IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 06-10

QR Pattern Driven Hardware Obfusfication and High- Level Transformations

[1]Y.Nisha, [2]S.Sangeetha, [3]Mr.V.Kishore Kumar,
[1,2]UG Students, [3]Assitatnt Professor, Department Of ECE Apollo Engineering College, Poonamalle.

Abstract : *In Recent Years Piracy Over Digital System Is Emerging And Hardware Security Is Aim To Thwart, Overbuilding, And Reverse Engineering (RE) By Obfuscating And/Or Camouflaging. However, These Techniques Incur High Complexity And Power Overheads, And Structural Changes Cannot Provide Any Protection For The Gate-Level Netlist Of The Third Party Intellectual Property (IP) Core Or The Single Large Monolithic IC. In Order To Circumvent These Weaknesses, In This Work We Carried Out QR Code Pattern Driven Functional Obfusfication And Elaborately Analyzes Security Levels And Proposes A Practical Logic Obfuscation Method Over FIR DSP Digital Design With Low Overheads Which Prevent An Adversary From RE Both The Gate-Level Netlist And The Layout-Level Geometry Of IP/IC And Protect IP/IC From Piracy And Overbuilding. Experimental Evaluations Demonstrate The Low Area, Power, And Zero Performance Overhead Of The Proposed Obfuscation Technique.*

Keywords *- Finite State Machine (FSM), Register Transfer Level (RTL) , Intellectual Property (IP) Etc.*

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:

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 Todays 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 . 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.

2.1 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 Clk Reconfigurator Reset Re-Set State M U X . Select Signal Connection 1 Connection 2 Connection K Obfuscating Configuration FSM Key (Switch Instances)

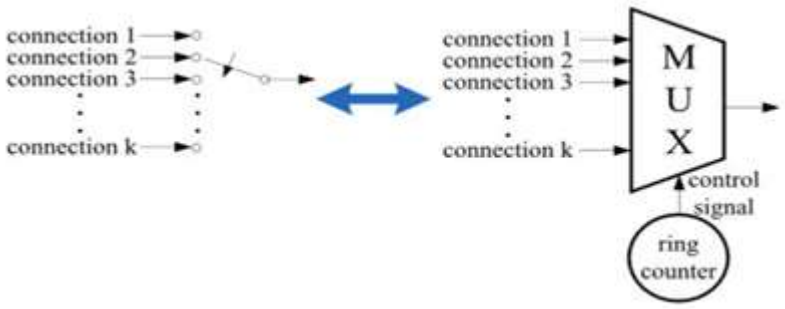

Fig 1.FSM Based Confusion Metrics Architecture

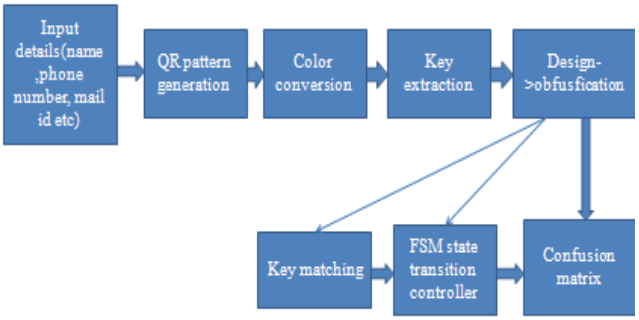

Fig 2. Funtional Block Diagram

2.2 Obfusfication Steps Involved

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).

Step3: 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.

Step4: 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.

Step5: 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.

Step6: 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.

2.3 COLOR QR Code Generation

QUICK Response (QR) Codes [1], [2] Have Rapidly Emerged As A Widely Used Inventory Tracking And Identification Method In Transport, Manufacturing, And Retail Industries [3]. Each QR Code Symbol Consists Of An Encoding Region, Alignment Patterns And Function Patterns, As Shown In Fig. 1. Function Patterns Includes Finder, Separator. These Are Not Used For Encoding The Data. These Are Detected With Several Versions From Version 1 To Version 40.

The Encode Steps Of QR Code Are Shown Below. Firstly Input Data Is Encoded Formed Bit Stream In An Efficient Mode. The Bit Streams Which Are Obtained By Encoding The Data Are Divided Into Code Words. These Code Words Are Again Divided Into Sets Of Blocks And Error Correction Level Is Added To All The Set Of Blocks.

Step 1.1 ─Transform Message M Into A Bit Stream B Of Codes;

Step 1.2 ─Transform Every Three Bits Of B Into Four Bits And Represent Them By A Binary Pattern Block, Resulting In A Pattern Image IP;

Step 1.3 ─Modulate Each Pattern Block Ti Of IP By Two Representative Values Calculated From The Y-Channel Values Of The Corresponding Block Bi Of Target Image IT, Yielding A Modulated Pattern Image IP';

Step 1.4 ─Replace The Y-Channel Of Target Image IT With IP' To Get A Signal-Rich-Art Code Image IC As The Output. In The Second Phase, Given A Camera-Captured Version IC' Of A Paper Or Display Copy Of The Signal-Rich-Art Code Image IC, A Message M', Which Is Supposed To Be Identical To M, Is Extracted From IC' By Four Major Steps:

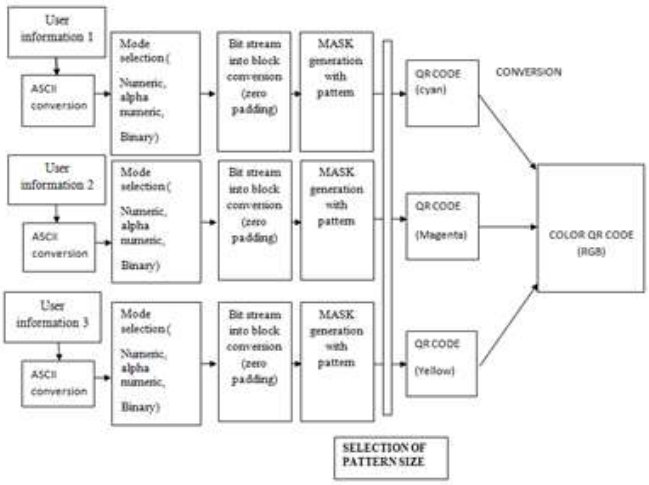

Fig.3 Color QR Code Generations

.

.

III. IMPLEMENTATION

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.

Fig. 4: Color QR Code

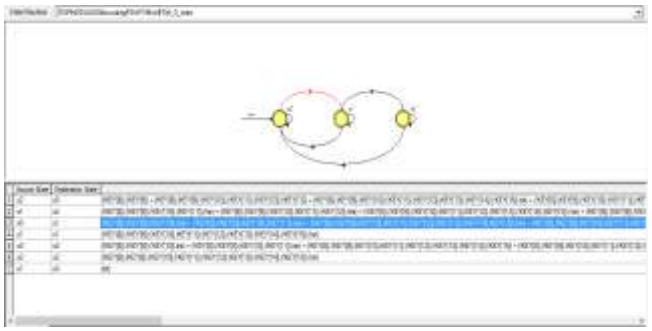

Fig. 5: FSM States

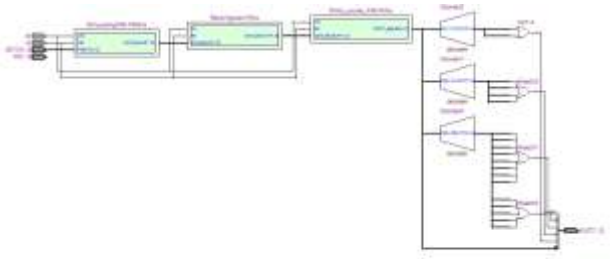

Fig. 6: RTL Viewer

Table 1 Hardware Complexity Report Comparison Using Cyclone III Family Devices

Type	AREA	SPEED
TYPE trade off design(maximum FSM states)	513	317.16 MHz
TYPE volume key input(optimal FSM states)	512	59.66 MHz

IV. CONCLUSION

In This Work, We Proved The Efficiency Of Structural And Functional Obfuscation By Utilizing High-Level Transformation Techniques With Variation In Modes. Here We Construct The Secure Reconfigurable Switch Design Which Will Increases Hardware Complexity Slightly As The As Compared To Existing Method. Compared With All Other Existing Obfuscation Methods, In Our Proposed Methodology, The Generation Of QR Code Followed By Multi Key Extraction Will Give Non-Meaningful Variation Modes In Levels. We Analyze The Complexity Trade-Off Between Numbers Of States In FSM Over Complexity. Finally In Order

To Reduce The Hardware Complexity Without Compromising Speed And Area QR Code Were Used And Its Efficiency Is Proved Through Hardware Synthesis.

REFERENCES

[1] B. Davis, "Signal Rich Art: Enabling The Vision Of Ubiquitous Computing," Proc. SPIE 7880: Media Watermarking, Security, And Forensics III, N. D. Memon, J. Dittmann, A. M. Alattar, And E. J. Delp III, Eds., Vol. 788002, Feb. 2011.

[2] S. Poslad, Ubiquitous Computing: Smart Devices, Environments And Interactions, John Wiley & Sons, Chichester, UK, 2009.

[3] E. Ouaviani, A. Pavan, M. Bottazzi, E. Bruncllli, F. Caselli, And M. Guerrero, "A Common Image Processing Framework For 2D Barcode Reading," In 7th Int. Conf. On Image Process. And Its Appl., Vol. 2, No. 465, Pp. 652–655, Jul. 1999.

[4] C. Zhang, J. Wang, S. Han, M. Yi And Z. Zhang, "Automatic Real-Time Barcode Localization In Complex Scenes," In IEEE Int. Conf. On Image Processing, Pp. 497-500, 2006.

[5] H. Yang, A. C. Kot, And X. Jiang, "Accurate Localization Of Four Extreme Corners For Barcode Images Captured By Mobile Phones," Proc. IEEE Int. Conf. On Image Processing, Pp. 3897-3900, 2010.

[6] 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.

[7] 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.

[8] 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 .

[9] 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.