfiguration Is Further Critical For Nano Electronic Systems [5] To Achieve Yield And Reliability By Bypassing Defective Or Degraded Devices And Interconnects [4], Which Occurrence Cannot Be Avoided Or Reduced Below A Certain Level As Is Determined By The Uncertainly Principle Of Quantum Physics .In This Paper, We Present That Reconfigurable Computing [2] Is Further A Critical Technology To Achieve Hardware Security In The Presence Of Supply Chain Adversaries. In Recent Years, A Growing Number Of Software Based Security Solutions Have Been Migrated To Hardware-Based Security Solutions For Much Enhanced Resistance To Software Based Security Threats. Such Systems Range From Smartcards To Specialized Secure Co-Processing Boxes, Wherein Hardware Provides The Source Of Security And Trust For A Number Of Security Primitives.

However, In Recent Years, It Has Been Brought Into Light That Hardware Is Also Subject To A Number Of Security Threats. The Existing Techniques Mostly Focus On Information Leak From A Hardware System: An Adversary May Extract Cryptographic Keys And Confidential Information From A System By Testing Reverse Engineering , Or Side-Channel Analysis . Design Automation And Test In Europe (DATE) [2] , 2014. Bao Liu Is With The University Of Texas, San Antonio, TX, 78249. Brandon Wang Is With Cadence Design Systems, Inc, San Jose, CA, 95134 . In Today's Global IC Industry, A Supply Chain Adversary, Such As An IP Provider, An IC Design House, A CAD Company, Or A Foundry May Have Access To The Source Code Of The Design, And May Easily Tamper A Hardware System By Planting Time Bombs Which Compromise Hardware Computation Integrity, Or Creating Back Doors Which Enable Information Leak, Bypassing Access Control Mechanisms At Higher (E.G., OS And Application) Levels. The Recently-Released Comprehensive National Cyber Security Initiative Has Identified This Supply Chain Risk Management Problem As A Top National Priority A Supply Chain Adversary's Capability Is Rooted In His Knowledge On The Hardware Design. Successful Hardware Design Obfuscation Would Severely Limit A Supply Chain Adversary's Capability If Not Preventing All Supply Chain Attacks. **Section II** To Show Resent Trents Of Hardware Intellectual Property(IP) Piracy And Reverse Engineering. **Section III** DSP Hardware Protection Methodology Through Obfuscation By Hiding Functionality Via High Level Transformations. **Section IV** To Implement Simulation Verified. **Section V** To Verified Different Value FSM Modes And Reduced Area

II. High Level Transformation

A Supply Chain Adversary Is An Insider Who Is Involved In The Design And Manufacturing Of A Hardware Device. The Tamper Capability Is Based On His Role In The Supply Chain, Specifically, His Read And Write Permission In The Design And The Manufacturing Process Of A Specific Device. An IP Provider [4] Or A Designer For A Specific Module May Have Limited Access To The Design, While A Foundry Or A Chip-Level Integration Designer Has Access To The Whole Device Design. The General Lack Of Access Control In Today's Supply Chain Further Facilitates An Adversary To Gain Knowledge Of A Design And Launch Attacks. Besides Based On His Role In The Supply Chain, A Supply Chain Adversary May Gain Further Knowledge Of A Design By Probing, Testing, Side-Channel Analysis, Or Reverse Engineering. The State-Of-The-Art VLSI Logic Encryption/Locking Techniques [2] Include Combinational Logic Locking And Finite-State Machine (FSM) Locking. Combinational Logic Locking Augments A Combinational Logic Network [3] With An Additional Group Of Lock Inputs Such That The Augmented Combinational Logic Network Has The Same Function As The Original Combinational Logic Network Only If A Specific Vector (Aka A Valid Key) Is Applied To The Lock Inputs .The Simplest Combinational Logic Locking Technique Is To Insert XOR And XNOR Gates Into A Combination Logic Network . An Adversary Knows Which Inputs Are Functional Inputs And Which Inputs Are Lock Inputs. He Can Then Identify The Lock Gates Connected To The Lock Inputs. If A Total Of M Lock Gates Are Inserted In A Combinational Logic Network, The Complexity For An Adversary To Find The Correct Logic May Not Be 2 M . Another Combinational Logic Locking Technique Is To Insert Multiplexers Or Combine Logic Functions Based On Shannon Expansion. The Reason Is As Follows. If A Lock Input Is Connected To A Lock Gate That Is Not A XOR Or XNOR Gate, The Key To The Lock Input Is Implied To Be The Non-Controlling Logic Value Of The Lock Gate An Adversary Can Then Easily Obtain The Key, Unless The Lock Input Is Connected To Multiple Lock Gates And Is Implied To Have Conflicting Logic Values - For Example, The Lock Input Is Connected To A Group Of AND Gates And A OR Gate Which Have The Same Function As A XOR Or XNOR Gate. Recent Trends Of Hardware Intellectual Property (IP) Piracy And Reverse Engineering Pose Major Business And Security Concerns To An IP-Based System-On-Chip (Soc) Design flow We Propose A Register Transfer Level (RTL) Hardware IP Protection Technique Based On Low-Overhead Key-Based Obfuscation Of Control And Data flow. The Basic Idea Is To Transform The RTL Core Into Control And Data flow Graph(CDFG)And The Integrate A Well Obfuscated finite State Machine (FSM) Of Special Structure, Referred As" Mode-Control FSM" ,Into The CDFG In A Manner That Normal Functional Behavior Is Enabled Only After Application Of A Specific Input Sequence.

III. Design Flow Of The Proposed Dsp Circuit Obfuscation Approach

A Novel DSP Hardware Protection Methodology Through Obfuscation By Hiding Functionality Via High-Level Transformations. This Approach Helps The Designer To Protect The DSP Design [5] Against Piracy By Controlling The Circuit Configuration Among The Generated Variation Modes F G SR Clkreconfigurator Reset Re-Set State M U X . . . Select Signal Connection 1 Connection 2 Connection K Obfuscating Configuration FSM Key (Switch Instances)

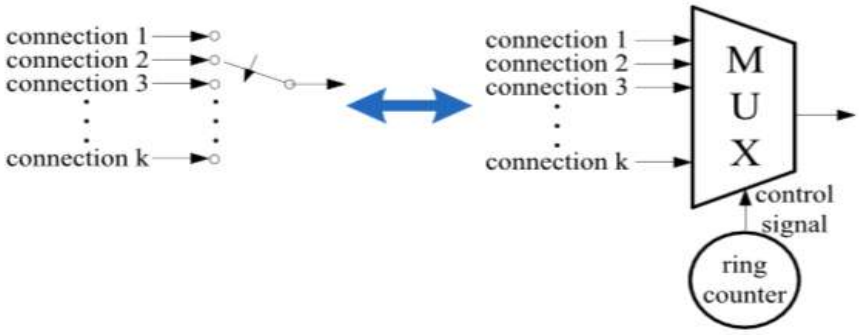


Fig.1 Secure Switch Design Of The Original Design

The Detailed Design Flow Is Described Below:

Step 1: DSP Algorithm. This Step Generates The DSP Algorithm Based On The DSP Application [3]

Step2: High-Level Transformation Selection. Based On The Specific Application, Appropriate High-Level Transformation Should Be Chosen According To The Performance Requirement (E.G., Area, Speed, Power Or Energy).

Step 3: Obfuscation Via High-Level Transformation. Selected High-Level Transformations Are Applied Simultaneously With Obfuscation Where Variation Modes, And Different Configurations Of The Switch Instances Are Designed.

Step 4: Secure Switch Design. The Secure Switch Is Designed Based On The Variations Of High-Level Transformations. Note That Different Configure Data Could Be Mapped Into The Same Mode, Which Only Involves Simple Combinational Logic Synthesis.

Step 5: Two-Level FSM Generation. The Reconfigurator And The Obfuscating FSM Are Incorporated Into The DSP Design As Shown In Fig2. The Configuration Key Is Generated At This Step.

Step 6: Design Specification. This Step Includes The HDL And Netlist Generation And Synthesis Of The DSP System. The Proposed Design Methodology Does Not Require Significant Changes To Established Verification And Testing Flows. In Fact, The Obfuscated DSP Circuit With The Correct Key Behaves Just Like The Original Circuit.

A) Secure Switch Design

Here We Use That The DSP Circuits Can Be Obfuscated Via High-Level Transformations By Appropriately Designing The Switches In A Secure Manner. The Switches Generated By High-Level Transformations Are Periodic N-To-1 Switches. These Switches Can Be Implemented As Multiplexers, Whose Control Signals Are Obtained From Ring Counters (As Shown In Fig 2.Thus, The Security Of The Switch Relies Upon Design Of The Ring Counters Such That The Outputs Of The Ring Counters Can Be Obfuscated. A Ring Counter Is Often Modeled As An FSM. An FSM Is Usually Defined By A 6-Tuple (I, O, S, S0, F,G), Where Is A Finite Set Of Internal States, I And O Represent The Inputs And Outputs Of The FSM, Respectively, F Is The Next-State Function, G Is The Output Function, And S0 Is The Initial State. However, Unlike General Fsms, The FSM [2] Of A Ring Counter Is Input Independent, Such That It Always Transits To The Next State Based On The Current State. As A Result, The Control Signal Of The Switches (I.E., Output Of The FSM) Will Be Periodic.

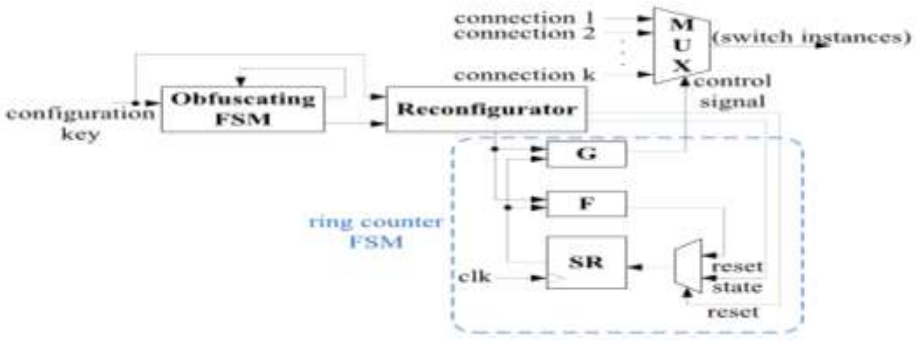


Fig 2 Complete Reconfigurable Switch Design

B) Reconfigurable Switch Design

In Existing Works Have Demonstrated That Functional Obfuscation Can Be Achieved By Embedding A Well-Hidden FSM (I.E., Obfuscating FSM) In The Circuit To Control The Functionality Based On A Key. In Order To Achieve Design Obfuscation By Using High-Level Transformations, We Propose A Reconfigurable Switch Design. The Detailed Implementation Is Shown In Fig. 3, Where SR Represents The State Registers That Store The Information Of The Current State [4]

C) Proposed Methodology

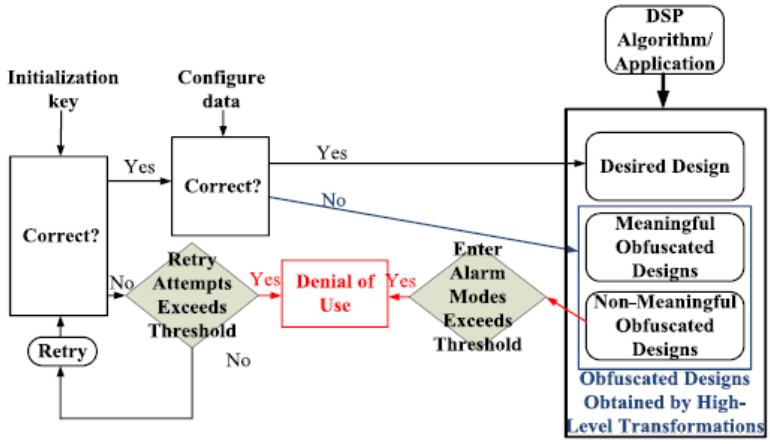
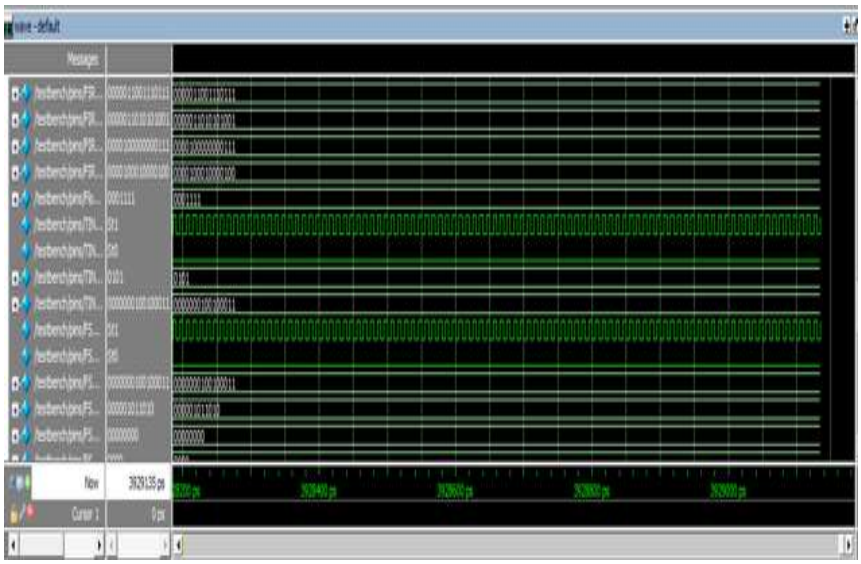


Fig. 3 Proposed Methodology Diagram

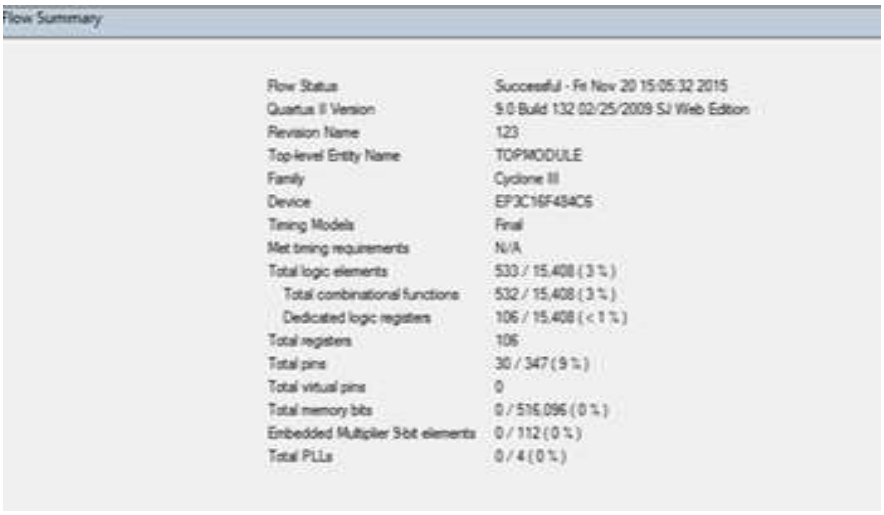
High-Level Transformations Also Allow Design Of Circuits Using Same Data Path But Different Control Circuits. For Example, A Data Path May Implement A 3rd-Order Or A 6thorder Digital Filter, Or In General A (3l) Th-Order Filter, Where L Is A Positive Integer. These Correspond To Different Modes. While These Modes Generate Outputs That Are Functionally Incorrect, These May Represent Correct Outputs Under Different Situations, Since The Output Is Meaningful From A Signal Processing Point [5] Of View. Finally, Other Modes Lead To Non-Meaningful Outputs. The Initialization Key And The Configure Data Must Be Known For The Circuit To Work Properly. Consequently, The Circuit Behaves As An Obfuscated Circuit.

IV. Software Implementation Results

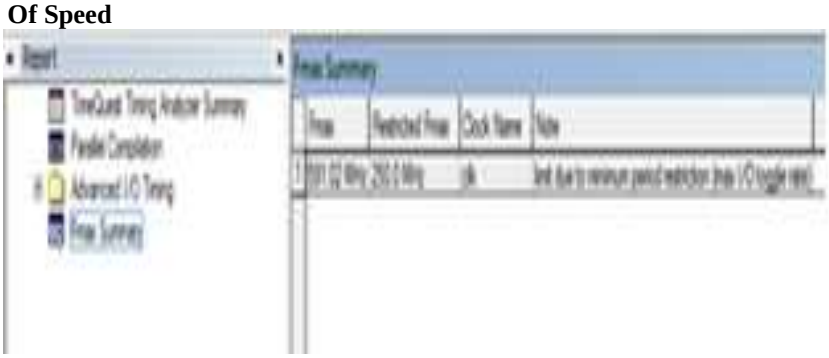
a) Functional Verification In Modelsim



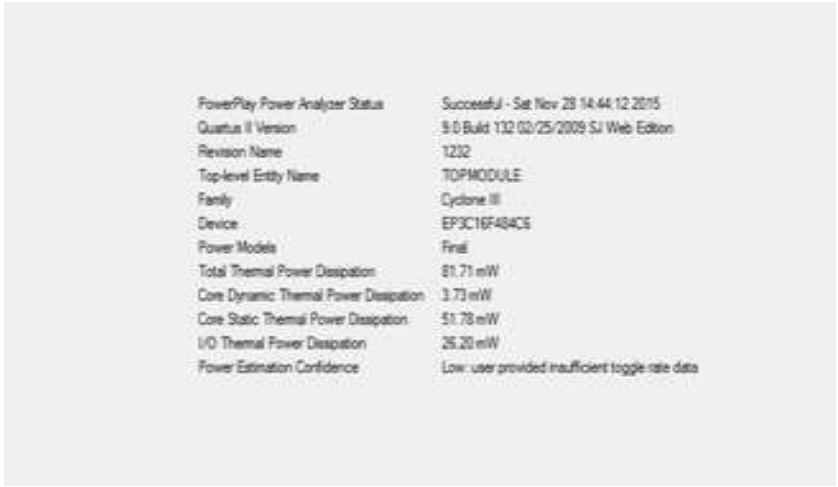
b) Performance Of Area



C) Performance Of Speed



D) Power Analyzer



V. Conculsion

This Paper Presents A Low- Over Head Solution To Design DSP Circuita That Are Obfuscated Both Structurally And Functionally By Utilizing High Level Transformations Techniques.It Is Shown That Verifying The Equivalence Of DSP Circuits By Employing High Level Transformations Will Be Harder If Some Switches Can Be Designed In Such A Way That Are Difficult To Trace, A Secureconfigurable Switch Design Is Incorporated Int The Proposed Design Scheme To Improve The Security.A Complete Design Flow Is Presented In The Proposed Obfuscation Methodology The Variation Modes And The Additional Obfuscating Circuits Could Also Be Designed Systematically Based On The High Level Transformations.Obfuscated And Reconfigure FSM Modes Of Which Reduces The Area Of Performance Speed Improved To 341.53MHZ.

References

[1] R. S. Chakraborty And S. Bhunia, "RTL Hardware IP Protection Using Key-Based Control And Data flow Obfuscation," In Proc. 23rd Int. Conf. VLSI Design, Jan. 2010, Pp. 405–410.

[2] R. S. Chakraborty And S. Bhunia, "HARPOON: An Obfuscationbasedsoc Design Methodology For Hardware Protection," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., Vol. 28, No. 10, Pp. 1493–1502, Oct. 2009.

[3] R. S. Chakraborty And S. Bhunia, "Hardware Protection And Authentication Through Netlist Level Obfuscation," In Proc. Int. Conf. Comput.-Aided Design, Nov. 2008, Pp. 674–677

[4] W. P. Griffin, A. Raghunathan, And K. Roy, "CLIP: Circuit Level IC Protection Through Direct Injection Of Process Variations," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., Vol. 20, No. 5, Pp. 791–803, May 2012.

[5] F. Koushanfar And Y. Alkabani, "Provably Secure Obfuscation Of Diverse Watermarks For Sequential Circuits," In Proc. Int. Symp.Hardw.-Oriented Security Trust, Jun. 2010, Pp. 42–47.