Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature

Anirban Sengupta, *Senior Member IEEE*, Saraju P. Mohanty, *Senior Member IEEE*, Fernando Pescador, *Senior Member IEEE* and Peter Corcoran, *Fellow IEEE*

***Abstract*—Digital signal processing (DSP) cores are an integral part of consumer electronics (CE) devices. This paper presents a novel methodology for obfuscation of transient fault secured circuits. The approach presented obfuscates fault secured DSP circuits such that the functions of the resulting hardware become non-obvious to an adversary (hindering reverse engineer process). The proposed methodology employs hybrid transformations in succession such as redundant operation removal, resource transformation, and connectivity change using tree height transformation, logic transformation, etc. These are achieved without affecting the functionality of the underlying DSP circuits or requiring significant increase in silicon footprint. The proposed methodology integrates an enhanced fault security feature using multi-cuts that ensures maximum detection capability against transient faults in the DSP circuit. Results of proposed approach indicate stronger obfuscation and enhanced fault security at lower design cost (avg. reduction ~ 14 %), compared to prior art.**

***Index Terms*—DSP core, Obfuscation, Structural change, Enhanced Fault security, CE devices.**

I. Introduction

A System-on-chip (SoC) is an integral component of all modern consumer electronics devices. In these smart devices, a SoC is responsible for the primary processing of data. In the majority of today's SoC designs one or more DSP circuits provide the core data intensive/ power intensive computation. As examples, a DSP engine is widely used in the telecom infrastructure for voice over internet protocol (VOIP) and in digital cameras, mobile phones, consumer audio systems, headsets and TV panels, [1]-[8]. However, a DSP chip may suffer from two diverse hardware vulnerabilities: (a) Single Event Upsets (SEU) [3] and (b) Reverse Engineering (RE) threat [9].

DSP cores need protection against reverse engineering attacks where an adversary could aim to backward engineer the design (from Graphic Data System (GDS) to netlist) to counterfeit and insert malicious logic. In such a case, a sophisticated fault secured DSP circuit can be fully copied without the knowledge of the maker. Research community has been trying to address this issue with the aid of various protection mechanisms such as hardware metering, obfuscation, etc. [10]. Further, as transistor complexity as well as faster devices continued to emanate, SEU manifesting into multi-cycle transient fault also become a major concern for DSP cores. These transient faults are caused due to alpha particles present in the SoC package of a DSP core. As a solution, fault secured DSP designs had emerged [3]. However, the past efforts of research community did not consider reverse engineering (RE) attacks on fault secured DSP cores. RE threats are attacks that are launched from the foundry by an adversary to backward engineer a GDS design of a DSP core to copy the netlist and insert malicious logic. A thematic overview is shown in Fig. 1. Thus, the key here is generating strongly obfuscated fault secured DSP designs that could hinder RE process [10].

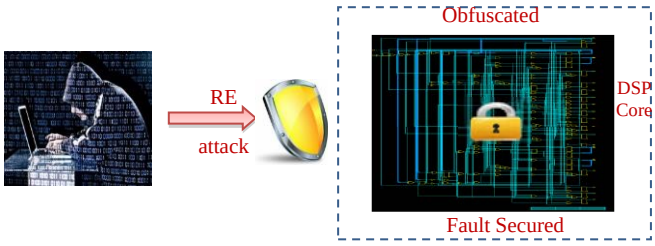

Fig.1. Overview of Obfuscated Fault Secured DSP Core.

The rest of this paper is organized as follows: section II presents novel contributions of this paper. Section III discusses the major related approaches; Section IV describes our proposed methodology. Further, results are presented in Section V, followed by conclusion in Section VI.

II. Novel Contributions of the Paper

The key contributions of this paper are the following:

- Proposes a novel obfuscation methodology for fault secured DSP circuits using hybrid transformations applied at structural level (register transfer level).
- Proposed obfuscation methodology applies successive transformations to the design in two phases, one during structural transformation to the graph and other during

This work has been submitted on March 27th, 2018. This work was financially supported by Council of Scientific and Industrial Research (CSIR) under sanctioned grant no. 22/730/17/EMR-II.

A. Sengupta is with the Discipline of Computer Science and Engineering, Indian Institute of Tech. Indore, 453552, India (e-mail: asengupt@iiti.ac.in).

S. P. Mohanty is with Department of Computer Science, University of North Texas, Denton, Texas 76203, USA (e-mail: saraju.mohanty@unt.edu).

F. Pescador is with the Computer Science and Electronic Engineering Dept., Universidad Politécnica de Madrid, 28031 Madrid, Spain (pescador@sec.upm.es)

P. Corcoran is with the College of Engineering & Informatics, National University of Ireland Galway H91 TK33 (e-mail: peter.corcoran@nuigalway.ie).

fault secured Dual Modular Redundant (DMR) design.

- Proposed obfuscation methodology for fault secured DSP circuits incorporates enhanced fault security capability induced through multi-cuts in the design.

Threat and Fault Model: The proposed work enhances the reverse engineering complexity for an adversary by hiding the original structure of a fault secured DSP design that provides fault security (detection) against transient fault. The proposed approach changes the structure of a fault secured DSP circuit as well as maximizes fault security without affecting its functionality in such a way, that an adversary would find it hard to identify the functionality by inspecting the design.

Problem Definition: Given a DSP design (in C-code or Control Data Flow Graph – CDFG) and assuming worst case transient fault strength (k_c), determine a low design cost structurally obfuscated fault secured DSP circuit. The generated obfuscated fault secured DSP circuit should yield reduced design cost (with minimal overhead) as well as enhance the fault security. In other words, generate an obfuscated fault secured DSP circuit at reduced design cost (A_T^{OBF+FS}, T_E^{OBF+FS}) subjected to transient fault constraint (k_c = 2 control steps), such that the resultant design is significantly structurally transformed than the original counterpart to hinder identification of functionality and reverse engineering process. A_T^{OBF+FS} and T_E^{OBF+FS} are the hardware area and execution time taken by the obfuscated fault secured DSP design respectively.

III. Related Prior Research

Consumer electronics literature has several works dealing with various aspects of digital signal processor [11], [12], [13]. They focus on different aspects of consumer electronics system characteristics such as energy efficiency, high performance, and area efficiency. However, there is lack of security aspect, which do not meet the needs of current scenario in critical CE design, where cyber security plays an imperative role [14], [15], [16]. The process of transforming an original design by keeping its functionality intact is termed as obfuscation such that reverse engineering becomes taxing [4]. Obfuscating a DSP IP can be performed in two ways: a) logic obfuscation, b) structural obfuscation [17], [18], [19], [20]. Through logic obfuscation, the DSP design gets modified by inserting additional component into it and by structural obfuscation; it gets modified by transformations of logic elements in the DSP design [21].

Structural obfuscation [4], [22] is performed for DSP circuits. However, the work in [4] has not performed multi-stage High Level Transformations (HLTs) for fault secured DSP designs. Additionally, obfuscation approach [4] has not obtained low-cost obfuscated fault secured design using multi-checkpointing. Moreover, optimal folding factor evaluation technique is not proposed in [4] that lead to higher design overhead. Further, obfuscation method [22] has not handled protection of fault secured DSP circuits. Therefore, techniques proposed in [22] are not applicable to obfuscate fault secured design. Moreover, no equivalent DSP circuit of obfuscated design is generated during synthesis. SAT solver presented in [23], [24] is capable to reduce the complexity of key-based obfuscated design for combinational/sequential circuit. However, SAT is not scalable for structurally obfuscated DSP cores. The reason is a SAT solver does not scale for multiplications operation [25]. It is observed that for a 3 bit multiplier it generates a large CNF containing 20 clauses. All

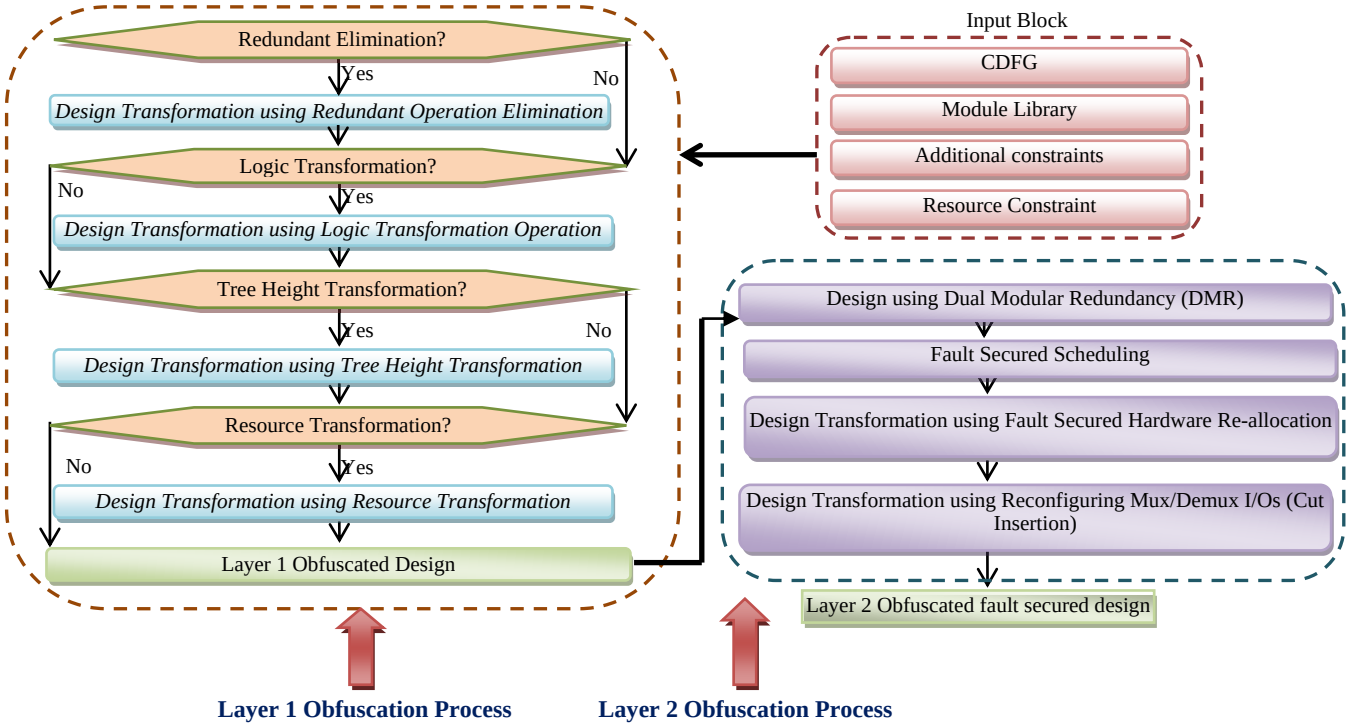

Fig.2. Proposed Obfuscation of Fault Secured DSP Circuits.

the DSP cores tested in this paper comprise of several number of large size multipliers. Moreover, SAT solver is not effective for structural obfuscation. Therefore, structurally obfuscated DSP cores are resilient to SAT solver.

Our proposed approach performs low-cost, compiler-driven, multi-stage HLT techniques for loop-based CDFG to achieve structural obfuscation during algorithmic synthesis. Previous works in the literature did not consider obfuscation of the fault secured DSP design. In the proposed approach a fault secured DSP design is obfuscated through a series of transformation techniques at low design cost. Further, this logic obfuscation employs additional XOR/XNOR gates in the circuits to protect the IP core [26], [27], [28]. This incurs some overhead in design due to insertion of additional logic components/circuitry. To effectively implement this approach with minimal impact on the circuit footprint, determination of the optimal location of these additional key gates is essential.

On the contrary, proposed approach protects the fault secured DSP circuits with minimal overhead and accompanied by multi-checkpointing for enhanced fault security capability. This is because our work employs compiler transformation techniques such as Redundant Operation Elimination (ROE), Logical Transformation Operation (LTO) and Tree Height Transformation (THT) and resource transformation which all are capable to eliminate operations, reduce critical path and reduce logic. Further, the proposed work employs multi-checkpointing that thrives on multiple cut insertion yielding reduction of latency of the design. These factors produce an obfuscated fault secured design with minimal or no overhead compared to a normal un-obfuscated fault secured design.

IV. Proposed Obfuscated Design Methodology

The proposed methodology employs hybrid transformations such as operation change, resource change, connectivity change etc. without affecting the functionality of the DSP circuit. It also integrates enhanced fault security feature that implants several check-points into the design to provide additional detection capability against transient fault.

A. Overview of Proposed Methodology

As shown in the Fig. 2 proposed approach takes a CDFG or C-code of a DSP core, resource constraint and transient fault strength (kc = 2) as input. For obtaining layer 1 obfuscated design, four transformation processes are used which include Redundant Operation Elimination (ROE), Logical Transformation Operation (LTO) and Tree Height Transformation (THT) and resource transformation (RT). The above transformations are performed in sequence. Further layer 2 obfuscated design is obtained from the layer 1 obfuscated design as follows: layer 1 obfuscated design is firstly converted into Double Modular Redundancy (DMR) design, followed with list scheduling on the basis of the user-given resource constraint. Subsequently, layer 2 obfuscated fault secured DSP design is obtained by applying fault secure hardware allocation rules on obfuscated DMR. Next to enhance fault security multiple checkpoints are added by inserting multiple cuts. The details of obfuscation based transformations and generating fault secure design is explained in detail in Section C and D respectively.

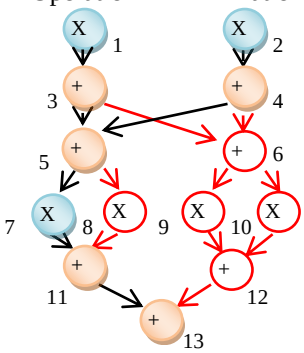

Fig.3. Proposed Redundant Operation Removal based obfuscation.

B. Evaluation Models

1) Area Model: Total area A_T^{OBF+FS} consumed by obfuscated fault secured design is adopted from [29], expressed as:

$$A^{OBF+FS}=\Sigma^{n}{}_{(i=1)}A(R_i)*N(R_i)+A(mux)*N(mux)+A(reg)*N(reg), \quad (1)$$

where, $A(R_i)$, A(mux) and A(reg) represent the area of i^{th} resource, multiplexers and one register respectively; $N(R_i)$, N(mux) and N(reg) represent the number of extracted i^{th} resource, mux and registers required respectively. Extracted resources of i_{th} resource is the maximum number of particular resource used in any control step after scheduling the obfuscated design on the basis of user-given resources.

2) Delay Model: Total latency T_E^{OBF+FS} of the obfuscated fault secured design is calculated using (2):

$$T_E^{OBF+FS}=No\ of\ Control\ Steps \quad (2)$$

Total number of control steps can be termed as the number of total steps required to complete the desired task in obfuscated fault secured design. Here, one control step is taken as 1ns.

3) Fitness Function: The fitness of solution is calculated (considering hardware area consumption and execution delay) on the basis of following fitness function (3):

$$C_f=Ø_1*(A^{OBF+FS}/A_{max}{}^{OBF+FS})+Ø_2*(T_E^{OBF+FS}/T_{max}{}^{OBF+FS}), \quad (3)$$

where, C_f is the cost of the solution; $A_{max}{}^{OBF+FS}$ and $T_{max}{}^{OBF+FS}$ indicates the maximum area and execution delay of obfuscated fault secured design respectively. $Ø_1$ and $Ø_2$ are user defined weights for area and delay respectively, the value lies between [0, 1] (*Note: Both* $Ø_1$ and $Ø_2$ *are kept 0.5 to provide equal preference during cost calculation*).

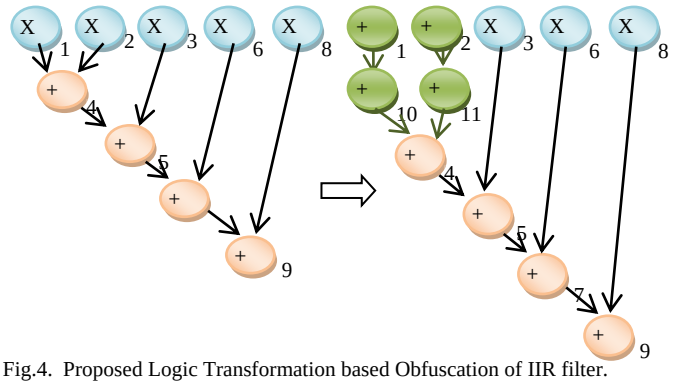

Fig.4. Proposed Logic Transformation based Obfuscation of IIR filter.

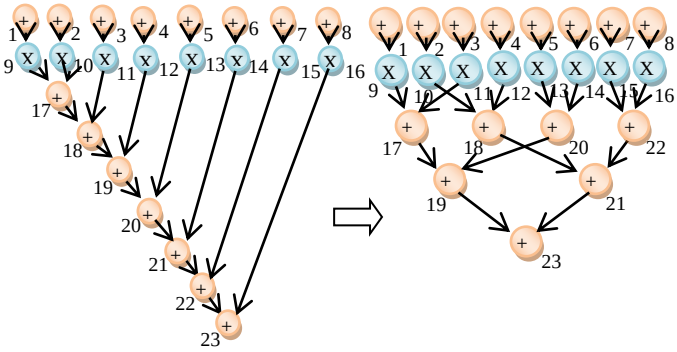

Fig.5. Proposed Tree Height Transformation based Obfuscation of FIR

C. Process of Proposed Obfuscation Methodology

As shown in Fig. 2, proposed obfuscation methodology during algorithmic synthesis is achieved through four different transformations. They are: (1) ROE (2) LTO (3) THT and (4) RT. Our proposed methodology takes the CDFG as input and applies each of the aforementioned transformation to obfuscate it. The detailed process of each obfuscation transformation is explained with a proper example in the following subsections.

1) Redundant Operation Elimination Process: It is an elimination process of redundant nodes which is applied to obfuscate the input DSP design. A node is considered redundant when other node(s) with the same inputs and same operation also exist. In our proposed approach we checked each node in ascending order with respect to the other node. If two such nodes are found satisfying the above conditions, then node with higher number is eliminated *(representing change in inputs of resource)* followed by all the required changes *(representing change of mux/demux configuration)* such that that functionality of the design remains intact. Finally, ROE based structurally obfuscated design is produced.

For example, after applying ROE on Fig. 3 (including all the nodes shaded and non-shaded) only shaded nodes remain in the CDFG (non-shaded nodes are redundant thus excluded). According to our proposed analysis nodes 6, 8, 9, 10, 12 are eliminated. Nodes 5 and 6 are redundant operations hence 6 is eliminates, as a result the input of 9 and 10 gets changed from 6 to 5. Similarly 7, 8, 9, 10 are also satisfying aforementioned conditions, therefore, 8, 9, 10 are deleted and simultaneously

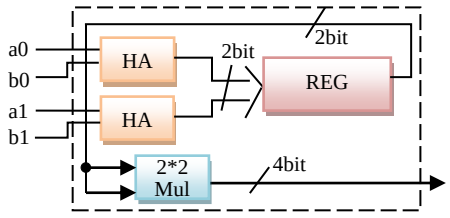

Fig.6. Custom design block used for resource transformation

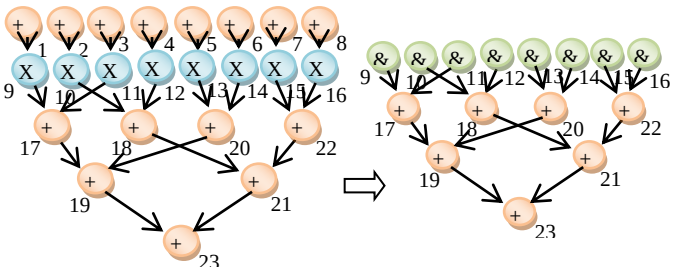

Fig.7. Proposed Resource Transformation based Obfuscation of FIR

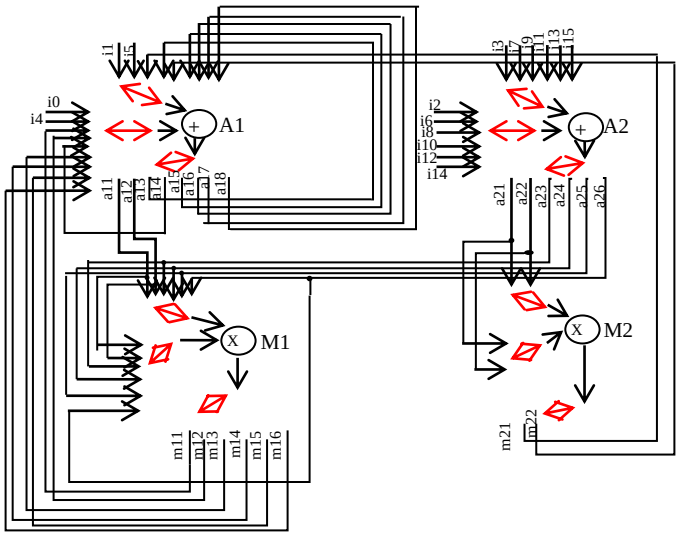

Fig.8. Original non-obfuscated, non-fault secured DSP circuit of a FIR filter

inputs of their children is also changed. After applying the ROE transformation, obfuscated design is obtained.

2) Logic Transformation Process: Another transformation process which is applied to obfuscate the design is, in which nodes of the graph are logically altered without change of functionality of the original graph. In our approach LTO is applied on the first layer of the graph operations and operation type of nodes are changed which leads to increase in number of the nodes. Finally, LT based structurally obfuscated graph is produced as output.

For example, Fig. 4 represents original and logic transformation driven obfuscated design of a FIR filter; newly added/modified nodes *(representing changed inputs to resources)* are marked in green colour and the modified dependencies *(representing changed muxes/demuxes interconnection)* are marked with green line (one multiplication resource is replaced by 2 adders). In this example node numbers 1 and 2 are assumed to have 4 and U ('U' is a variable) as their inputs. As evident, both the designs are functionally equivalent and produce same outputs.

3) Tree Height Transformation Process: It is another obfuscation process which obfuscates the input CDFG by decreasing its height. It divides the critical path dependency

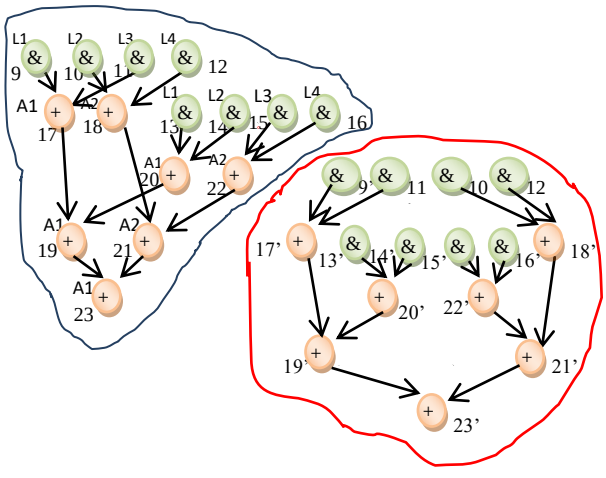

Fig.9. Proposed Obfuscated DMR design of a FIR filter

into temporary sub-computations and evaluates in parallel **(***representing change of mux/demux configuration and resource inputs***)**, therefore, functionality of the graph remains intact. Finally, THT based structurally obfuscated graph is produced as output. Fig. 5 shows the transformation of a FIR filter design before and after THT. Here operations which are done in sequential order are done parallel by shifting the nodes up such that functionality of CDFG remains intact. Nodes 18, 20, 21 and 22 are shifted up, thus, 23 also shifts up.

4) Operation (Resource) Amalgamation: It is one of the obfuscation transformations where two operations are merged into one operation type *(representing a new resource type, inputs configuration, mux/demux connectivity)*. For our proposed approach we designed a *customized resource* that performs "addition followed by a multiplication" (Fig. 6). However, this transformation is applicable only for nodes whose inputs are independent. In this paper we represent this custom resource by symbol '&'. Resource transformation is performed whenever adder execution is followed by multiplier execution during scheduling where the output of adder is used only by same multiplier and inputs of multiplier should also come only from that adder. For example, as shown in Fig. 7, resource transformation is applied on all adders followed by multipliers on first step.

D. Transient Fault security (Detection) and Layer 2 Obfuscation

Due to significance of DSP cores in consumer electronics devices/applications, usually security against transient faults is also incorporated. It has been emphasized in [34], one of the major sources of creating single event transient in DSP SoC is alpha particles. It is also mentioned in [34], the temporal effect (pulse width) of transient fault affecting more than one

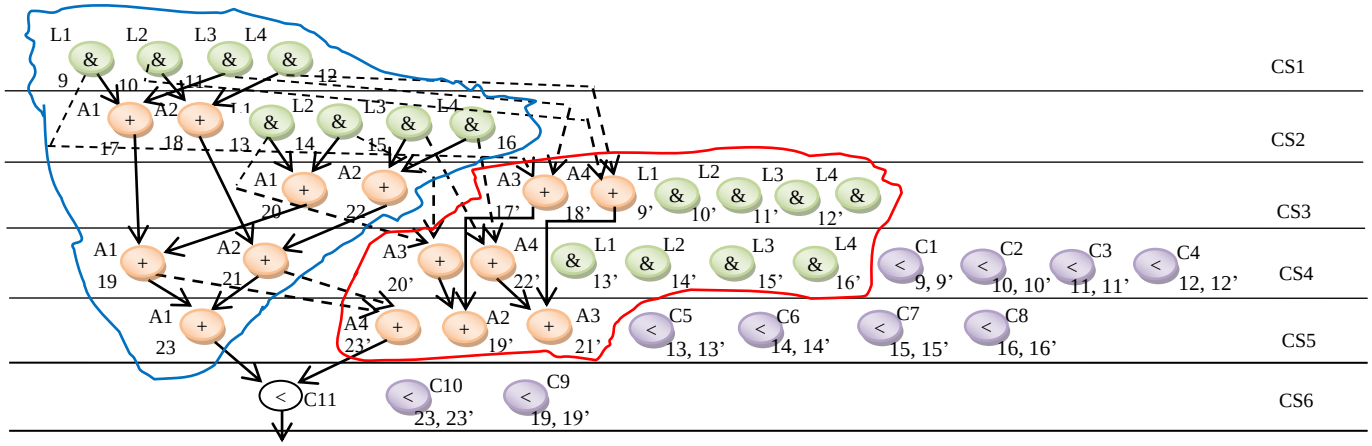

Fig.10. Proposed Obfuscated Fault Secured DSP design of FIR filter (with enhanced fault security feature – multi-cuts)

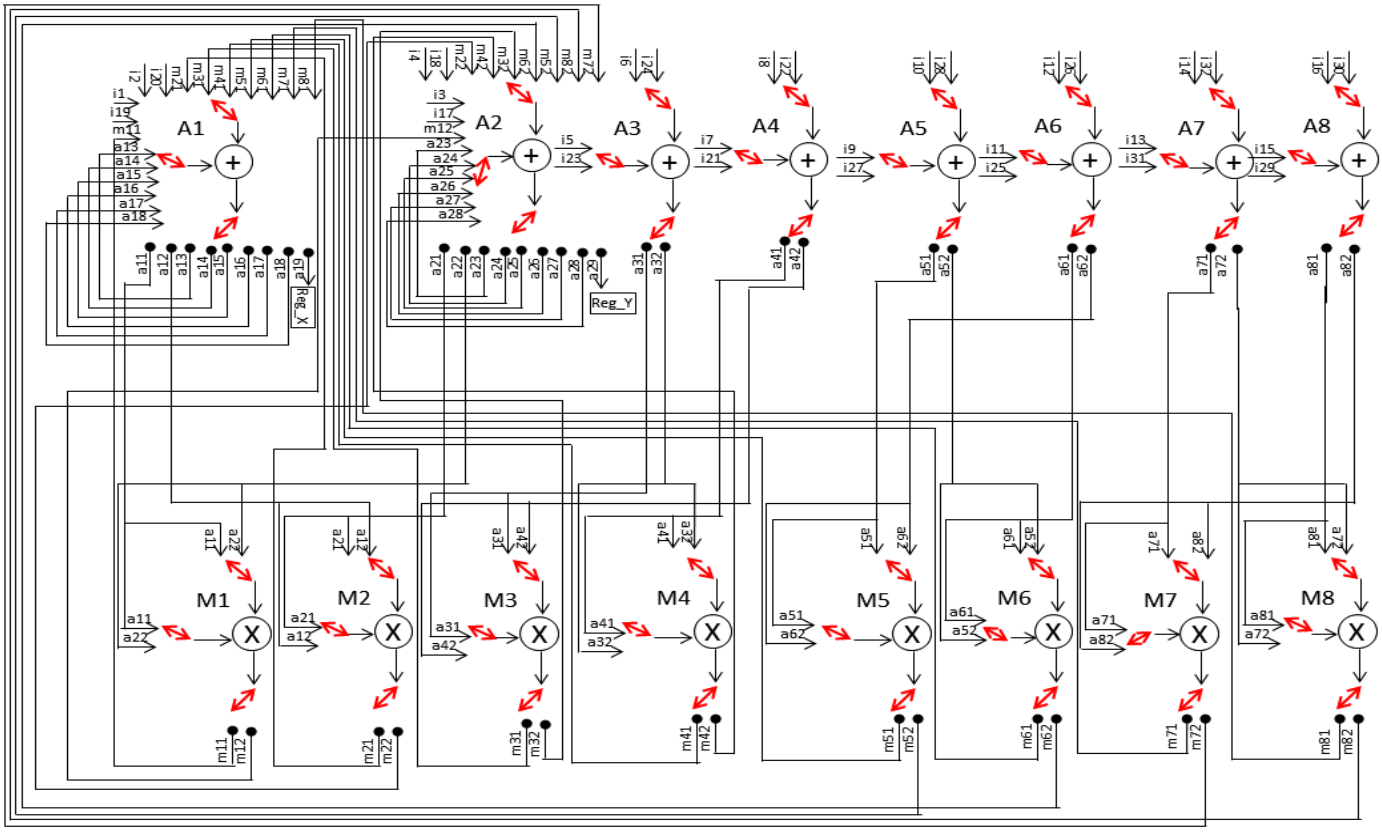

Fig.11. Non-obfuscated DSP circuit of a FIR filter with normal fault security (no enhancement in fault security capability based on [31]).

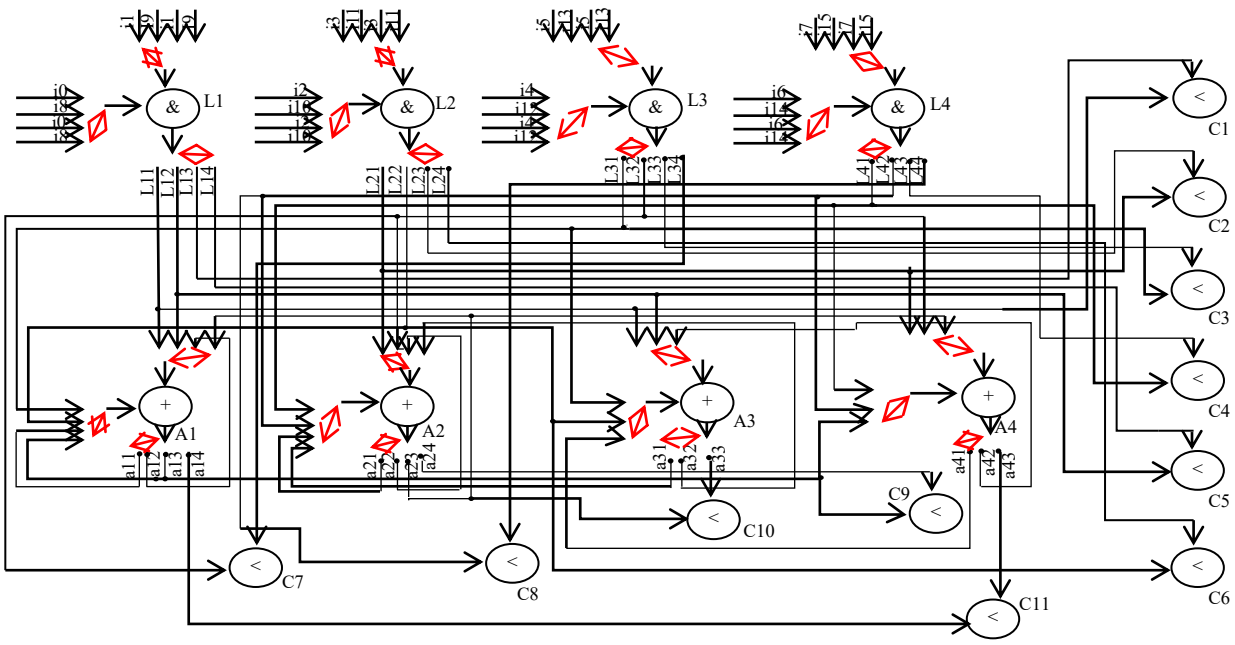

Fig.12. Proposed Obfuscated Fault Secured DSP circuit of FIR filter with enhanced fault security feature.

cycle/control step (up to a range of 2000ps) is likely due to high energy particles. For experimental purpose, authors have assumed that particle with high Linear Energy Transfer (LET) may affect multiple cycles/control steps between the range of 1000 ps (kc=1) to 2000 ps (kc=2).

1) Double Modular Redundancy (DMR) of Obfuscated design: The first step to fault security is generation of DMR version of final obfuscated graph of level 1 obfuscation. Obfuscated DMR represents original and duplicate units of obfuscated graphs obtained earlier during layer 1 obfuscation process. Fig. 9 shows the layer 1 obfuscated DMR design of FIR benchmark (duplicate is encircled with red boundary).

2) Fault Security of Obfuscated design: Transient faults are the faults which affect the device transiently and remain no longer active after some time. When the fault occurs at any resources it gives erroneous output and after k_c-cycles (fault strength), the same resource starts giving back the desired output. Once obfuscated DMR is obtained in previous step, both original and duplicate unit operations are initially scheduled (in concurrency) on the basis of user constraint. After scheduling the original obfuscated design on the basis of user-given constraints, resources are extracted. Extracted resources are the maximum individual resources which are used at any particular control step rather than the resources provided. This initial resource configuration is useful in estimating the initial design cost before fault security rules are incorporated. As discussed earlier, the longest lasting transient fault is 2000ps (which is equivalent to $k_c = 2$ for 1GHz). In next paragraph, we present the fault secured hardware allocation/re-scheduling rules [30]. The initial obfuscated DMR scheduling obtained, may undergo re-scheduling in order to accommodate the fault security rules. Subsequently the final extracted resource configuration will be obtained after this.

Fault Secured Hardware Allocation/Re-Scheduling Rules

1. If delay (control step) difference of the original and duplicate sister operation is greater than k_c, allocate same operator in original and duplicate operation.
2. If rule 1 is not satisfied and delay difference of original and duplicate operation is not greater than or equal to k_c then allocate distinct hardware resource.
3. If either of the above rule is not satisfied and delay difference of original and duplicate operation is less than k_c, then keep shifting duplicate operation by 1 CS below until either of the above rule is satisfied.

Checkpoint (acting as layer 2 obfuscation): Implementing fault security on the obfuscated design, may incur delay design overhead. Cut insertion is done in order to optimize the delay overhead on the fault secure design as well as improve checkpointing. Some data dependency edge is cut in graph therefore, shifting that operation one CS up. According to our proposed approach, a cut is performed after generation of

TABLE I
Comparison of proposed obfuscation with [32] in terms of obfuscation strength.

Benchmark	Proposed approach						[32]	Enhancement in Strength of Obfuscation (%)
	REO (Unique nodes)	LTO (Unique nodes)	THT (Unique nodes)	ALU (Unique nodes)	# of gate affected	SoO		
IIR	-	3	3	-	3040	0.666667	0.33333	100
ARF	10	6	-	-	2400	0.571429	0.42857	33.33
BPF	5	6	2	2	960	0.517241	0.44827	15.38
DWT	-	10	-	-	6688	0.588235	0.52941	11.11
FIR	-	-	12	11	4288	1	0.5	100

TABLE II
Results of proposed methodology for obfuscated fault secured DSP designs.

Benchmark	kc	Resources	FU area (um^2)	Mux area (um^2)	Reg area (um^2)	Area (um^2)	Latency (ns)	Cost
IIR	2	3A,3M,1C	300.418	25.559	6.29146	332.268	8	0.508934
ARF	2	5A,6M,1C	564.659	77.9551	10.2236	652.838	13	0.528534
BPF	2	5A,2M,1ALU,1C	357.827	75.3992	9.43718	442.663	13	0.505261
DWT	2	5A,1M,1C	187.171	63.8976	7.07789	258.147	15	0.490004
FIR	2	4A ,4ALU,1C	473.433	34.5047	3.14573	511.083	8	0.350224

TABLE III
Results of un-obfuscated, non-fault secured (baseline) DSP design.

Benchmark	kc	Resources	FU area (um^2)	Mux area (um^2)	Area (um^2)	Delay (ns)	Cost
IIR	0	1A,3M	245.3674	6.38976	251.757	5	0.35439387
ARF	0	3A,6M	509.609	34.5047	544.114	8	0.40416636
BPF	0	3A,4M	358.6134	34.5047	393.118	8	0.40932128
DWT	0	3A,4M	358.614	19.1693	377.783	10	0.57481188
FIR	0	4A,4M	377.4884	28.1149	405.603	9	0.34422066

DMR followed by employing the hardware allocation rules for transient fault security. In proposed approach, maximum possible cuts are inserted thus resulting in maximum checkpoints (Security). For example, Fig. 10 is the proposed completely obfuscated (layer 1 and 2 integrated) fault secured design obtained after applying 10 checkpoints (maximum possible checkpoints with extracted resources) which results in area overhead as 10 comparators are used but this cost overhead is almost neutralized by decrease in latency (from 8 CS to 6 CS).

In this example, extracted resources are: (4A, 4&). Next checkpoints are applied at 9, 10, 11, 12, 13, 14, 15, 16, 19 and 21 at their respective duplicate nodes (can be seen in Fig. 10). Because of checkpoint at 9 and 11, and 10 and 12, the node 17' and 18' respectively shifted one CS up as they are no longer dependent on 9' and 11', and 10' and 12'. Similarly, the dependencies of 20', 22' and 23' are also altered, hence these all are now dependent upon original graph, thus resulting in shifting to upper CS. Through proposed approach, higher fault security through multi checkpointing can be obtained. The number of comparisons are increased thus fault can be detected at an early stage. Fig. 12 shows the diagram of multi-structural obfuscated fault secured FIR circuit with multi-checkpoint; while fig. 8 represents the un-obfuscated non-fault secured DSP circuit of FIR. Further, Fig. 11 shows the un-obfuscated fault secured circuit of FIR with single checkpoint.

V. Experimental Results

Our proposed approach generates a low-cost obfuscated fault secured DSP circuit through a series of successive hybrid transformations and multi-checkpointing:

A. Experimental Setup and Benchmark

Both proposed approach and, [31], [32] have been implemented in object oriented programming language and executed at 1.90GHz. Area calculations are performed on 15nm technology scale in terms of NAND gates [33].

B. Result of Proposed approach and prior work in terms of Strength of Obfuscation

The Strength of Obfuscation (SoO) provides a measure of difference between the obfuscated fault secured circuit and the original fault secured circuit. TABLE I shows the comparison of SoO of the proposed obfuscation methodology and the corresponding design from [32]. Obfuscation [32] has been selected for comparison as it also performed transformations on CDFGs. The SoO is calculated by counting the unique nodes which are modified after performing 1st layer of obfuscation (Fig. 2) using Eqn. (4):

$$\text{SoO} = (\Sigma^{m}_{(i=1)} \textit{Number of unique nodes modified})/(\textit{Number of nodes before obfuscation}) \quad (4)$$

Higher is the value of SoO, stronger is the obtained security of the design. Hence, harder it is to reverse engineer the circuit. A node is considered as a modified one if either of the following condition is true [32]:

- A parent node or a primary input of a node of an obfuscated CDFG is different from original.
- The child of a node in an obfuscated CDFG is different from original.
- The resource type of a node in an obfuscated CDFG is changed.
- A node of an original CDFG is non-existent in the corresponding obfuscated CDFG.

TABLE I refers the count of nodes modified through individual obfuscation phases. The enhancement of SoO in proposed design is clearly shown in the table.

C. *Results of Proposed approach in terms of Obfuscation Fault Secure DSP design*

TABLE II shows the functional unit area, area of required multiplexers, register area, latency and design cost after performing proposed 1st layer of obfuscation (Fig. 2) and making the DSP fault secure by considering worst fault strength i.e. k_c=2. Functional unit area is calculated corresponding to extracted resources and comparator. It is worthwhile to consider that sometimes an obfuscated design achieves lower latency than a non-obfuscated design since the proposed approach performs series of transformations and optimizations (such as ROE, THT, LT, resource transformations etc.). Thus in such specific scenario, the graph after scheduling may result into lower latency. On the other hand, TABLE III contains the details of the non-obfuscated non-secure DSP design. The major concern associated with

TABLE IV
Results of proposed obfuscated fault secured approach (without checkpointing) and un-obfuscated fault secured [31].

Benchmark	Proposed approach (without checkpointing)				[31]			
	Resources	Area (um^2)	Latency (ns)	Cost	Resources	Area (um^2)	Latency (ns)	Cost
IIR	3A,3M,1C	332.268	8	0.50893418	3A,6M,1C	545.195	7	0.65487893
ARF	5A,6M,1C	652.383	13	0.52853461	7A,7M,1C	747.013	10	0.54227425
BPF	5A,2M,1ALU,1C	442.663	13	0.5052612	6A,4M,1C	545.686	10	0.55590242
DWT	5A,1M,1C	258.147	15	0.4900046	3A,3M,1C	350.946	13	0.57814952
FIR	4A,4ALU,1C	511.083	8	0.35022486	8A,8M,1C	837.945	11	0.52130083

TABLE V
Results of proposed obfuscated fault secured approach (including multi-checkpointing).

Benchmark	kc	Number of Checkpoint(s)	Resources	FU area (um^2)	Mux area (um^2)	Reg area (um^2)	Area (um^2)	Latency (ns)	Cost
IIR	2	1	3A,3M,2C	317.719	30.6708	6.29146	354.681	7	0.4979806
ARF	2	4	5A,6M,5C	633.865	72.8433	11.7965	718.505	10	0.526472276
BPF	2	4	5A,2M,1ALU,5C	427.033	86.9007	11.7965	525.73	11	0.55074730
DWT	2	4	5A,1M,5C	256.377	74.1212	10.2236	340.722	12	0.55391034
FIR	2	10	4A,4ALU,11C	646.448	30.6708	9.43718	686.556	6	0.35180240

TABLE VI
Comparison of proposed obfuscated fault secured approach: with multi-checkpointing vs without checkpointing.

Benchmark	Proposed approach (with multi-checkpointing)					Proposed approach (without checkpointing)			
	# cuts	Resources	Area (um^2)	Latency (ns)	Cost	Resources	Area (um^2)	Latency (ns)	Cost
IIR	1	3A,3M,2C	354.681	7	0.497980	3A,3M,1C	332.268	8	0.50893
ARF	4	5A,6M,5C	718.505	10	0.526472	5A,6M,1C	652.383	13	0.52853
BPF	4	5A,2M,	525.73	11	0.550747	5A,2M,1ALU,1C	442.663	13	0.50526
DWT	4	5A,1M,5C	340.722	12	0.553910	5A,1M,1C	258.147	15	0.49000
FIR	10	4A,4ALU,11C	686.556	6	0.351802	4A,4ALU,1C	511.083	8	0.35022

DMR is either area or delay gets increased; While TABLES II and III are the evidence that in spite of using DMR in proposed approach, the enhancement of cost is marginal.

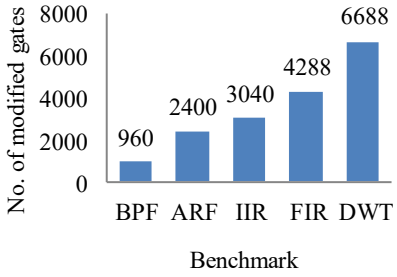

Fig. 13. # of gates affected (structural change) through proposed obfuscation.

D. Comparison of Proposed Obfuscated Fault Secure DSP design with prior work in terms of design cost and obfuscation

TABLE IV shows the comparison of proposed design without insertion of cuts and [31] in terms of area, latency and cost. The cost of proposed design is unsubstantial compared to related design because resource extraction is followed by proposed design which reduces the functional unit area. The proposed approach assures low cost design which is multi structural obfuscated with enhanced fault security whereas [31] comprises only fault secured design with high cost.

TABLE V represents the detailed information of the obfuscated fault secured design with maximum multi-checkpointing in terms of area (functional unit area, mux area and registers area), latency, number of checkpoints applied and cost. Moreover, TABLE VI compares the area, latency and cost of the proposed approach with and without checkpointing. Proposed approach uses the different comparators for all the checkpoints. Further, fig. 13 represents the total modified gates in proposed approach with respect to [31]. For FIR benchmark: Gate count in proposed approach=10592; Gate count in related approach=14880. Moreover, the prominent improvement in the design cost as compared to [31] is shown in fig. 14.

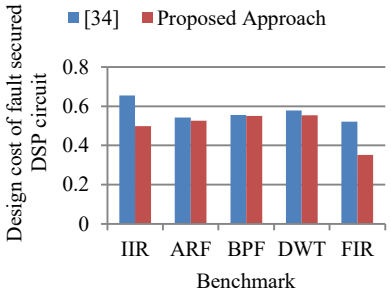

Fig. 14. Comparison of design cost between proposed and [31].

VI. Conclusion

This paper presented a novel methodology for obfuscation of fault secured DSP circuits with enhanced fault security capability. Our future research includes IP core protection using both structural and functional obfuscation.

References

[1] H. Yang, N. Basutkar, P. Xue, K. Kim, and Y. H. Park, "Software defined DVT-T2 demodulator using scalable DSP processors," *IEEE Trans. Consum. Electron*, vol. 59, no. 2, pp. 428–434, 2013.

[2] P. J. Lobo, E. Juarez, F. Pescador, G. Maturana, and M. C. Rodrguez, "A DVB-H receiver and gateway implementation on a FPGA- and DSP based platform," *IEEE Trans. Consum. Electron*, vol. 57, no. 2, pp. 372–378, May 2011.
[3] Anirban Sengupta "Resilient Soft IP-Core Design Against Terrestrial Transient Faults for CE Products", *IEEE Consum. Electron. Mag.*, Volume: 5, Issue: 4, Oct. 2016, pp. 129 - 131.
[4] Y. Lao and K. K. Parhi, "Obfuscating DSP Circuits via High-Level Transformations," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 5, pp. 819–830, May 2015.
[5] S. P. Mohanty, "GPU-CPU Multi-Core For Real-Time Signal Processing," in Proceedings of the *27th IEEE International Conf. on Consumer Electronics*, 2009, pp. 55–56.
[6] S. Walz and Y. Schrder, "A privacy-preserving system architecture for applications raising the energy efficiency," in *Proc. 6th International Conference on Consumer Electronics (ICCE-Berlin),* 2016, pp. 62–66.
[7] A. Sengupta, "Hardware Security of CE Devices," *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 130–133, Jan 2017.
[8] S. P. Mohanty, *Nanoelectronic Mixed-Signal System Design*. McGraw-Hill Education, 2015, no. 0071825711.
[9] A. Sengupta, "Intellectual Property Cores: Protection designs for CE products," *IEEE Consum. Electron. Mag.*, vol. 5, no. 1, pp. 83– 88, Jan 2016.
[10] K. K. Parhi, "Verifying equivalence of digital signal processing circuits," in *Conference Record of the 46th Asilomar Conference on Signals, Systems and Computers (ASILOMAR),* Nov 2012, pp. 99–103.
[11] J. Kim, E. S. Jung, Y. T. Lee, and W. Ryu, "Home appliance control framework based on smart TV set-top box," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 3, pp. 279–285, Aug 2015.
[12] S. Thavalengal and P. Corcoran, "User Authentication on Smartphones: Focusing on iris biometrics," *IEEE Consum. Electron. Mag.*, vol. 5, no. 2, pp. 87–93, April 2016.
[13] S. Lu, X. Huang, L. Cui, Z. Zhao, and D. Li, "Design and implementation of an ASIC-based sensor device for WSN applications," *IEEE Trans. Consum. Electron*, vol. 55, no. 4, pp. 1959–1967, November 2009.
[14] A. Sengupta and S. Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis*," IEEE Access*, vol. 4, pp. 2198–2215, 2016.
[15] J. L. Wong, D. Kirovski, and M. Potkonjak, "Computational forensic techniques for intellectual property protection," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 6, pp. 987–994, June 2004.
[16] F. Koushanfar, *Hardware Metering: A Survey.* New York, NY: Springer New York, 2012, pp. 103–122.
[17] M. Brzozowski and V. N. Yarmolik, "Obfuscation as Intellectual Rights Protection in VHDL Language," *in Proc. 6th International Conf. on Comp. Info. Systems and Industrial Manag. Appli.,* 2007, pp. 337–340.
[18] C. Barria, D. Cordero, C. Cubillos, and R. Osses, "Obfuscation procedure based in dead code insertion into crypter," *in Proc. 6th International Conf, on Computers Comm. and Control (ICCCC),* 2016, pp. 23–29.
[19] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging*," in Proc. ACM SIGSAC Conf. on Computer: Communications Security*, 2013, pp. 709–720.
[20] Y. M. Alkabani and F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security," *in Proc. 16th USENIX Sympo. on Security*, 2007, pp. 20:1–20:16.
[21] A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar, and S. Kundu, "Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 64–77, Jan 2017.
[22] A. Sengupta and D. Roy, "Protecting an intellectual property core during architectural synthesis using high-level transformation based obfuscation," *Electronics Letters*, May 2017.
[23] Keshavarz et al. "SAT-based Reverse Engineering of Gate-Level Schematics using Fault Injection and Probing", 2018. arXiv:1802.08916
[24] D. Liu, C. Yu, X. Zhang and D. Holcomb, "Oracle-guided incremental SAT solving to reverse engineer camouflaged logic circuits," in *Proc. Design, Auto. & Test in Europe Conf. & Exhibition*, 2016, pp. 433-438.
[25] A. Sengupta, D. Kachave and D. Roy, "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*. doi: 10.1109/TCAD.2018.2818720.
[26] J. Zhang, "A Practical Logic Obfuscation Technique for Hardware Security," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 3, pp. 1193–1197, March 2016.
[27] J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending Piracy of Integrated Circuits," *in Proc. Design, Auto. and Test in Europe*, 2008, pp. 1069–1074.
[28] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," *in Proc. Design Automation Conf.*, 2012, pp. 83–89.
[29] D. Roy and A. Sengupta, "Low Overhead Symmetrical Protection of Reusable IP Core Using Robust Fingerprinting and Watermarking During High Level Synthesis," *Future Generation Comp. Sys.*, vol. 71, no. C, pp. 89–101, Jun. 2017.
[30] A. Sengupta and R. Sedaghat, "Swarm Intelligence Driven Design Space Exploration of Optimal k-Cycle Transient Fault Secure Datapath during High Level Synthesis Based on User Power-delay budget", *Elsevier Journal on Microelectronics Reliability*, Vol. 55, issue 6, May 2015, pp-990-1004, March 2015.
[31] T. Inoue, H. Henmi, Y. Yoshikawa, and H. Ichihara, "High-Level Synthesis for Multi-Cycle transient fault Tolerant Datapaths", in *Proc. 17th IEEE International On-Line Testing Sympo.*, 2011, pp 13-18.
[32] A. Sengupta, D. Roy, S. P. Mohanty, and P. Corcoran, "DSP Design Protection in CE through Algorithmic Transformation Based Structural Obfuscation", *IEEE Trans. Consum. Electron.*, Vol. 63, Issue 4, Nov. 2017, pp. 467-476.
[33] NanGate 15 nm open cell library. [Online]. Available: http: //www.nangate.com/?pageid=2328.
[34] Gaillard, Rémi. "Single event effects: Mechanisms and classification." *Soft Errors in Modern Electronic Systems*, pp. 27-54. Springer, 2011.

Anirban Sengupta (M'09-SM'17) is a Tenured Faculty in CSE at Indian Institute of Technology Indore. He has over 150 Publications. He is Distinguished Speaker of IEEE CE Society and serving as Senior Editor of IEEE Consumer Electronics Magazine and General Chair of ICCE 2019.

Saraju P. Mohanty (S'00-M'04-SM'08) is a Professor at the Department of CSE, University of North Texas. He is an author of 250 publications. He is Distinguished Speaker of IEEE CE Society and serves as EiC of IEEE Consumer Electronics Magazine.

Fernando Pescador (M'07, SM'13) obtained his Ph.D. from Universidad Politécnica de Madrid. He is Associate Professor at the same university, head of the Electronic department and Editor-in-Chief of IEEE Transactions on Consumer Electronics.

Peter Corcoran (F'10) is the Founding Editor of IEEE Consumer Electronics Magazine and Personal Chair in Electronic Engineering at NUI Galway. He is co-author on 300+ publications. He is emeritus EiC of IEEE Consumer Electronics Magazine.