High Level Synthesis Based Hardware Security and IP Core Protection (IPP)

IEEE ISICAS Satellite Workshop

Oct 20, 2024

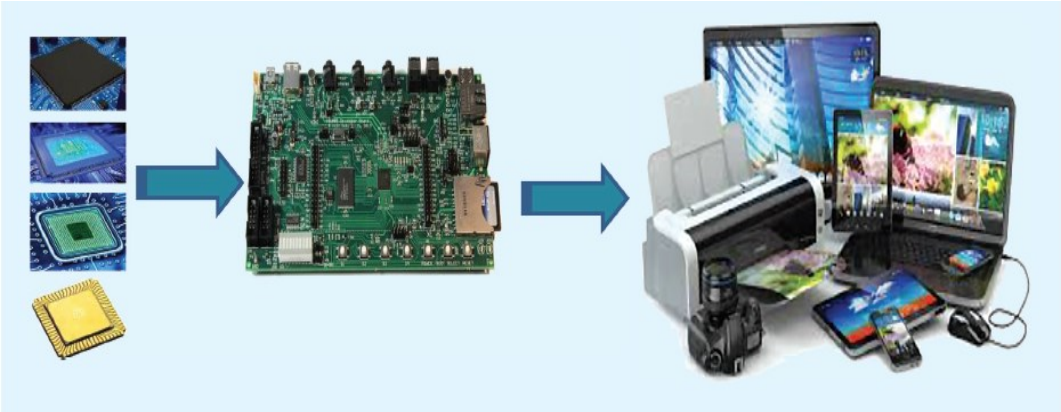
Prof. Anirban Sengupta, FIET, FBCS, FIETE, SMIEEE, P.Eng
Professor, CSE, Indian Institute of Technology Indore

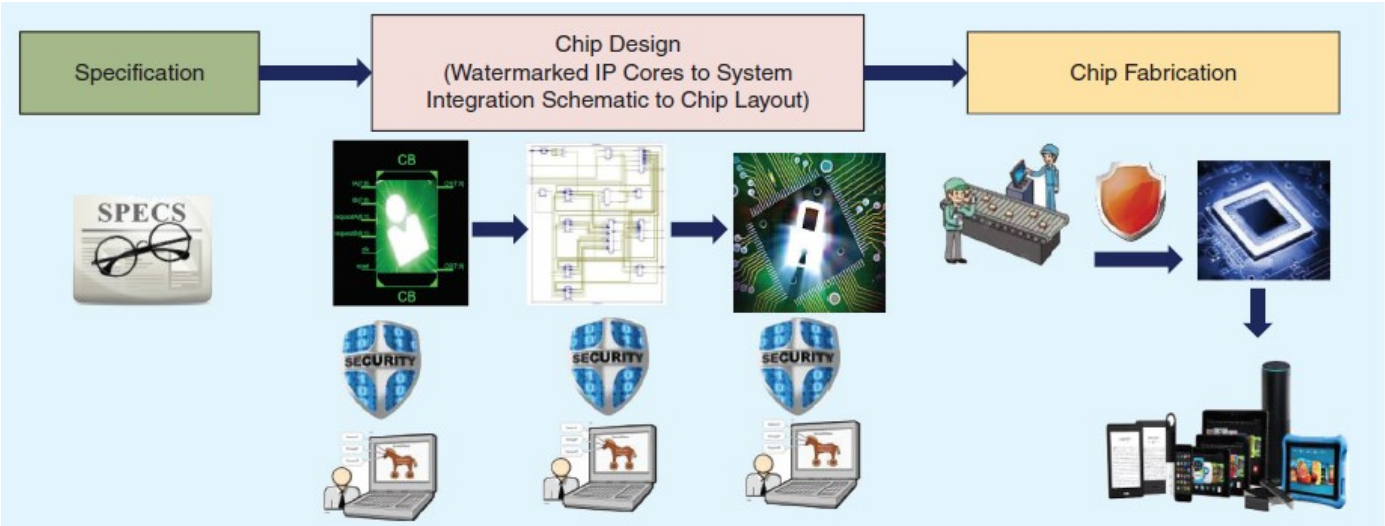
IEEE Distinguished Lecturer, IEEE Consumer Electronics Society
IEEE Distinguished Visitor, IEEE Computer Society
Editor-in-Chief, IET Computers and Digital Techniques
Associate Editor, IEEE Transactions on VLSI Systems
Associate Editor, IEEE Embedded Systems Letters
Associate Editor, IEEE Transactions on Consumer Electronics
Associate Editor, Nature Scientific Report
Former Chairman, IEEE-CS Technical Committee on VLSI
Founder & Former Chair, IEEE CTSoc Chapter – Bombay Section

IEEE COMPUTER SOCIETY

IEEE

CE System Vulnerabilities





Anirban Sengupta et. al "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", **The Institute of Engineering and Technology (IET)**, 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0

Introduction

- Hardware Security and Intellectual Property (IP) Core protection is an emerging area of research for semiconductor community that focusses on protecting designs against standard threats such as reverse engineering, counterfeit, forgery, malicious hardware modification etc.

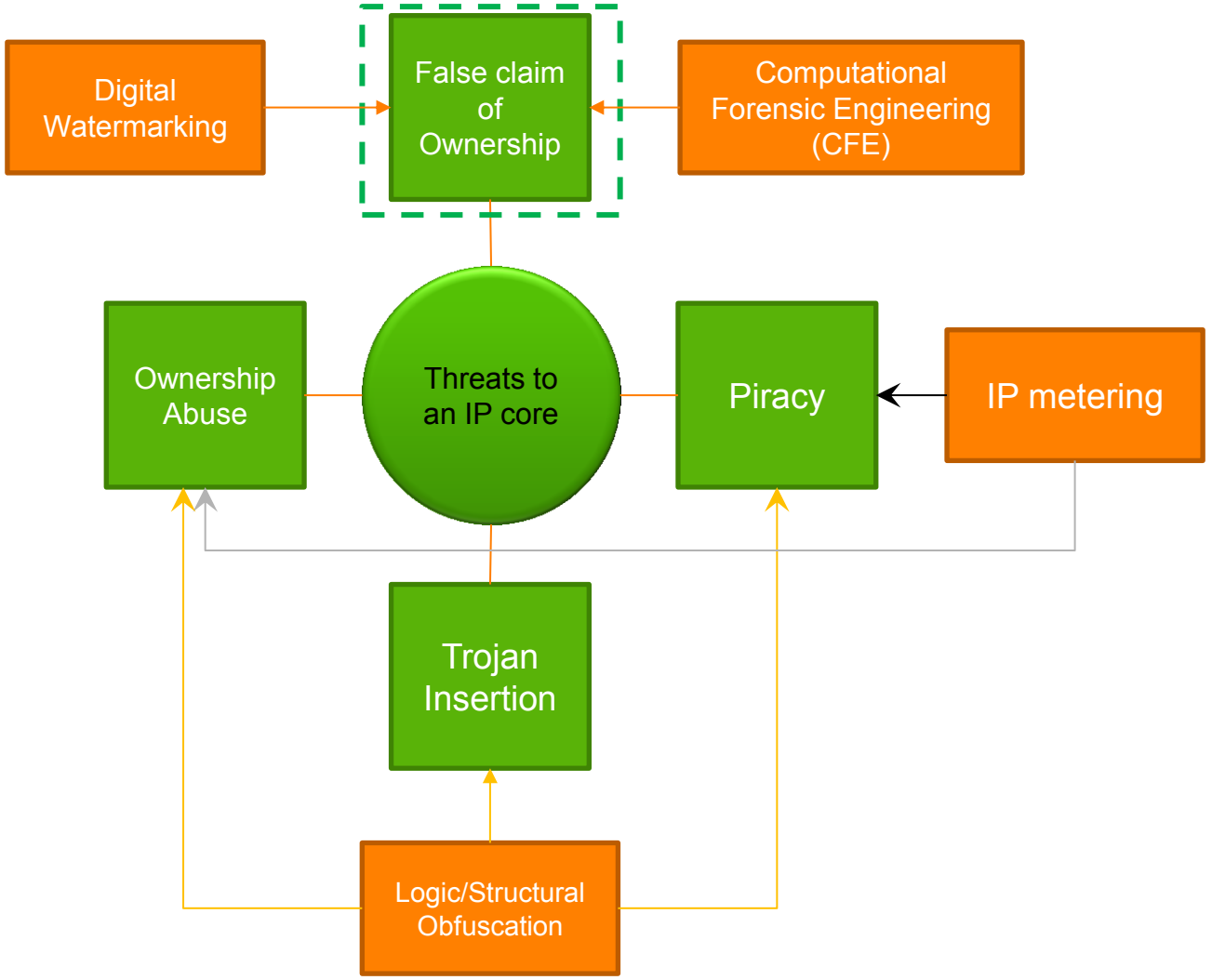
- Hardware security is broadly classified into two types: (a) authentication based approaches (b) obfuscation based approaches.
- The second type of hardware security approach i.e. obfuscation can again be further sub-divided into two types: (i) structural obfuscation (ii) functional obfuscation.
- Structural obfuscation transforms a design into one that is functionally equivalent to the original but is significantly more difficult to reverse engineer (RE), while the second one is active protection type that locks the design through a secret key.

Anirban Sengupta, Saraju P. Mohanty "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", **The Institute of Engineering and Technology (IET)**, 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0

Anirban Sengupta, Mahendra Rathor "Protecting DSP Kernels using Robust Hologram based Obfuscation", **IEEE Transactions on Consumer Electronics**, 2019

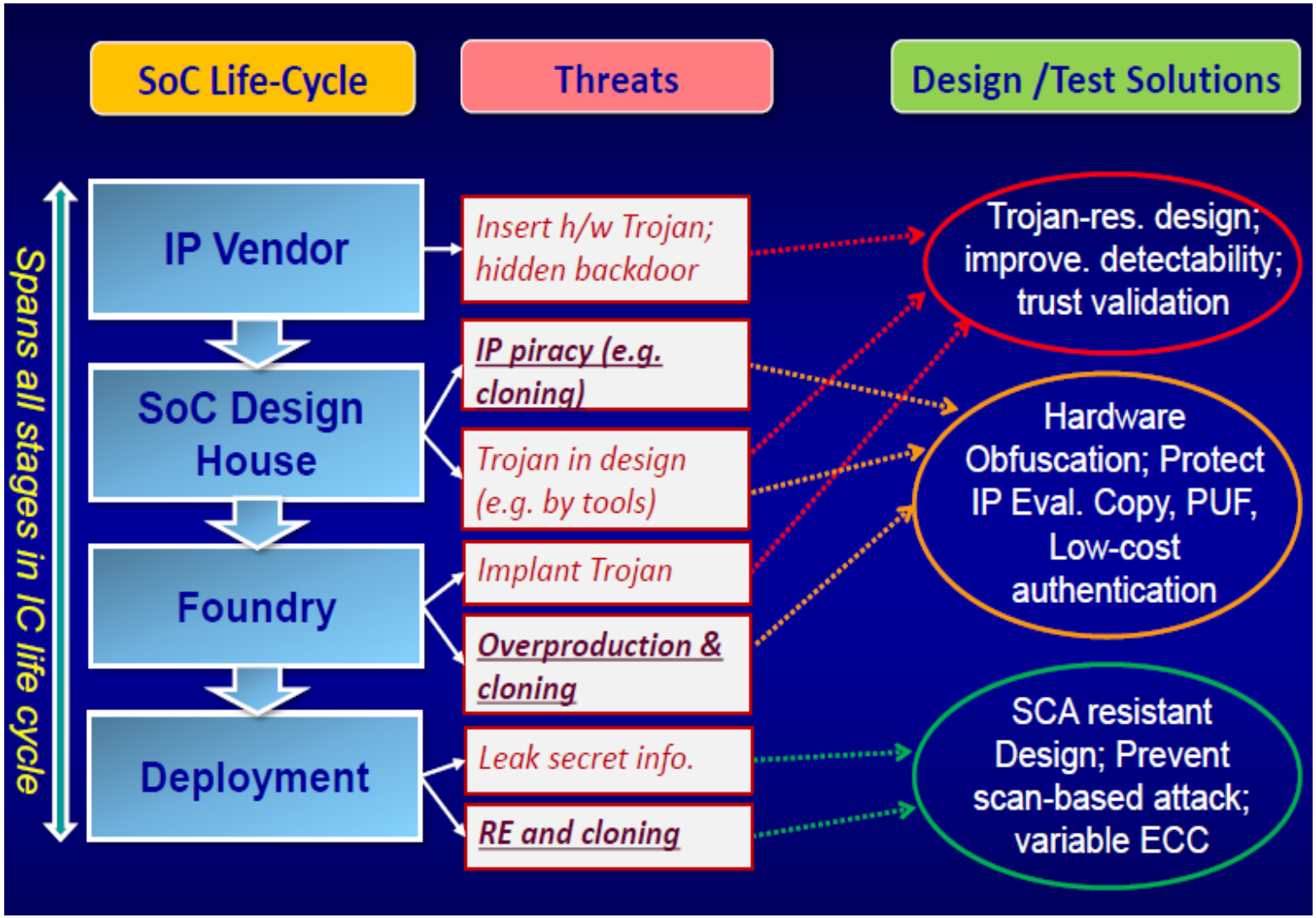
IEEE

Approaches for Hardware Security and IP Protection



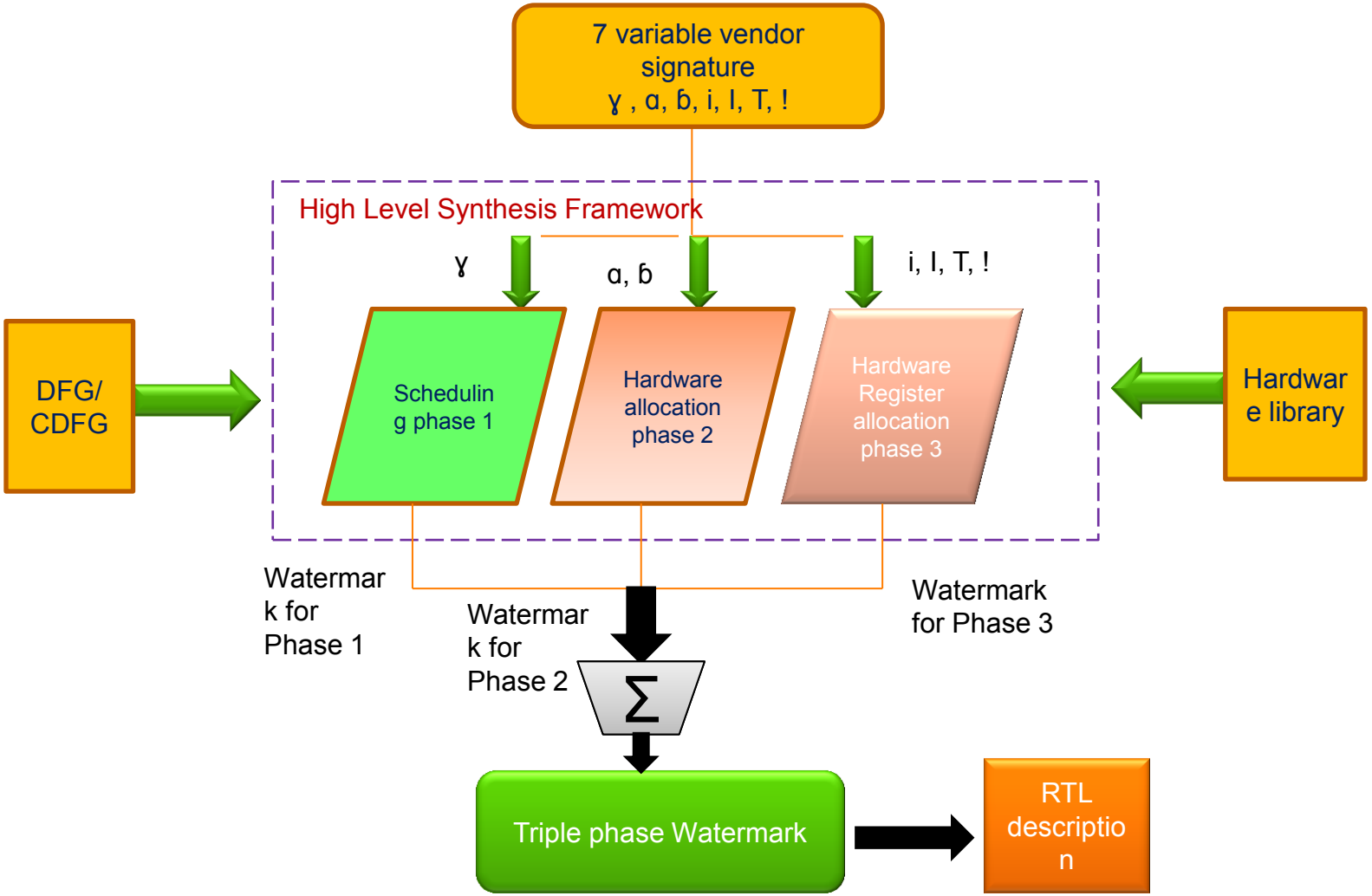
Anirban Sengupta, Dipanjan Roy, Saraju Mohanty, Peter Corcoran "DSP Design Protection in CE through Algorithmic Transformation Based Structural Obfuscation", **IEEE Transactions on Consumer Electronics**, Volume 63, Issue 4, November 2017, pp: 467 - 476

IP CORE Protection AND HARDWARE SECURITY



IEEE

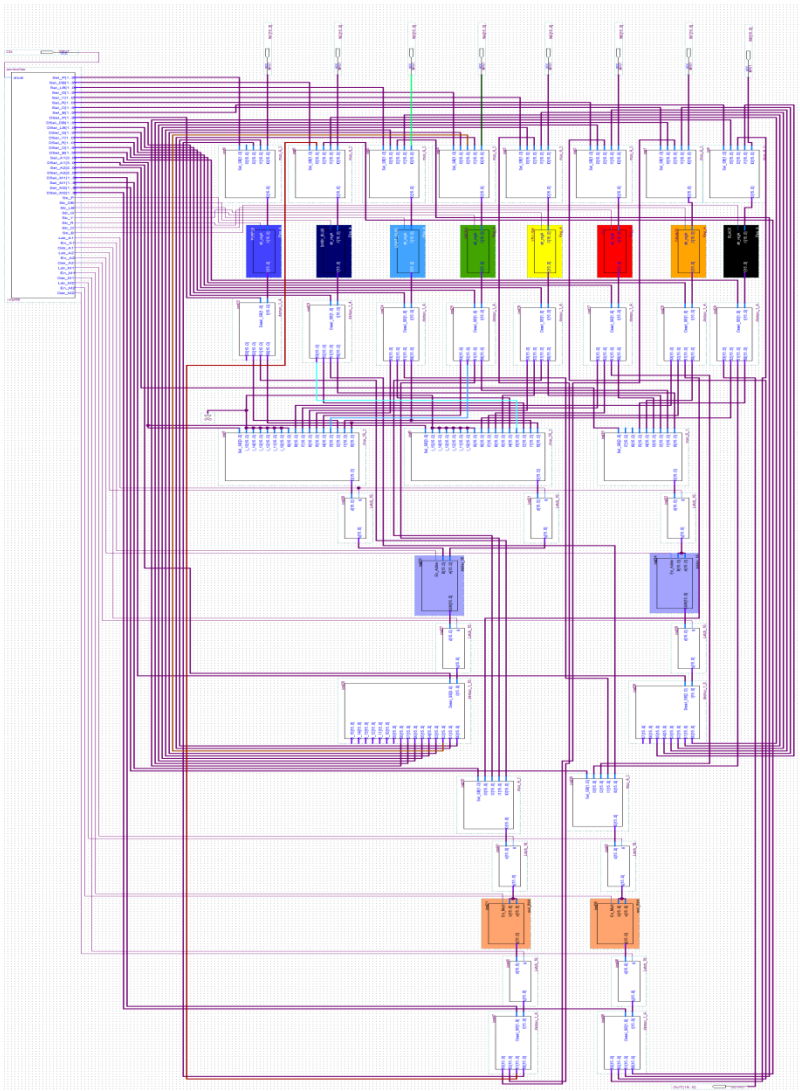
HLS based Triple phase watermarking

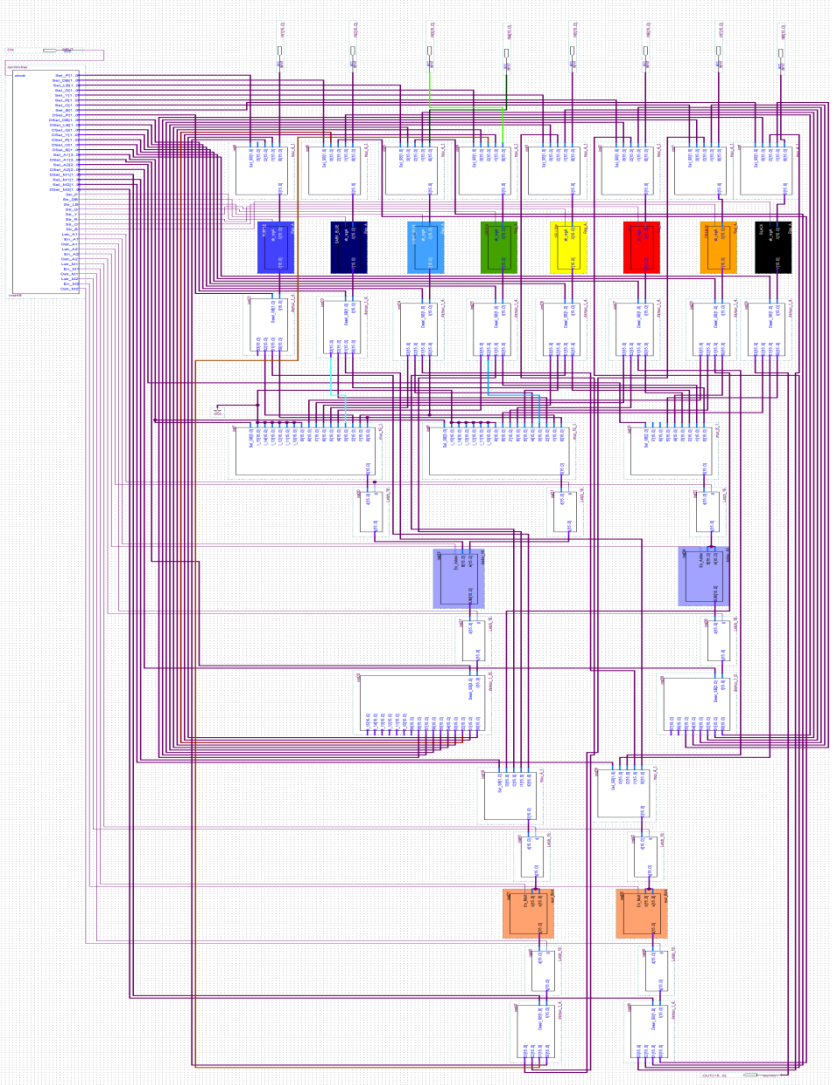


Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** Volume: 37, Issue: 4, April 2018, pp. 742 - 755

IEEE

Watermarked FIR Vs Non-Watermarked FIR at RTL

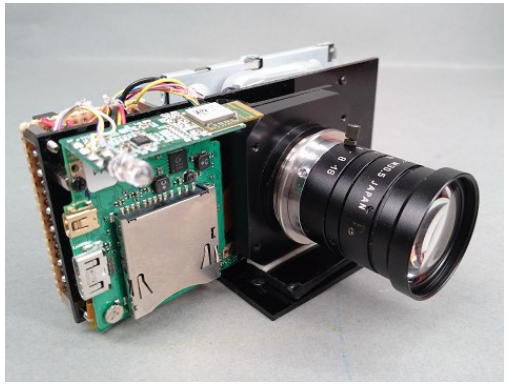


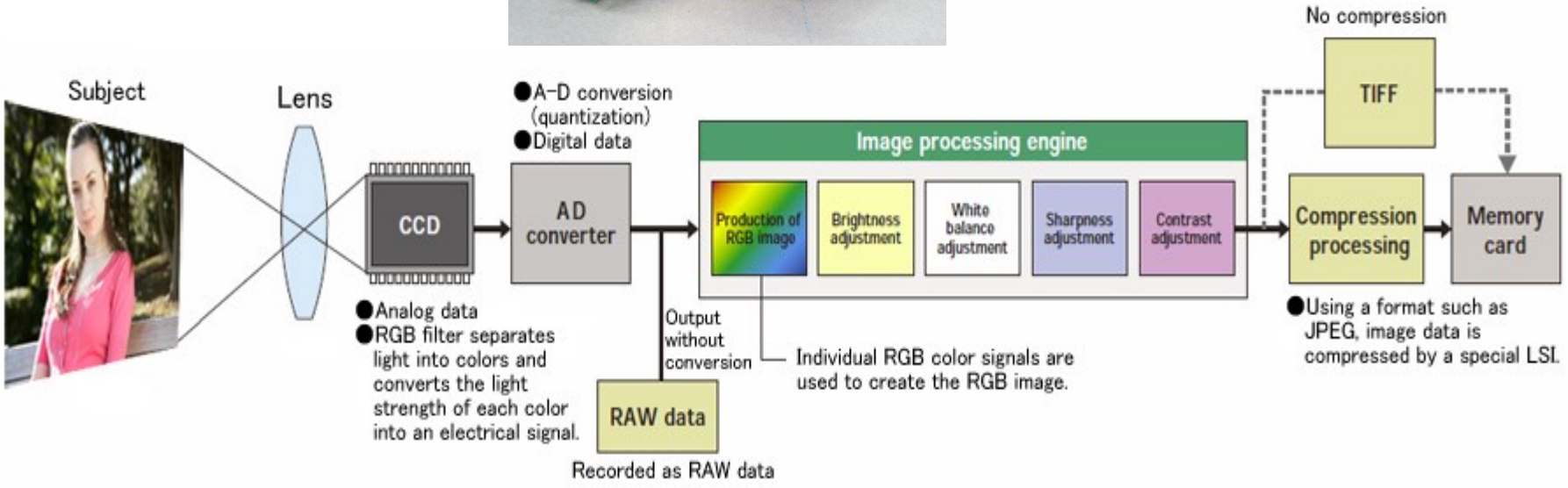


Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** Volume: 37, Issue: 4, April 2018, pp. 742 - 755

Example of CE Device : Digital Camera

- ✓ Simply converting an analog image that is captured by the CCD into digital data does not create a digital image.
- ✓ Only after the image processing engine and CODEC engine performs a variety of calculations on a huge amount of digital image data can we see a completed color/grayscale image.



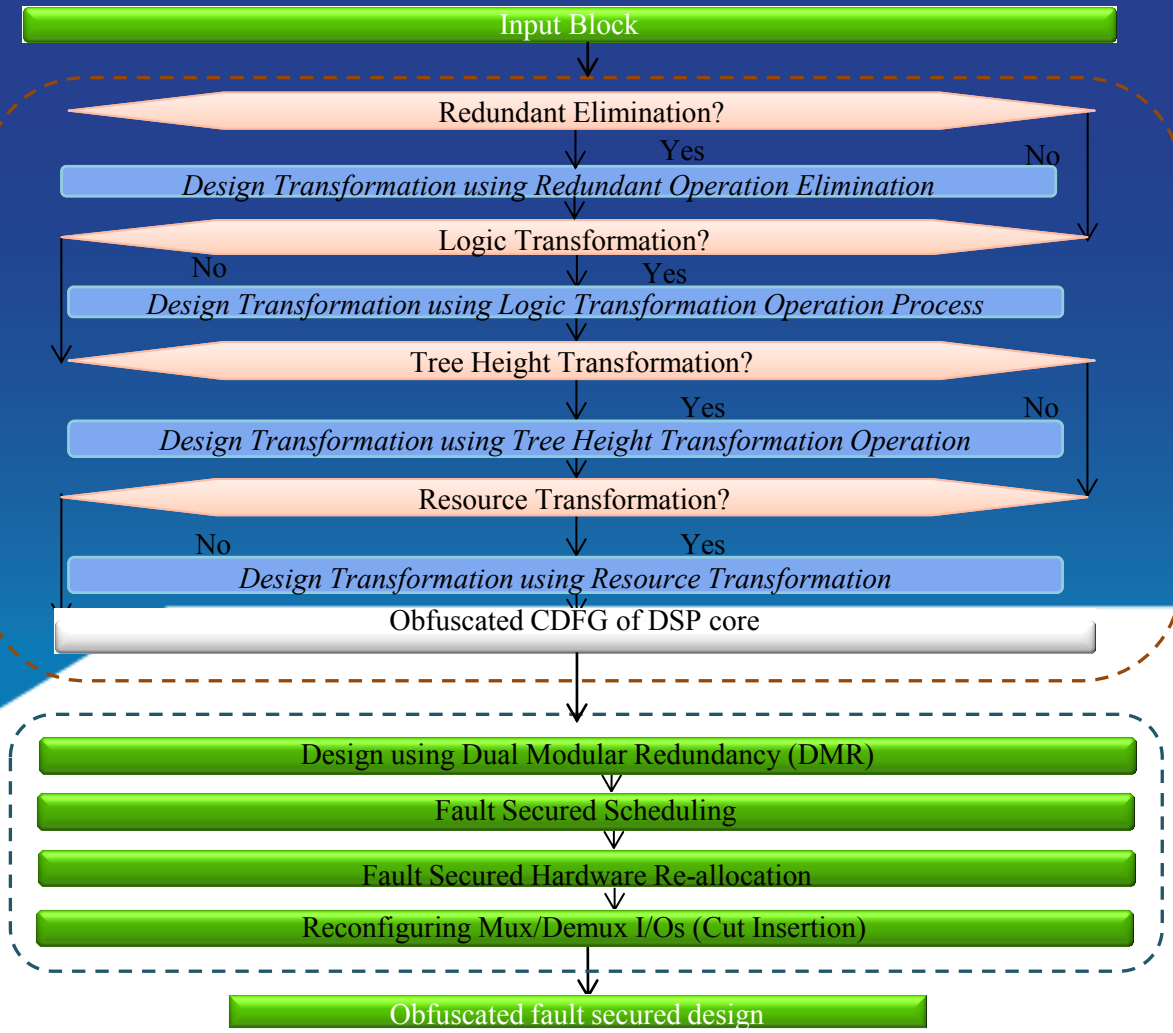


Complex JPEG codec

Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, Peter Corcoran "Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware", **IEEE Transactions on Consumer Electronics,** Volume: 64, Issue:3, August 2018, pp:365-374.

IEEE

Generic Design Flow of the Structural Obfuscation process

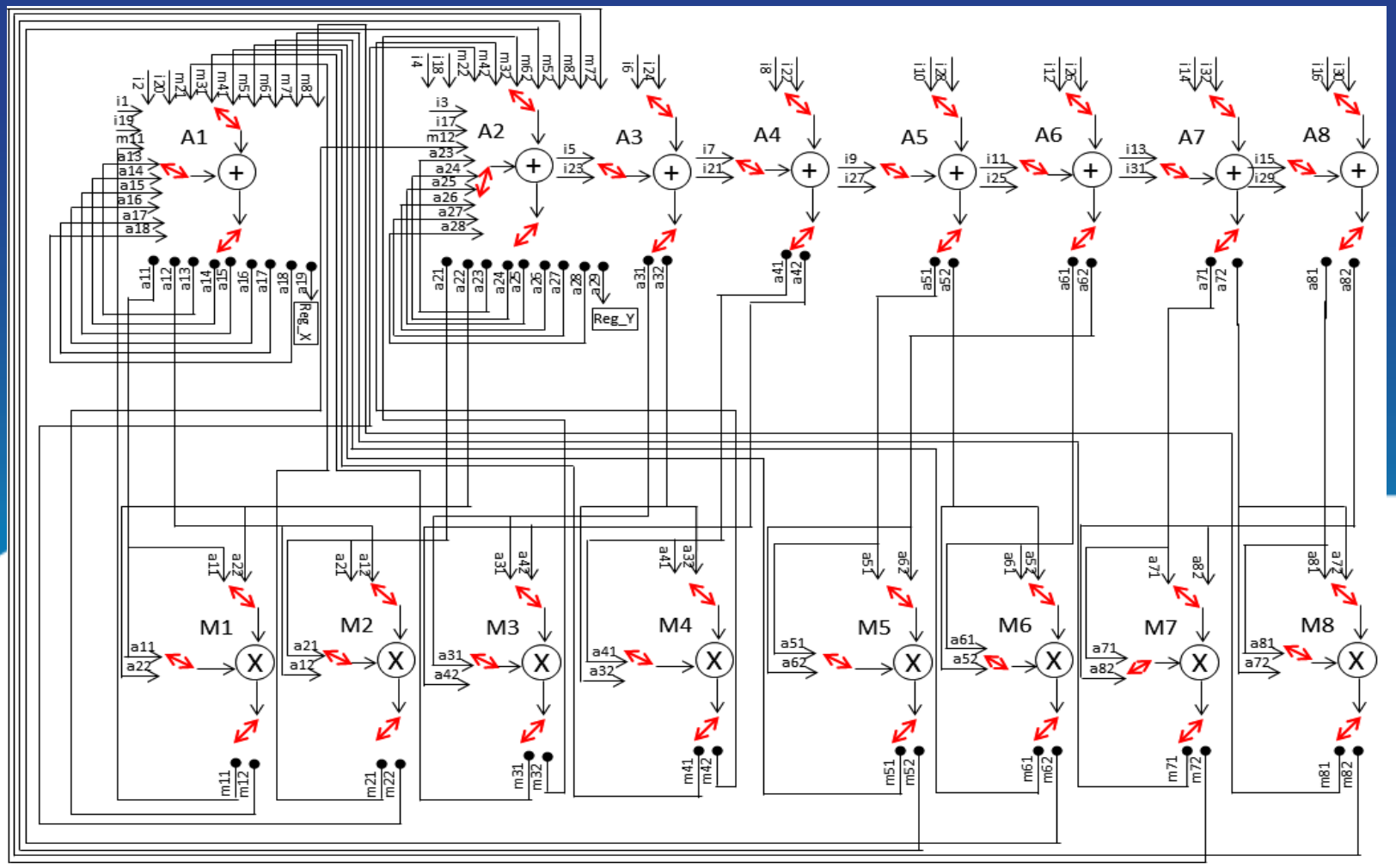


Obfuscation for fault Secured DSP Designs

IEEE

Anirban Sengupta, Saraju P Mohanty, Fernando Pescador, Peter Corcoran "Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature**", IEEE Transactions on Consumer Electronics**, Volume: 64, Issue:3, August 2018, pp: 356-364

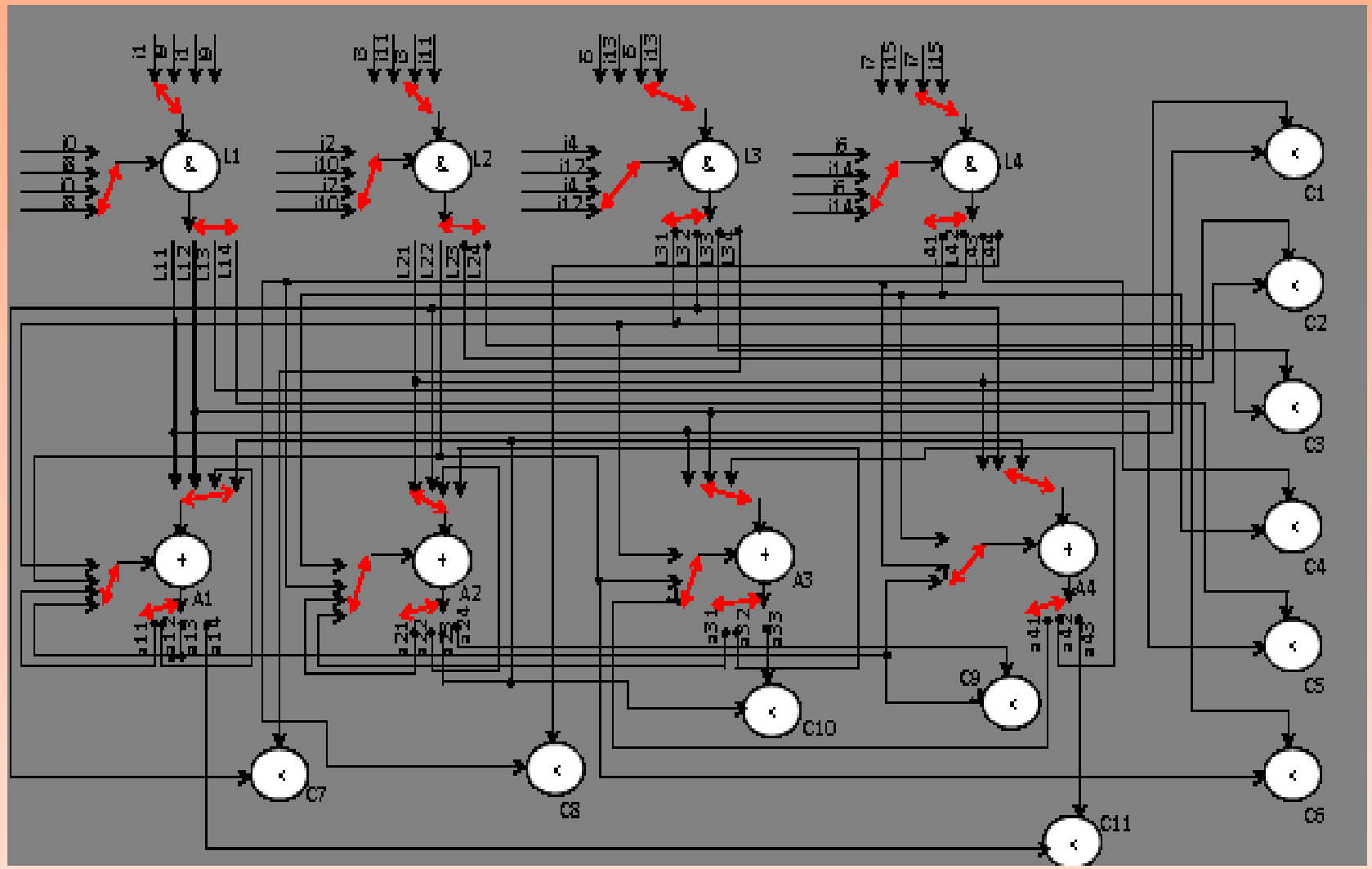
Non-obfuscated DSP circuit of a FIR filter with normal fault security



Anirban Sengupta, Saraju P Mohanty, Fernando Pescador, Peter Corcoran "Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature**", IEEE Transactions on Consumer Electronics**, Volume: 64, Issue:3, August 2018, pp: 356-364

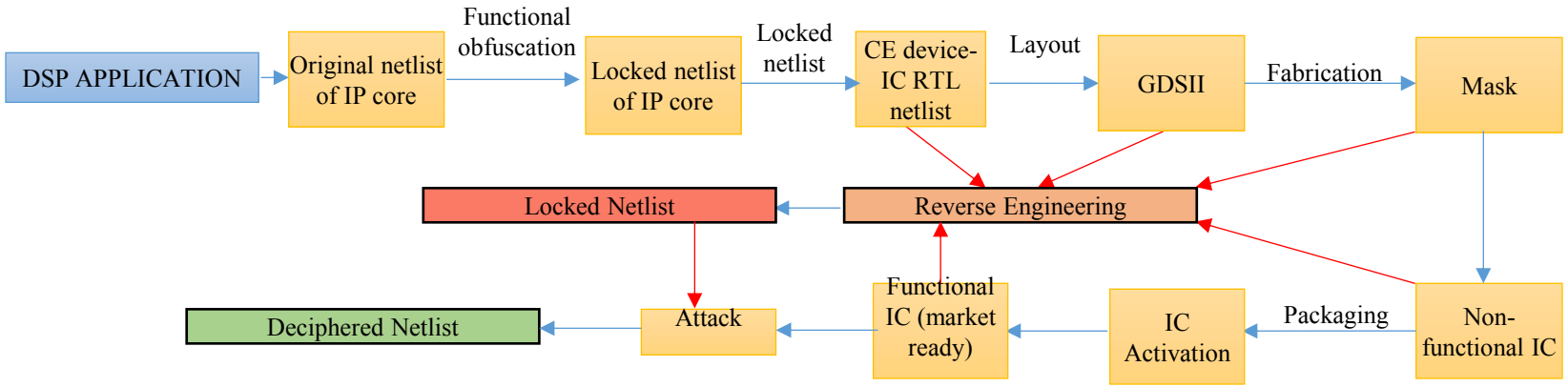
IEEE

Obfuscated Design of fault secured FIR filter



Anirban Sengupta, Saraju P Mohanty, Fernando Pescador, Peter Corcoran "Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature**", IEEE Transactions on Consumer Electronics**, Volume: 64, Issue:3, August 2018, pp: 356-364

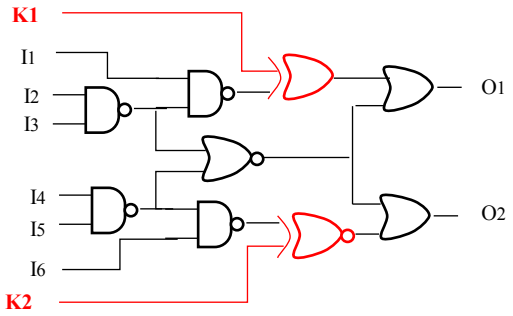
How Hardware of a CE device can be compromised ?



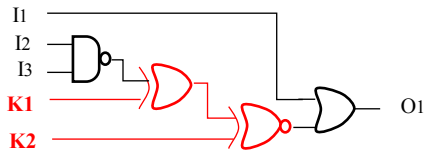
- Reverse engineering (RE) of a DSP core is a process of gaining the complete understanding of its **functionality**, **design** and **structure**.
- However, RE can be used for dishonest intention such as **overbuilding**, **piracy**, or **counterfeiting** a DSP core or inserting a **hardware Trojan**.

Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** 2019

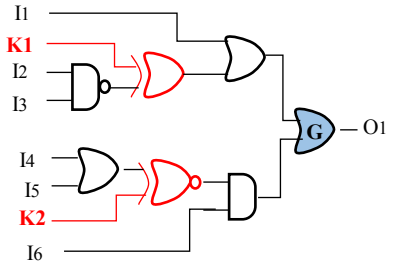
Possible Threat Scenarios



Isolated key gates K1 and K2



Run of key gates K1 and K2



Concurrently mutable key gates K1 and K2

1. **Sensitization attack:**

   a. **Isolated key-gates**: As there is no path between K1 and K2, they are isolated key-gates. An attacker can sensitize the value of K1 as 0 to the O1 by applying '100XXX' i/p pattern.

   b. **Run of key-gates**: If a set of key-gates are connected back-to-back. It increases the possible correct key combinations. Here, both '01' and '10' are correct key.

   c. **Concurrently mutable key-gates**: If two or more key-gates converges but have no common path between them. Here, applying I_6=0 will mute K2, then K1 can be sensitize at O1.

Functional Obfuscation

- Functional obfuscation using **logic locking** is a technique that inserts locking units in the design such that the design cannot generate correct functionality until a **valid key** is applied to the locked circuit.
- These locking units accept **key bits** as **input** and based on these key value it produces the **output** of the **design**.
- Applying **correct key** produces **correct result** while applying **wrong keys** led to exhibit an **incorrect functionality** of the design.
- Thus functional obfuscation **thwarts RE** process for **fraudulent intentions**.

Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** 2019

Features of ILBs

- **Multi-pairwise security:** Any key bit of the ILBs cannot be sensitized to the o/p, without applying/controlling all of the remaining 7 key inputs. Thus, multi-pairwise security ensures protection against key-sensitization based attack.

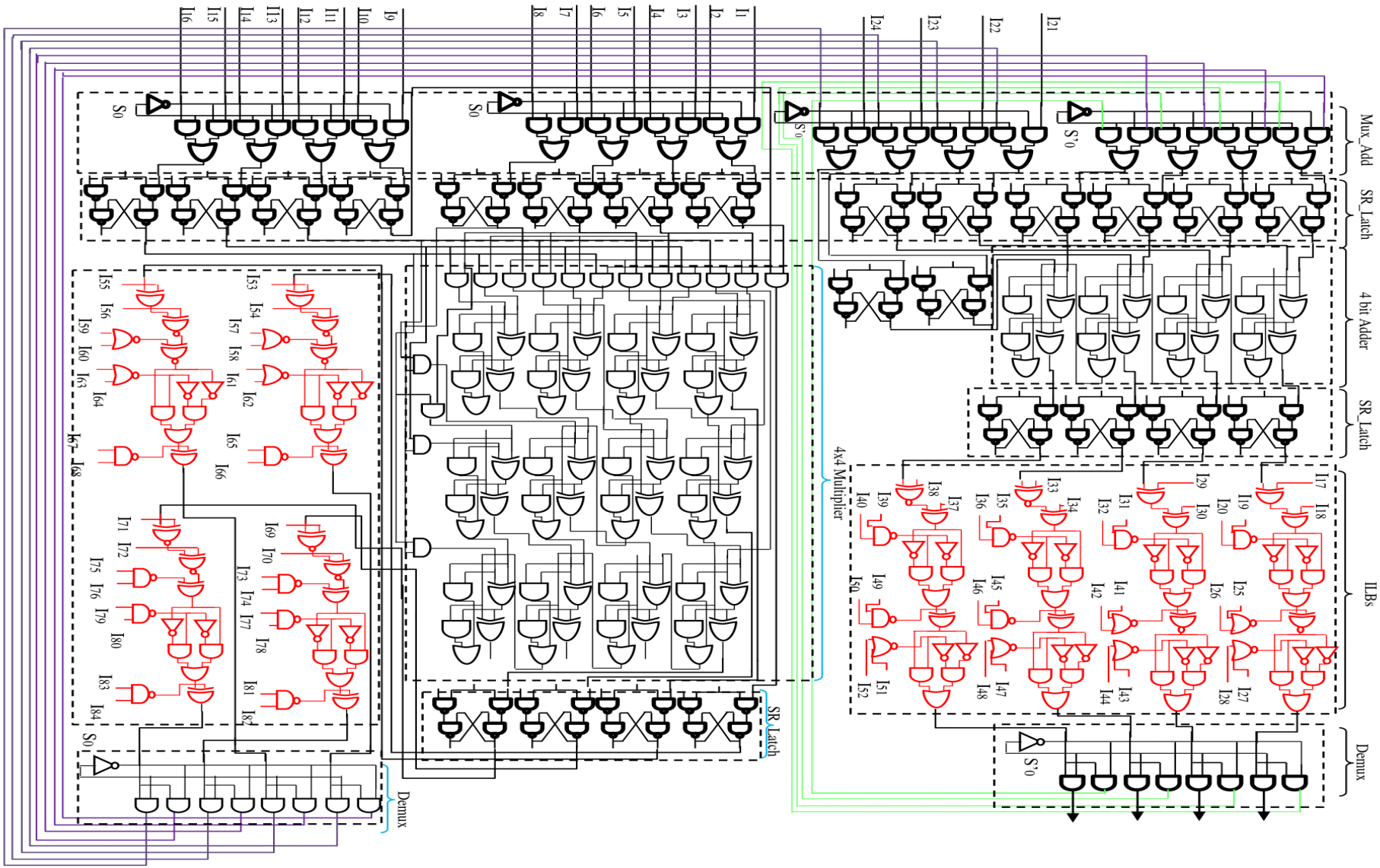
- **Prohibiting key gate isolation:** Proposed ILBs are a combination of multiple key gates dependent on each other thus ensuring no-isolation among key inputs. Hence, impedes an attacker's attempt to sensitize key without knowing/controlling key-bits.

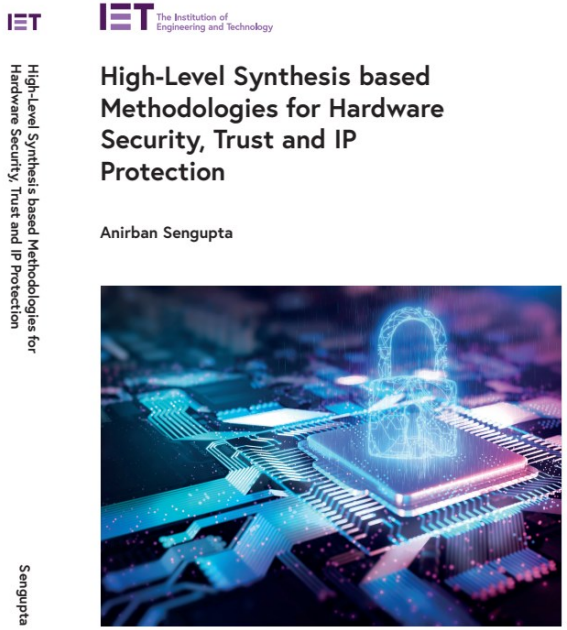
Cont...

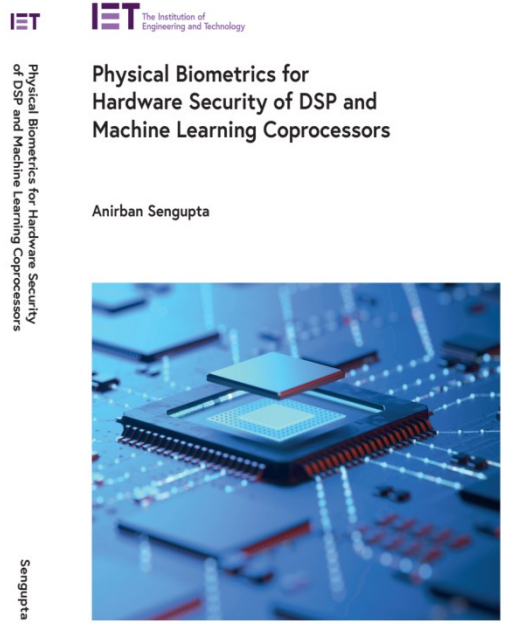
- **Ensuring protection against run of key-gates:** In the proposed ILB structure key gates are connected in a composite fashion (with intertwining among gate structures for 8 key i/ps). Therefore, replacing run of key-gates with a single key-gate is difficult.

- **Non-mutable key gates:** The proposed ILB encode 8 key gates per data output bit thus it is infeasible to mute the remaining 7 keys to sensitize a specific key by controlling one single input. Thus, proposed ILBs are secured from Convergent key-gates based attack.

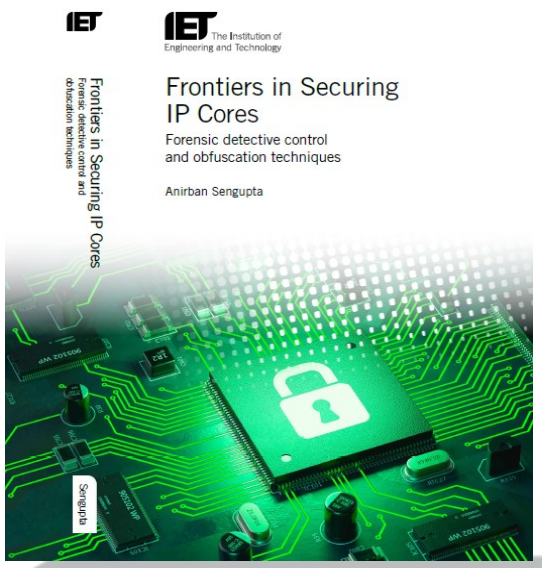
Obfuscated gate structure of FIR Filter



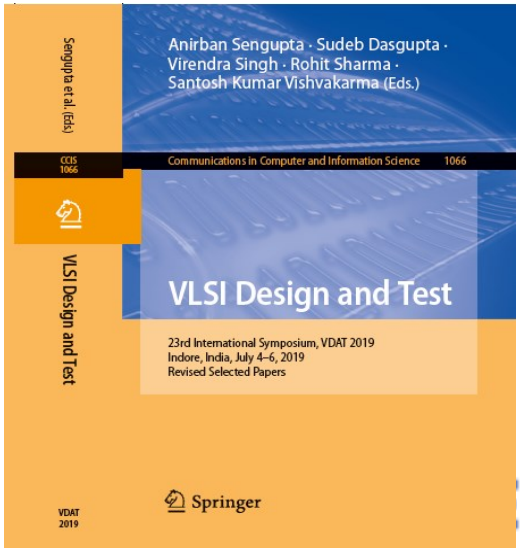

IET
High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection
Sengupta
IET The Institution of Engineering and Technology
High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection
Anirban Sengupta


IET
Physical Biometrics for Hardware Security of DSP and Machine Learning Coprocessors
Sengupta
IET The Institution of Engineering and Technology
Physical Biometrics for Hardware Security of DSP and Machine Learning Coprocessors
Anirban Sengupta


IET
Secured Hardware Accelerators for DSP and Image Processing Applications
Sengupta
IET The Institution of Engineering and Technology
Secured Hardware Accelerators for DSP and Image Processing Applications
Anirban Sengupta


IET
Frontiers in Securing IP Cores
Forensic detective control and obfuscation techniques
Sengupta
IET The Institution of Engineering and Technology
Frontiers in Securing IP Cores
Forensic detective control and obfuscation techniques
Anirban Sengupta


IET
IP Core Protection and Hardware-Assisted Security for Consumer Electronics
Sengupta and Mohanty
IET The Institution of Engineering and Technology
IP Core Protection and Hardware-Assisted Security for Consumer Electronics
Anirban Sengupta and Saraju P. Mohanty
USER SAFE


Sengupta et al. (Eds.)
CCIS 1066
VLSI Design and Test
VDAT 2019
Anirban Sengupta · Sudeb Dasgupta · Virendra Singh · Rohit Sharma · Santosh Kumar Vishvakarma (Eds.)
Communications in Computer and Information Science 1066
VLSI Design and Test
23rd International Symposium, VDAT 2019
Indore, India, July 4–6, 2019
Revised Selected Papers
Springer

References

- Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9
- Anirban Sengupta, Mahendra Rathor "Protecting DSP Kernels using Robust Hologram based Obfuscation", IEEE Transactions on Consumer Electronics, Volume: 65, Issue: 1, Feb 2019, pp. 99-108
- Anirban Sengupta, Saraju P. Mohanty "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", The Institute of Engineering and Technology (IET), 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0
- Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 37, Issue: 4, April 2018, pp. 742 – 755
- Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 38, Issue 4, April 2019, pp. 604 – 616
- Anirban Sengupta, Saraju P Mohanty, Fernando Pescador, Peter Corcoran "Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature", IEEE Transactions on Consumer Electronics, Volume: 64, Issue:3, August 2018, pp: 356-364
- Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, Peter Corcoran "Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware", **IEEE Transactions on Consumer Electronics,** Volume: 64, Issue:3, August 2018, pp:365-374.

Conclusion

The future of electronics system design is Energy-Security Tradeoff !

Thank You