Functional Obfuscation of DSP cores using Robust Logic Locking and Encryption

Anirban Sengupta[1], Saraju P. Mohanty[2]
[1]Computer Science & Engineering, Indian Institute of Technology Indore, India
[2]Computer Science & Engineering, University of North Texas, USA
Email: asengupt@iiti.ac.in; Saraju.Mohanty@unt.edu

Abstract— **Obfuscation plays a key role in thwarting attacks launched through reverse engineering process. This work presents a new obfuscation process for DSP cores using improved logic locking and encryption that incurs minimum design overhead and achieves reduced design cost compared to state of the art approaches. The proposed approach integrates particle swarm optimization driven design space exploration system (PSO-DSE) for obtaining reduced design cost of obfuscated DSP designs. Enhanced security of locking is provided through locking blocks that are capable of locking each output data bit of functional resources with 8 key bits. The presented approach includes countermeasures against key sensitization attacks, SAT attacks and removal attacks. Results indicate that the proposed approach has been capable of achieving enhanced obfuscation security by at least 4.29 e+9 times and a design cost reduction ~ 6.5 % compared to a recent approach.**

Keywords— robust locking, functional obfuscation, DSP core

I. INTRODUCTION

The rapid technology scaling alongside with high cost of maintaining advanced fabrication facility has forced many design houses to become fabless. These fabless design houses have to rely on third-party fabrication facilities rendering feasibility of several threats resulting into IP piracy, Trojan, IC overbuilding etc. Consequently, several Intellectual Property (IP) core protection/hardware security mechanisms have been proposed such as IP metering, Trojan detection, watermarking, etc. [1-14]. Another recent mechanism is 'functional obfuscation' also known as 'functional locking' where the primary motive of functional locking is to insert locking components into the design such that correct output cannot be extracted until the valid keys are applied to the locked design.

Functional locking can be performed using several locking units such as AND/OR gate [3], muxes [4],[12], XOR/XNOR gate[7]. Each of these techniques has its own advantages and vulnerabilities. Authors in [7],[8] have presented 'key sensitization' based vulnerabilities and have suggested protection mechanism against it. Though the logic locking technique presented in [7],[8] is good, but it fails to integrate 'multi-pairwise' security. Further, this technique does not incorporate mechanism to generate optimal functionally obfuscated design as well as does not target DSP cores, unlike proposed approach.

In our proposed approach, we present novel 'IP functional locking blocks' (ILBs) for obfuscation of DSP cores. Further, through our sample ILBs we have presented a robust security locking against 'key sensitization' attacks through 'multi-pairwise' security. The novelties of proposed approach are:

a. The proposed approach presents novel ILB based functional obfuscation for DSP cores (represented as control data flow graphs (CDFGs)).

b. The proposed approach induces enhanced security in ILBs against 'key sensitization' attacks through 'multi-pairwise' security.

c. The presented methodology incorporates PSO-DSE to generate low-cost locked netlist based on power-delay tradeoff.

II. PREVIOUS WORKS

This paper targets protection against 'key sensitization attacks' (introduced in [7]) through sample IP Locking blocks. Authors of [7], [8] have introduced few security features that provides protection against 'key sensitization attacks'. In our method, we have enhanced these security characteristics inducing enhanced resiliency against 'key sensitization attacks' as discussed later in section III. The approach presented in [7], [8] proposes resiliency through logic obfuscation using XOR/XNOR gates only. However, proposed ILBs being a composite blend of several different gate types enhances security of our approach using 'multi-pairwise' security feature. Authors of [10], [7] have shown SAT attack on ISCAS'85 Benchmark. Although, SAT attacks are not scalable (applicable) on multiplication [15-19] (thus not applicable on multipliers present in DSP cores) we have shown proactive protection against SAT attacks using AES encryption as an anti-SAT block. Moreover, the proposed work integrates optimization framework to generate optimal solution using power-delay tradeoff.

III. OBFUSCATION APPROACH FOR DSP CORES

A. Problem

A CDFG, library, control parameters are provided as inputs. To generate a robust, low-cost, locked netlist resilient to 'key sensitization' and SAT attacks

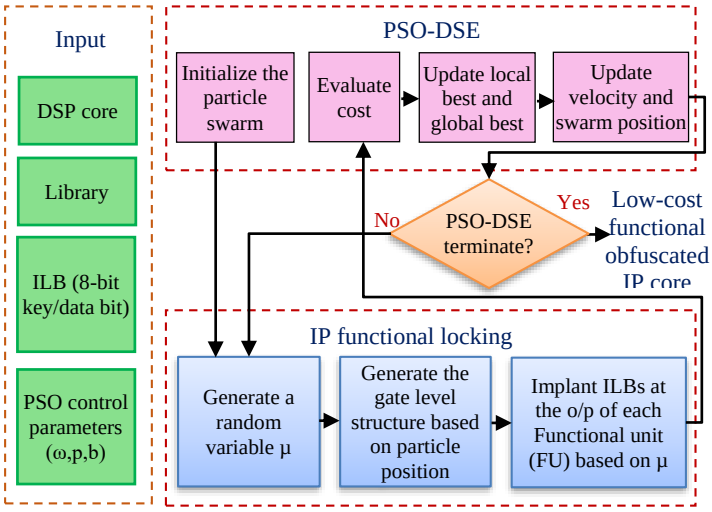

Fig.1. proposed functional obfuscation methodology

B. Motivation of using PSO-DSE during obfuscated netlist generation.

In this section we will elaborate on motivation for incorporating PSO-DSE framework. As depicted in fig. 1, introduced methodology includes chief components namely PSO-DSE component and IP functional locking component. The PSO-DSE component is responsible for exploring low cost design solution, while IP functional locking components performs the logic locking of the design solution. In initial step of our proposed methodology inputs are provided into PSO-DSE component where each particle is encoded as per eq.(1).

$$X_i = \{n(R1), n(R2), \ldots, n(Rd), \mu\}, \quad (1)$$

Where, X_i denotes i^{th} particle of the swarm, $n(R_d)$ signifies the number of resource in d^{th} dimension of the design space and μ is ILB insertion parameter. The initial particles are set using the following technique:

$X_1 = \{\min(R_1), \min(R_2), \ldots, \min(R_d), \mu\}$

$X_2 = \{\max(R_1), \max(R_2), \ldots, \max(R_d), \mu\}$

$X_3 = \{(\min(R_1)+\max(R_1))/2, (\min(R_2)+\max(R_2))/2, \ldots \ (\min(R_d) + \max(R_d))/2, \mu\}$,

Where, $\min(R_1)$ and $\max(R_1)$ denotes minimum and maximum number of resources of resource type R_1. Similarly, the remaining particles in the swarm can be initialized as

$X_i = [\{(\min(R_1)+\max(R_1))/2 \pm \alpha, (\min(R_2)+\max(R_2))/2 \pm \alpha, \ldots, (\min(R_D) + \max(R_d))/2 \pm \alpha\}, \mu]$

Where α symbolizes an arbitrary integer between minimum and maximum number of resource in d^{th} dimension of the design space. Subsequently, for each particle $X_1, X_2, \ldots, X_n$ based on its respective position (resource configuration) in the design space gate level structure is produced. Later on the sample IP functional locking blocks (ILBs) are implanted at the output bit

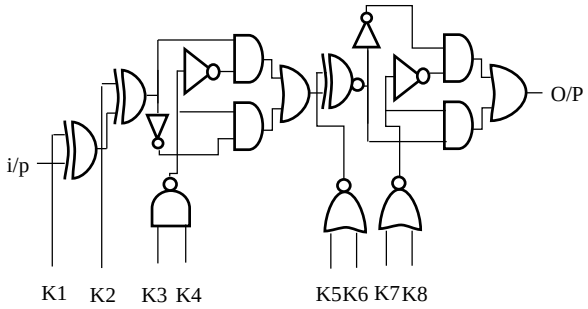

Fig. 2 Sample configured IP functional locking block

of resource Rj, as per ILB insertion parameter 'μ'. For example if 'μ = 2' then one of the ILBs is randomly selected and inserted at first two output bits of Rj. This process is repeated till ILBs are inserted at o/p bits of all the resources. Subsequently, for each particle X_n, the cost of the locked netlist is evaluated as per eq. (2)

$$C_f(X_i) = \varphi_1 \frac{P^{FL}}{P_{max}^{FL}} + \varphi_2 \frac{D^{FL}}{D_{max}^{FL}} \quad (2)$$

Here $C_f(X_i)$ represents normalized fitness of particle X_i, φ_1 and φ_2 signifies user specified weight of power and latency of the cost function (kept at 0.5 each to give same priority). P^{FL} and D^{FL} signify power and delay respectively of functionally locked (FL) design solution. P_{max}^{FL} represents maximum power of FL design in the design space. Likewise, D_{max}^{FL} signifies maximal latency of FL design. Once cost is evaluated local best is evaluated for each particle (X_i) as the minimal cost solution obtained by that specific particle till the present iteration. Subsequently, global best is evaluated. Subsequently, the particle's velocity and positions are updated. This is continued till stopping criterion is met (see [20] for PSO-DSE). Thus, an optimal solution is obtained based on power-delay tradeoff.

C. Security perspective of proposed IP functional locking methodology

C.1 ILB

We introduce IP functional locking blocks. A sample configured ILB is shown in Fig.2. Similar ILBs can be configured (with different architecture but same security) based on the designer's requirement (encrypted output). The sample ILBs includes strong security characteristics such as multi-pairwise security, valid key space, prevention of key gate seclusion etc. These characteristics deliver robust security against Reverse Engineering (RE) and key sensitization attacks. Using this attack, an adversary aims to recognize input combinations on locked netlist which (when applied on functional IC [7]) can produce valid key-bits to outputs.

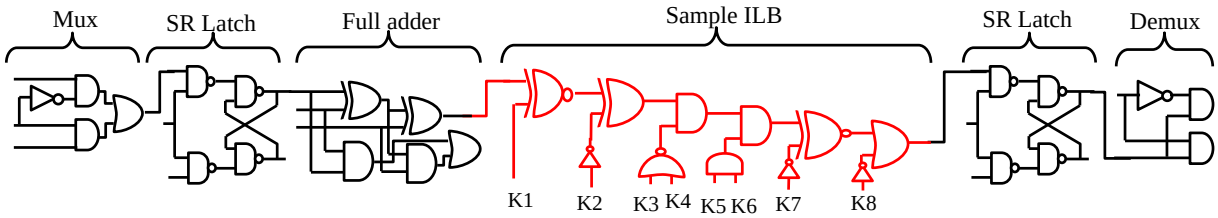

Fig. 3 randomly extracted portion of locked obfuscated netlist showing ILB reconfigured based on AES encrypted output

- Multi-pairwise security: If an attacker is unable to sensitize key-bit K1 to o/p without adjusting the value of key-bit K2 (vice-versa), then K1 and K2 are pairwise secure [7]. Multi-pairwise security is achieved when any key-bit cannot be sensitized to the output without adjusting the remaining key-bits (usually more than one). For example in fig. 2, any key bit of the Sample ILBs cannot be sensitized to the o/p, without adjusting all of the residual 7 key inputs. Thus, defence against key-sensitization based attack can be augmented using multi-pairwise security.
- Prohibiting key gate seclusion: Isolated key gates are vulnerable to key sensitization attack. An isolated key gate is described as a gate K_{iso} if there is non-existent link between K_{iso} and any of the residual key gates (key bit i/ps) and vice-versa. However, presented ILBs are a mixture of interdependent key inputs thus prohibiting isolated key gates.
- Defence against run of key gates: Some combinations of key gates linked adjacent to each other have been shown to be replaceable with a single key gate. This type of run of gates vulnerability is infeasible for ILB due to complex interleaving within gates for 8 key i/ps.
- Non-mutable key gates: Muting is an effort of an adversary to control primary input between any two key gates k_n and k_m such that k_n's value cannot prevent sensitization of k_m[7].

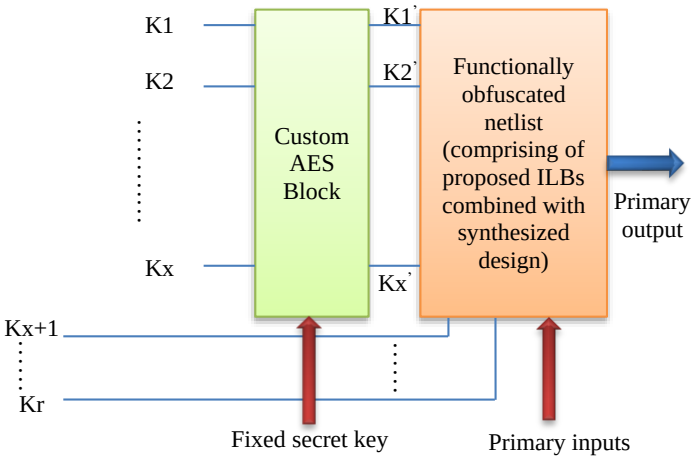

Fig. 4 Safeguarding from SAT attack and removal attack

Our proposed ILBs enhances the security of each key input with the remaining 7 key inputs i.e. an attacker cannot sensitize any key input without knowing/controlling remaining 7 key inputs. Moreover, there is no controllable primary inputs in our proposed ILBs.

C.2 Resiliency against different attack scenarios

(i) *Resiliency against key sensitization*: As discussed in the section III.C.1, a circuit comprises of isolated or mutable key gates is vulnerable to key sensitization attack. However, our customized ILBs doesn't comprises of either isolated or mutable key gates thus are resilient to key sensitization based attacks. Moreover, our proposed ILB structure enhances the security of the proposed approach through multi-pairwise security feature and confirms defense against run of key gates.

(ii) *Resiliency against IP piracy and Trojan insertion attacks*: The primary motive of a pirate is to achieve monetary gain by reselling an IP. However, to achieve this motive he/she has to unlock the correct functionality of the locked IP. Similarly, insertion of Hardware Trojans has to be done at safe places hence requires correct understanding of an IP. This being difficult for proposed work, hence makes proposed obfuscated design resilient to IP Piracy and Trojan insertion based attack.

(iii) *Resiliency against SAT attacks*: SAT attacks are not scalable for multiplications as its results in large CNF even for a small size multiplier. Since DSP cores comprise of several multiplications (multipliers), thus, SAT solver will not be scalable for these designs. Nevertheless, a proactive countermeasure against SAT (considering efficient SAT solvers are developed in future) using **lightweight (using less than 1 % of cyclone II FPGA resources) custom (not in public domain) AES block** is shown in fig.4. An AES circuit with fixed secret key for an input generates an encrypted output. Based on the

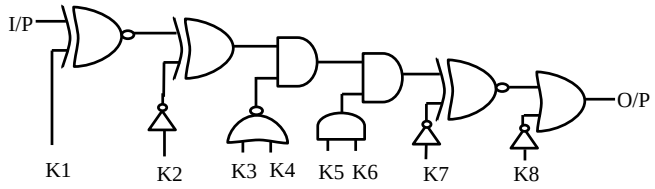

Fig.5. Sample of a single reconfigured ILB using encryption resulting from AES (only one ILB is shown for brevity)
Sample complete encrypted o/p: CDADC8663FFF1E8C2FD9F36409624A60

encrypted output the ILBs can be internally re-organized by the designer such that key inputs of ILBs matches with the encrypted output of AES block. Fig. 5 shows an example of a reconfigured ILB based on the AES.

(iv)*Removal attack*

(i) The presented approach uses subset of re-configured (re-organized) ILB (refer fig.5) implanted in the netlist. This reconfiguration is performed subjected to the AES encrypted o/p conforming to the secret key. This indicates that inside ILB configuration gets modified every time depending on the covert key and i/p selected. It is difficult for an attacker to recognize the reconfigured ILB as there is no fixed template and corresponding secret key to encrypt is unknown.

IV. IMPLEMENTATION

Approach [7] and approach work both have been realized in java and run on Intel Core i5 3210M CPU with 4GB. 15 nm NanGate library is as a base for evaluating the cell values of power and delay [21].

A. Security analysis

The security is represented through eq. (3)

$$K_S = 2 \wedge (b * m * f) \quad (3)$$

Where K_S represents the key-space (S^{OBF}), b = key-bits per ILB, m = # of ILBs per resource, f = number of resources in the datapath. Table I shows that we have obtained a security enhancement of at least 4.29 e+9, w.r.t. [7] for the tested DSP benchmarks. This is because in the proposed approach we have incorporated 8-bit key per o/p data bit for improved logic locking. This results in higher functional obfuscation security than [7].

B. Design cost analysis

Table II illustrates the comparative study of cost between proposed approach and [7]. Cost minimization on average of 6.33% is observed for the tested DSP cores. As discussed earlier design cost reduction is achieved due to low-cost obfuscated design solution explored using PSO-DSE framework integrated with proposed obfuscation approach. The proposed approach results in marginal increase in critical path delay as overhead due to addition of ILBs (compared to baseline). However considering the bigger picture, the overall delay becomes optimized after integrating PSO-DSE compared to [7]. Thus production cost does not increase at all compared to state of the art techniques.

V. INFERENCE

This work introduced a new optimal obfuscation process that incorporates improved security techniques. Comparative study with [7] yielded significant security enhancement (strength of obfuscation) and reduction of cost.

Table I. Comparative study of proposed approach with [7] in terms of security (obfuscation)

Benchmark		No. of key-bits encoded for proposed obfuscation (r)	S^{OBF} of proposed approach (using eq. 3)	No. of key-bits encoded for [7] (r)	S^{OBF} of [7] (using eq. 3)	S^{OBF} enhancement of proposed approach (by factor of)
Name	Size					
DWT	10958	128	3.40 e+38	96	7.92 e+28	4.29 e+ 9
ARF	14833	256	1.15 e+77	112	5.19 e+33	2.23 e+43
FIR	16047	320	2.13 e+96	144	2.23 e+43	9.57 e+52
JPEG IDCT	42710	1344	3.83 e+404	432	1.10 e+130	3.46 e+274

Table II. Comparative study of proposed work with [7]

Benchmark	Proposed functionally obfuscated Design Solution	Cost of proposed approach	Design Solution of [7]	Cost of [7]	Cost Reduction (in %)
IIR	1A, 2M, μ=4	0.6810	2A, 4M	0.7427	8.30 %
DWT	1A, 1M, μ=1	0.7549	3A, 3M	0.7708	2.06 %
ARF	2A, 2M, μ=3	0.5259	3A, 4M	0.5281	0.41 %
FIR	3A, 2M, μ=4	0.5638	4A, 5M	0.5853	3.67 %
JPEG IDCT	11A,10M,μ=2	0.3629	12A,15M	0.4455	18.54 %

ACKNOWLDGEMENT

This Publication is an outcome of the R&D work undertaken in the project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India, being implemented by Digital India Corporation (formerly Media Lab Asia) and also financially supported by Council of Scientific and Industrial Research under sanctioned grant no. 22/730/17/EMR-II

REFERENCES

[1] A. Sengupta, "Intellectual Property Cores: Protection designs for CE products," in IEEE Consumer Electronics Magazine, vol. 5, no. 1, pp. 83-88, Jan. 2016.

[2] A. Sengupta, "Hardware Security of CE Devices [Hardware Matters]," in IEEE Consumer Electronics Magazine, vol. 6, no. 1, pp. 130-133, Jan. 2017.

[3] S. Dupuis, P. Ba, G. D. Natale, M. Flottes, and B. Rouzeyre, "ANovel Hardware Logic Encryption Technique for Thwarting Illegal Overproduction and Hardware Trojans," in Proc. IEEE International On-Line Testing Symposium, 2014, pp. 49–54.

[4] J. Rajendran, H. Zhang, C. Zhang, G. Rose, Y. Pino, O. Sinanoglu,and R. Karri, "Fault Analysis-Based Logic Encryption," IEEE Trans. Comput., vol. 64, no. 2, pp. 410–424, 2015.

[5] A. Sengupta and S. Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis," in IEEE Access, vol. 4, pp. 2198-2215, 2016.

[6] A. Sengupta and S. Kundu, "Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions," in IEEE Transactions on Very

Large Scale Integration (VLSI) Systems, vol. 25, no. 12, pp. 3265-3267, Dec. 2017.

[7] M. Yasin, J. Rajendran, O. Sinanoglu, and R. Karri. "On improving the security of logic locking." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 35, no. 9 (2016): 1411-1424.

[8] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. "Security analysis of logic obfuscation." In Proceedings of the 49th Annual Design Automation Conference, ACM, 2012, pp. 83-89.

[9] A. Sengupta, S. Bhadauria and S. P. Mohanty, "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 4, pp. 655-668, April 2017.

[10] Subramanyan, Pramod, Sayak Ray, and Sharad Malik. "Evaluating the security of logic encryption algorithms." In Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on,pp. 137-143. IEEE, 2015.

[11] A. Sengupta and D. Roy, "Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach [Hardware Matters]," in IEEE Consumer Electronics Magazine, vol. 6, no. 2, pp. 118-124, April 2017.

[12] S. M. Plaza and I. L. Markov, “Solving the Third-Shift Problem in IC Piracy With Test-Aware Logic Locking,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 34, no. 6, pp. 961–971, 2015.

[13] A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran, "DSP design protection in CE through algorithmic transformation based structural obfuscation," in IEEE Transactions on Consumer Electronics, vol. 63, no. 4, pp. 467-476, November 2017.

[14] A. Sengupta, D. Roy and S. P. Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. PP, no. 99, pp. 1-1.

[15] B. Brady, Y. Yang ,”The Effects of Arithmetic Encodings on SAT Solver Performance”, [Online] http://citeseerx.ist.psu.edu/viewdoc/ download? doi=10.1.1.92.6332&rep=rep1&type=pdf.

[16] Y. Xie A. Srivastava, ”Mitigating SAT Attack on Logic Locking”, [Online] https://iacr.org/workshops/ches/ches2016/presentations/0917% 20Session%203/CHES2016_Session3_1.pdf, 2018

[17] P. Beame, V Liew ”Towards Verifying Nonlinear Integer Arithmetic” 29 th international conf. on CAV, 2017, pp. 239.

[18] S. Chakraborty, A. Gupta, R. Jain “Matching Multiplications in Bit-Vector Formulas”, Springer International Publishing, 2017, pp.131-150.

[19] M. Finke, “Equisatisfiable SAT Encodings of Arithmetical Operations”, [Online] http://www.martin-finke.de/documents/ Masterarbeit_bitblast_ Finke.pdf, 2015.

[20] V. K. Mishra, and A. Sengupta. "MO-PSE: Adaptive multi-objective particle swarm optimization based design space exploration in architectural synthesis for application specific processor design." *Advances in Engineering Software* 67 (2014): 111-124.

[21] Express benchmarks http://www.ece.ucsb.edu/EXPRESS/benchmark/