IEEE computer society

IEEE

Paradigms for Hardware Security of CE Systems

CyVIT: The Annual Cyber Security Conclave 2019

April 5,2019

Dr. Anirban Sengupta, FIET, FBCS (UK), SMIEEE, P.Eng
Associate Professor, CSE
INDIAN INSTITUTE OF TECHNOLOGY INDORE
IEEE Distinguished Lecturer, IEEE Consumer Electronics Society
IEEE Distinguished Speaker, IEEE Computer Society
Chairman, IEEE Technical Committee on VLSI
Founder & Chairman, IEEE CESoc Chapter – Bombay Section

IEEE COMPUTER SOCIETY

IEEE

Who We Are

- The IEEE Computer is the world's home for computer science, engineering, and technology. Known as the organization that empowers the people who drive technology, the IEEE Computer Society brings forward-thinking technology professionals together to discover the next technological innovation, develop international standards, form communities, and share knowledge.

Our Vision:

To be the leading provider of technical information, community services, and personalized services to the world's computing professionals.

IEEE

IEEE Computer Society Today

Global Reach

60,000+
Members

480
Chapters

168
Countries

Technical Breadth

200
Conferences

600,000+
Trusted Technical
Documents

30+
Top-cited
Periodicals

121+
Active
Standards

Trusted, Reliable Information

Publications

IEEE Computer Society produces a wide range of quality publications that make the exchange of technical knowledge and information possible allowing members to stay current on the latest technology breakthroughs with IEEE Computer Society publications.

IEEE Computer Society Magazines – 13 of the top cited magazines in computer science, computer engineering

IEEE Computer Society Transactions – 19 peer reviewed journals publishing cutting edge research, and breakthrough discoveries.

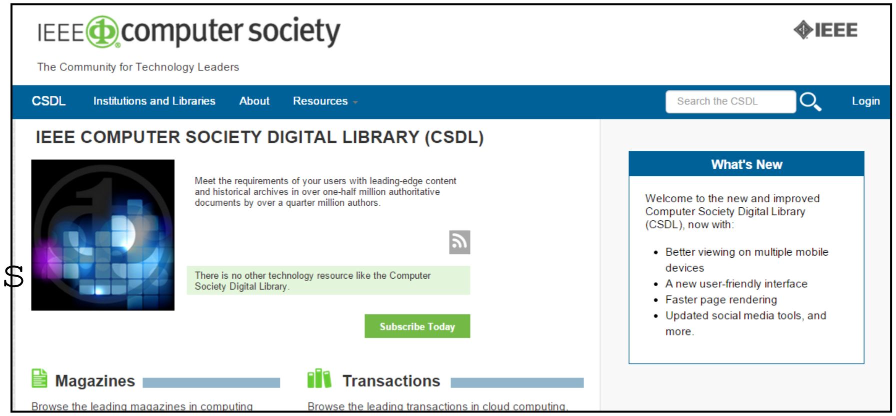
IEEE Computer Society Conference Proceedings – Cutting edge papers presented at conferences globally.

IEEE

IEEE Computer Society Digital Library

The IEEE Computer Society Digital Library is your gateway to the most trusted research – magazines, transactions, conference proceedings – to help you build from previous research and inspire new ideas.

- Powerful search
- User-friendly interface
- 13 magazines
- 19 transactions
- 5,200 conference publications
- 600,000 technical papers and articles



Included with student membership. Others pay an additional US $130 for

IEEE COMPUTER SOCIETY
CONFERENCE & EVENT SERVICES

Sponsor

- More than 200 technical conferences per year
- Cutting-edge research topics
- Peer reviewed
- Backed by technical committees

Publisher

- 300+ conference titles per year
- Print, digital, online media
- Posting to digital libraries
- Commercial indexing
- Peer review
- Now available: Mobile app and ebook options

Hacking Network on Wheels

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

BMW, Audi and Toyota cars can be unlocked and started with hacked radios

share

The affected cars include BMW's 730d, as well as models from Audi, Honda, Ford and Toyota. CREDIT: RICHARD NEWTON

Researchers Show How to Steal Tesla Car by Hacking into Owner's Smartphone

Friday, November 25, 2016 Mohit Kumar

G+1 55 Like 2K Share 681 Tweet 259 in Share 98 Share 1071

Key fobs contain a short-range radio transmitter, and must be within a certain range, usually 5–20 meters, of the car to work. When a button is pushed, it sends a coded signal through radio waves to a receiver unit in the car, which locks or unlocks the door.

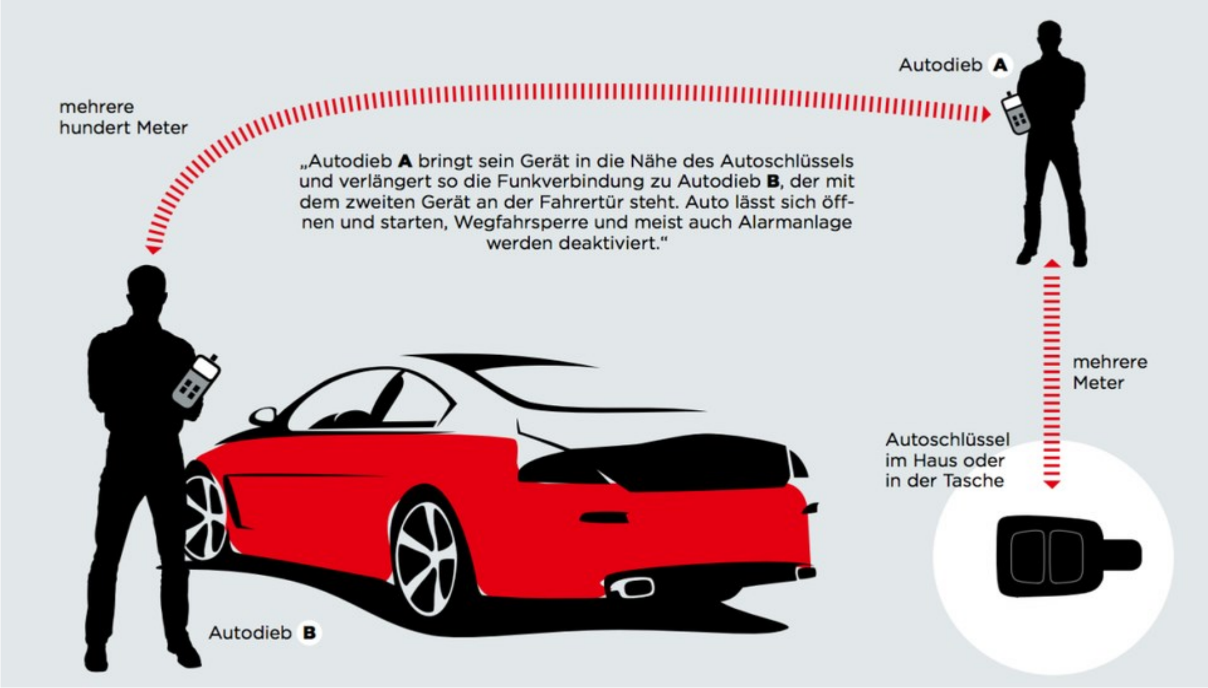
IEEE

Acknowledgement: Dr. Sandip Ray, UFL, USA

Hacking Network on Wheels

- ✓ The attack involves two hackers, whose radios collect the signals sent between the fob and the car to unlock doors and start engines.

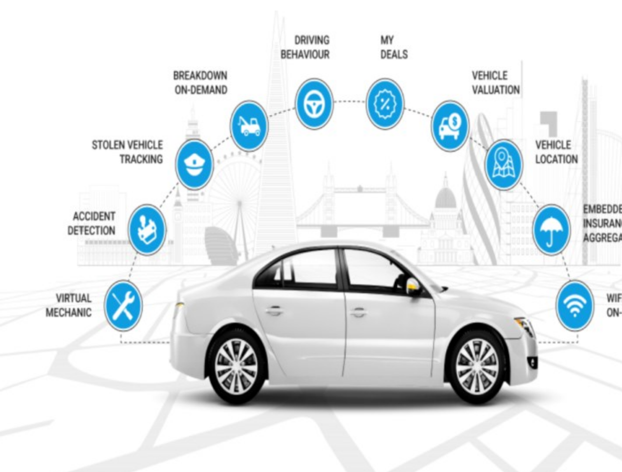
- ✓ One hacker carries a radio that collects signals from a target vehicle's fob. This is then passed to an co-conspirator, as far away as several hundred meters, who uses it to open the doors and start the engine.



Key fobs contain a short-range radio transmitter, and must be within a certain range, usually 5–20 meters, of the car to work. When a button is pushed, it sends a coded signal **with time stamp** using **PRNG/HRNG** through radio waves to a receiver unit in the car, which locks or unlocks the door. The time stamp expires after immediate use. Thus blocking replay attacks.

IEEE

Vulnerability through Connectivity



Beckstrom's Laws of Cybersecurity

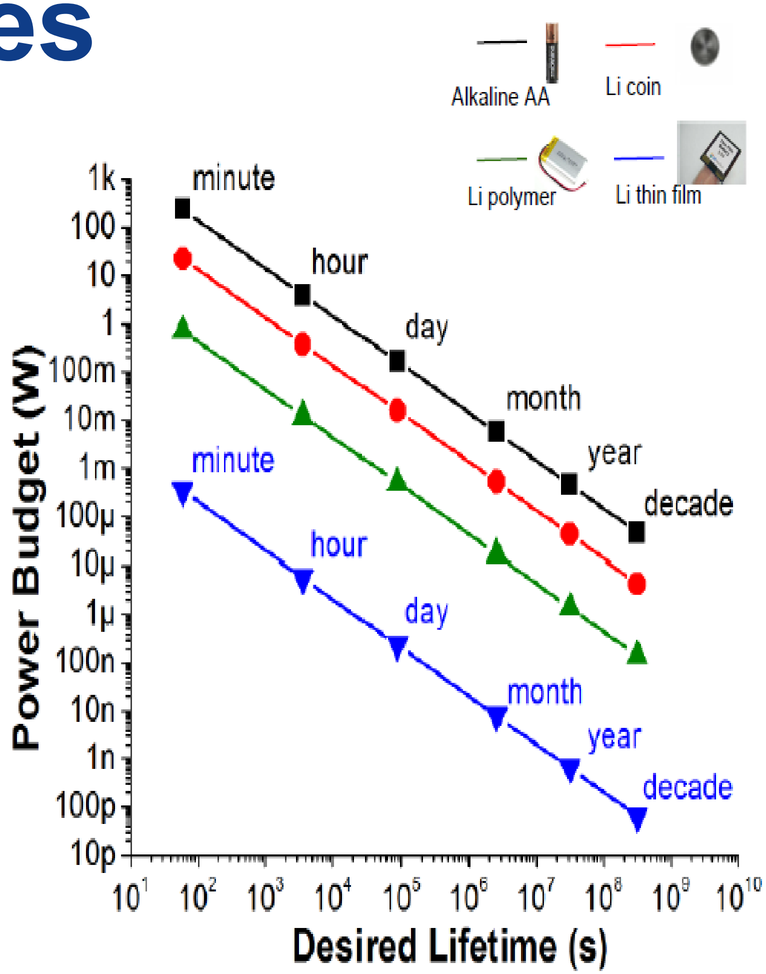
- Anything attached to a network can be hacked
- Everything is being attached to networks
- Everything can be hacked

Rod Beckstrom, CEO and President of ICANN, former Director of the National Cyber Security Center

Acknowledgement : Dr. Sandip Ray, UFL, USA

IoT Device Features

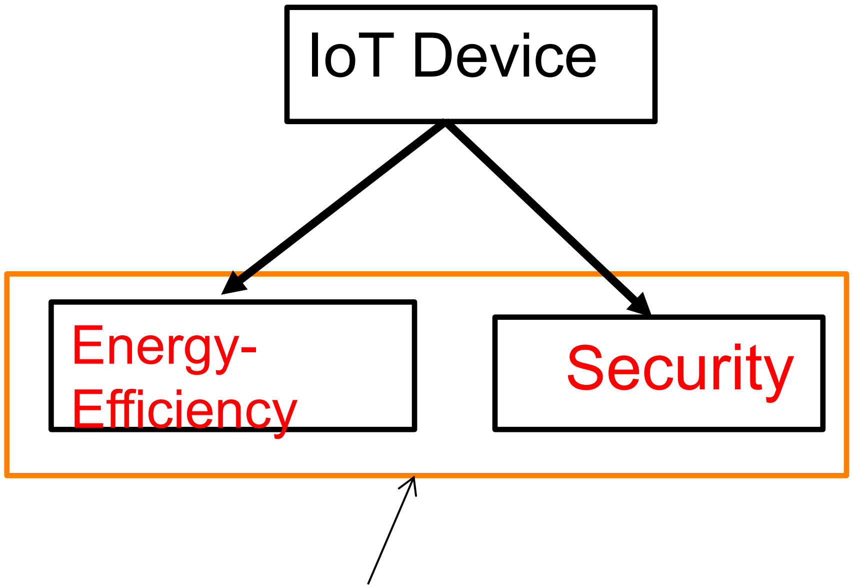
- Typically battery operated
- Small in size
- Transmit data through Wireless Sensor Nodes
  - Uses crypto algorithm for secure communication
  - Lightweight cryptography



Battery life time Vs power consumption

Acknowledgement : Dr. Himanshu Thapliyal, U Kentucky, USA

Challenges in Embedded and IoT Devices



Design Challenges in IoT devices

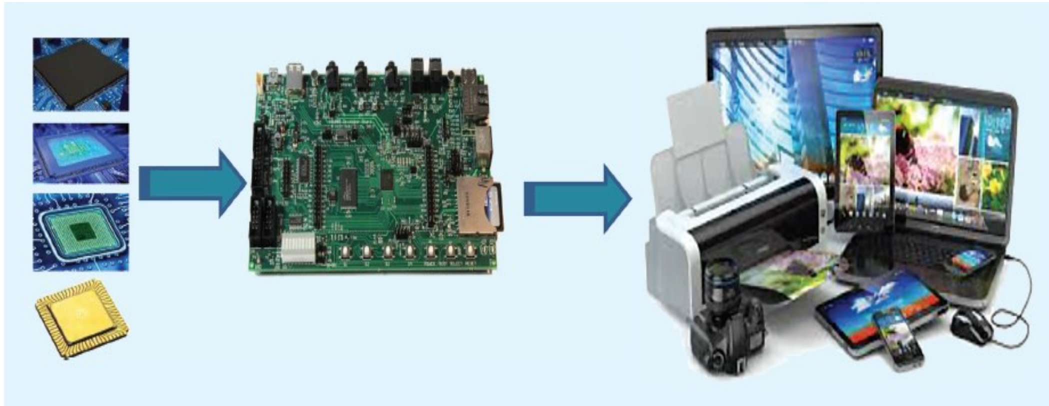
- Typically battery operated
  - Energy-efficient design
- Vulnerable to hardware/malware attacks
  - Power analysis attacks
  - IC piracy, IC counterfeiting, Hardware trojan

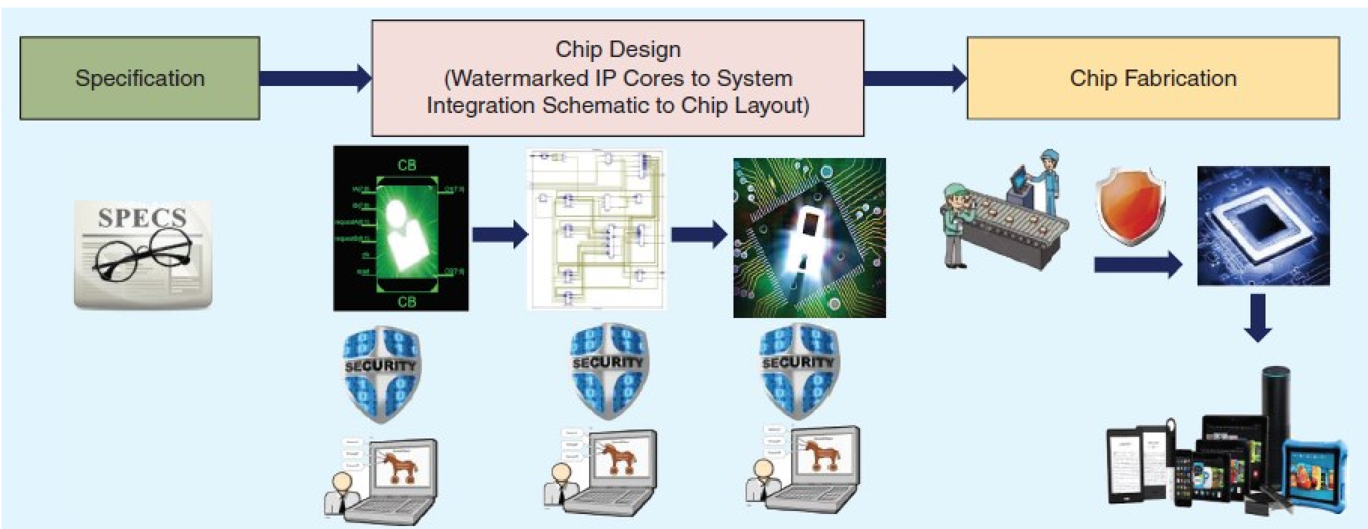
Cyberattacks are threat to reliability, safety, consumer's personal information and piracy or cloning of intellectual property (IP) core.

IEEE

Acknowledgement : Dr. Himanshu Thapliyal, U Kentucky, USA

CE Device 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

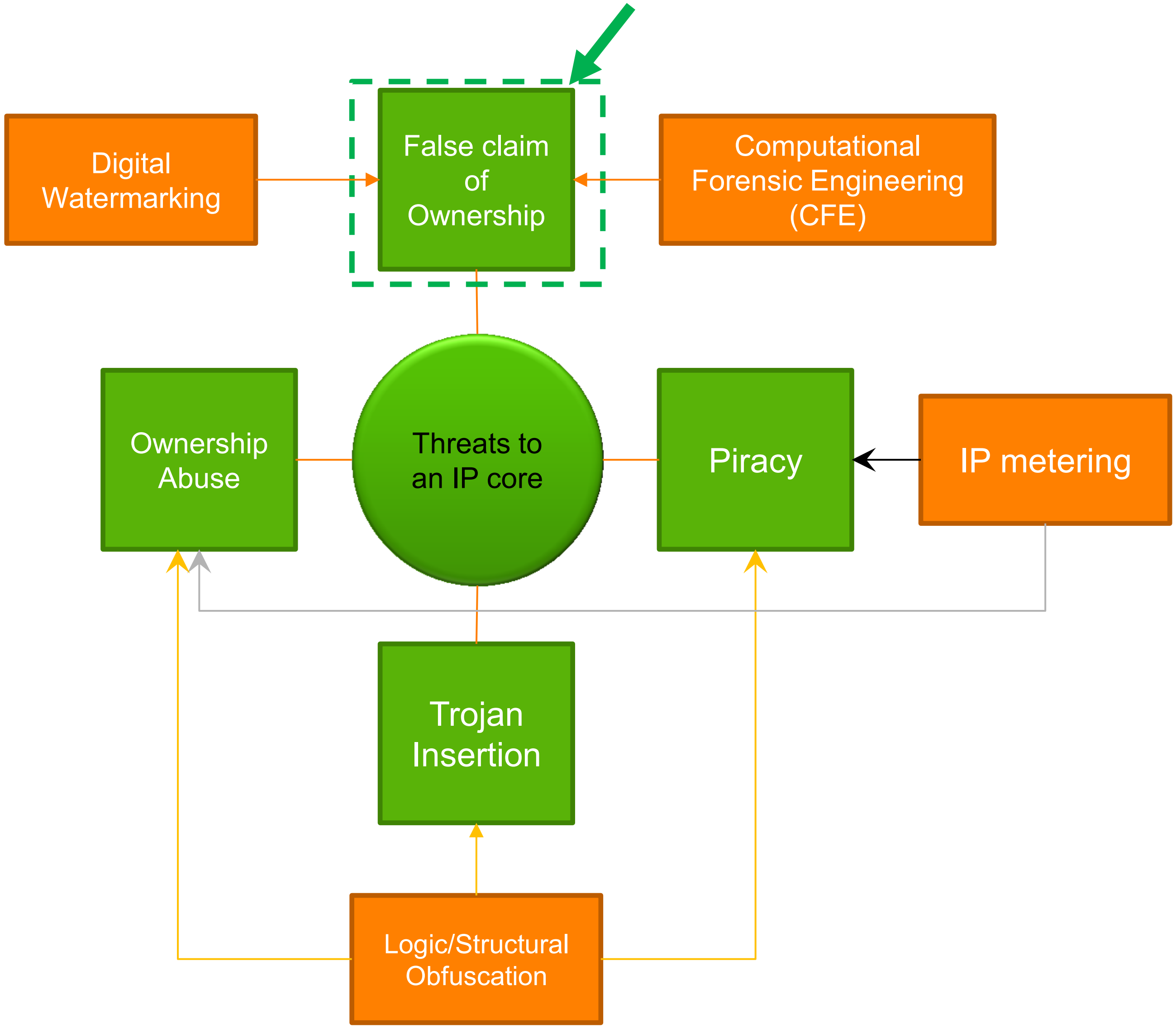
- Hardware Security and Intellectual Property (IP) Core protection is an emerging area of research for semiconductor community that focusses on protecting designs against standard threats such as reverse engineering, counterfeit, forgery, malicious hardware modification etc.
- Hardware security is broadly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

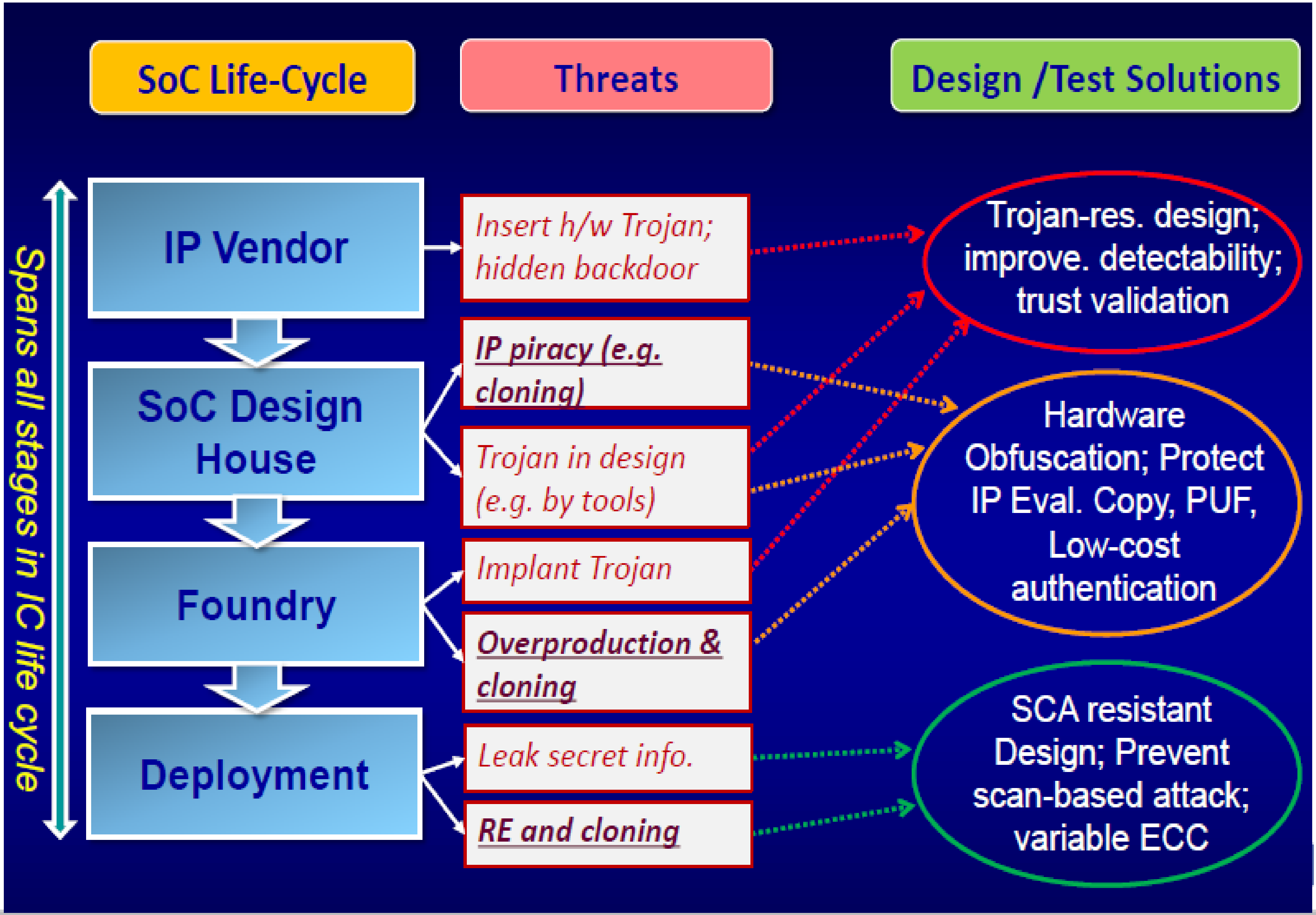
IEEE

Approaches for 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

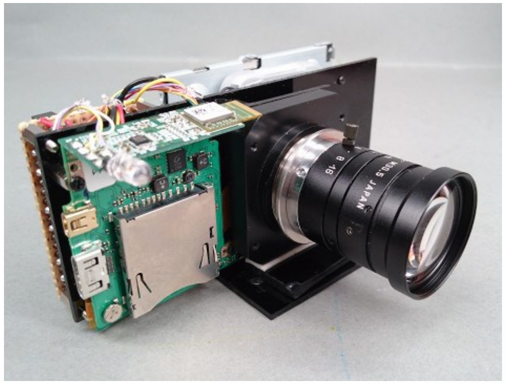
IP CORE Protection AND HARDWARE SECURITY

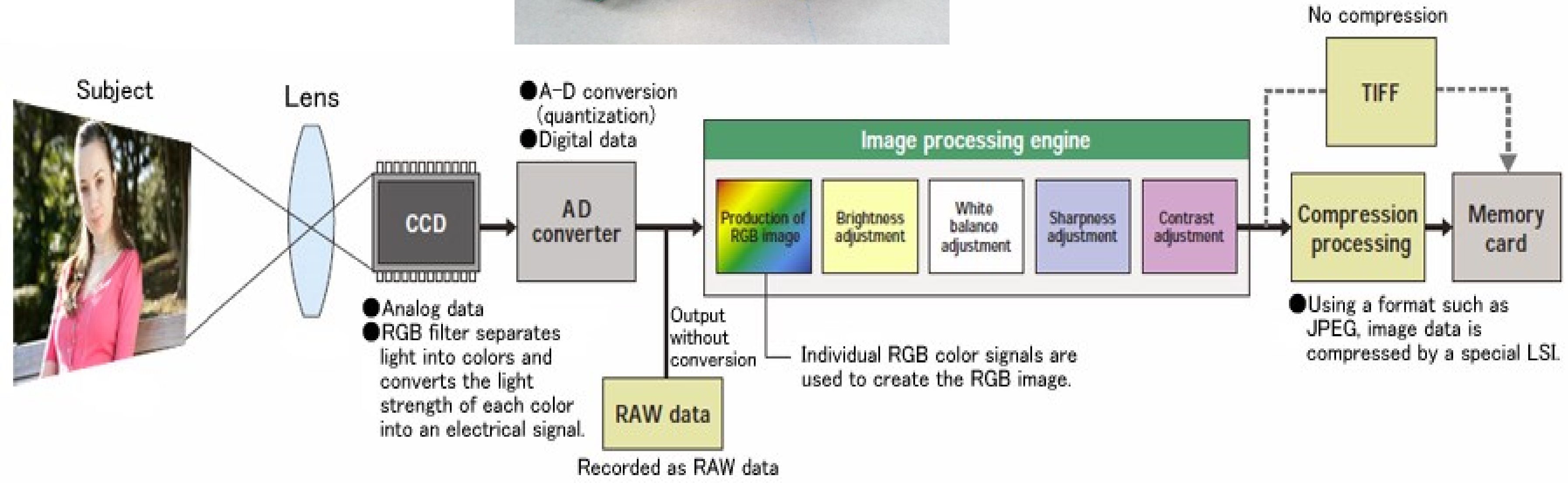


IEEE

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.

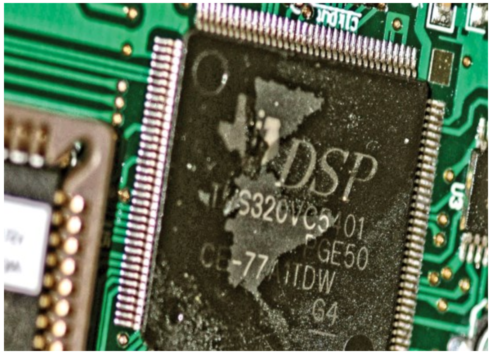




IEEE

Example of DSP Core in Digital Camera

- ✓ But when you're recording video, if the videos are not processed fast, then you start missing frames.
- ✓ This is why digital video cameras almost always have a second microprocessor built-in, dedicated to video calculations. This is a Digital Signal Processor or DSP — the job of which is to perform repetitive mathematical tasks in real time.
- ✓ So, while your iphone's main microprocessor is checking to see if you have an incoming call, running your email in the background and managing your Wi-Fi signal, when video is coming through the lens, those calculations are handed off to a second microprocessor.

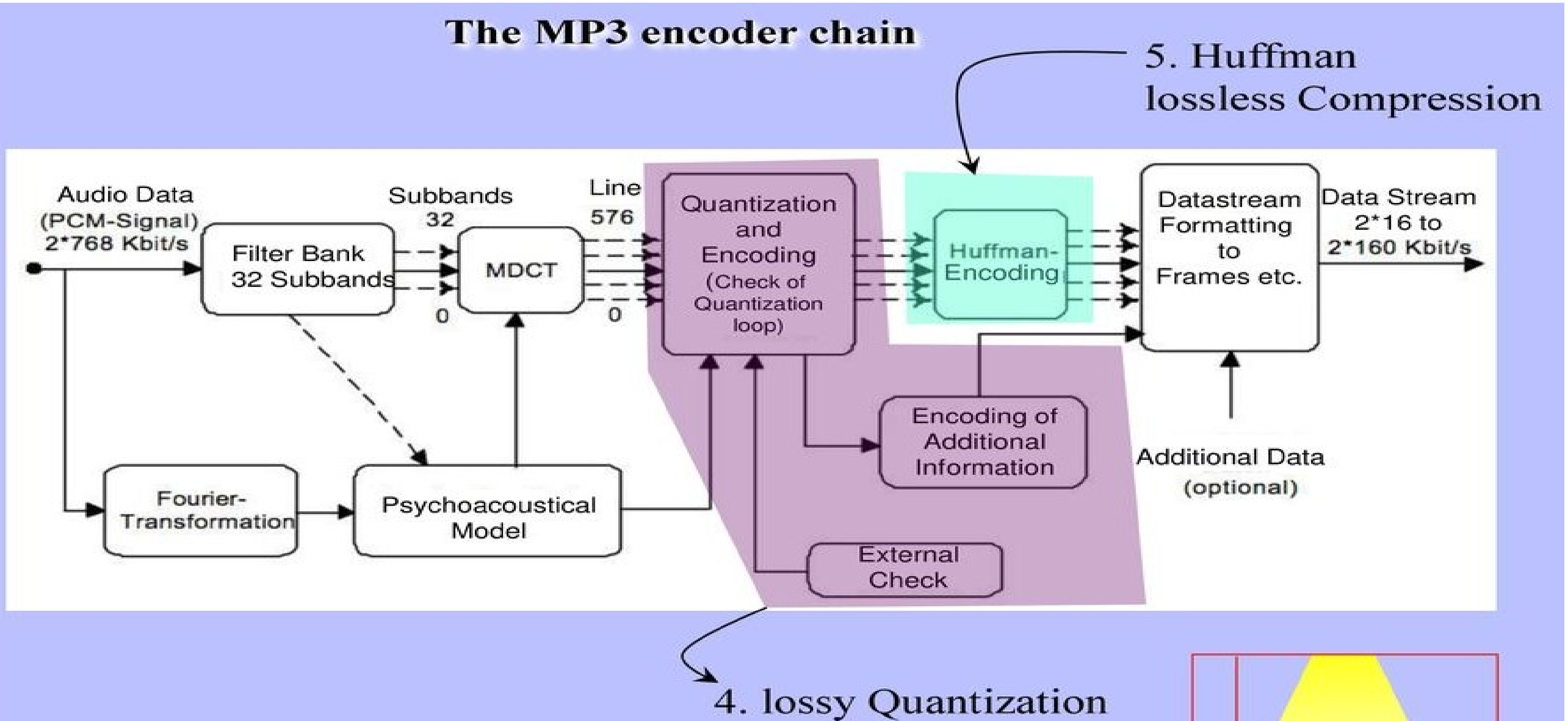


Nikon EXPEED, a system on a chip including an image processor, video processor, digital signal processor (DSP) and a 32-bit microcontroller controlling the chip

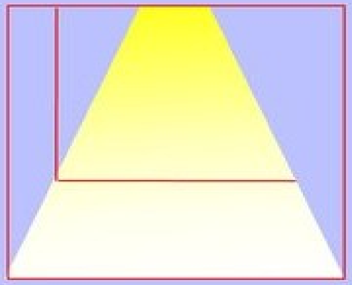
Complex JPEG codec

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.

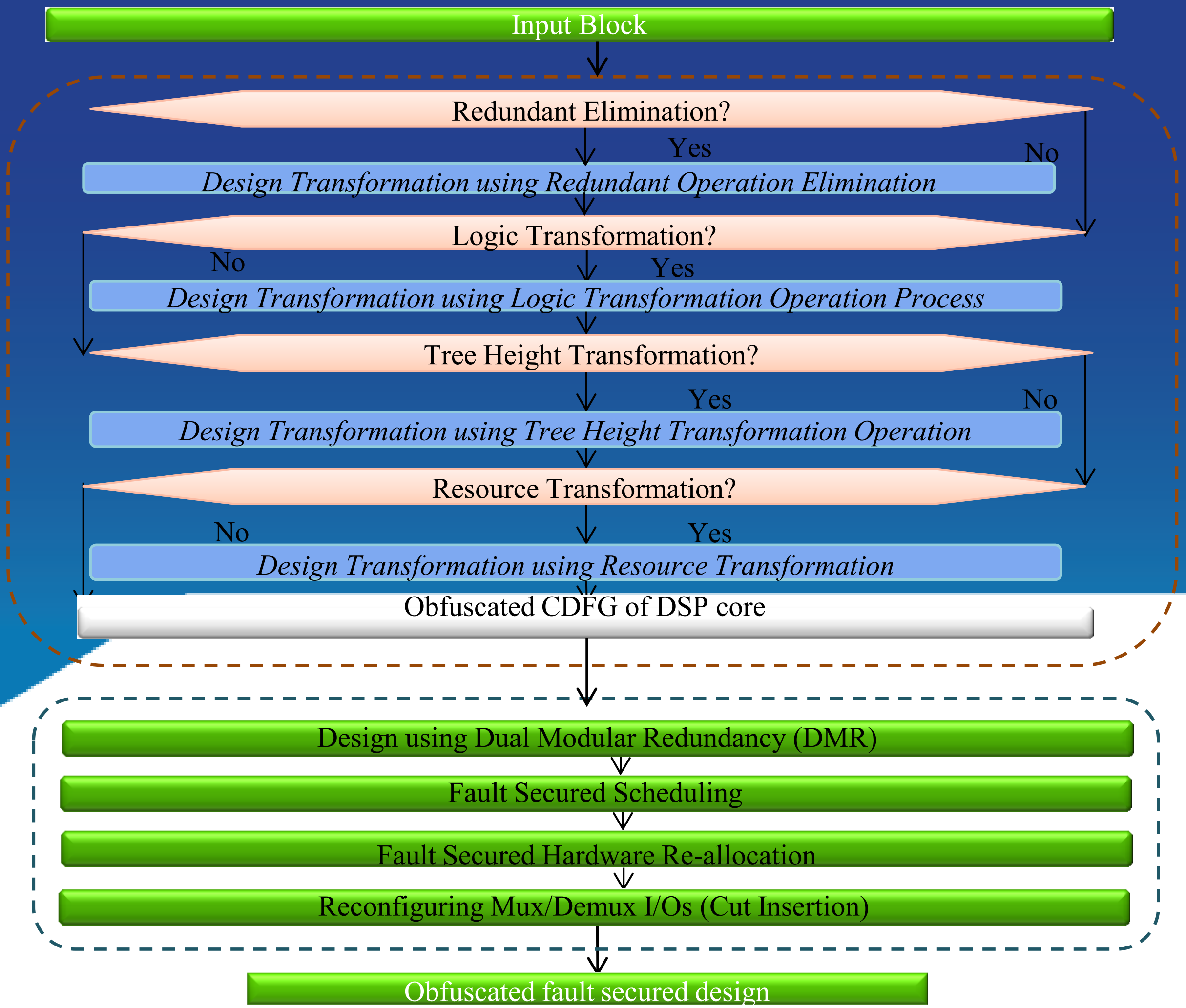
Another example of DSP in CE



Already discussed, Ok!!!!
40% of compression



Generic Design Flow of the Obfuscation process

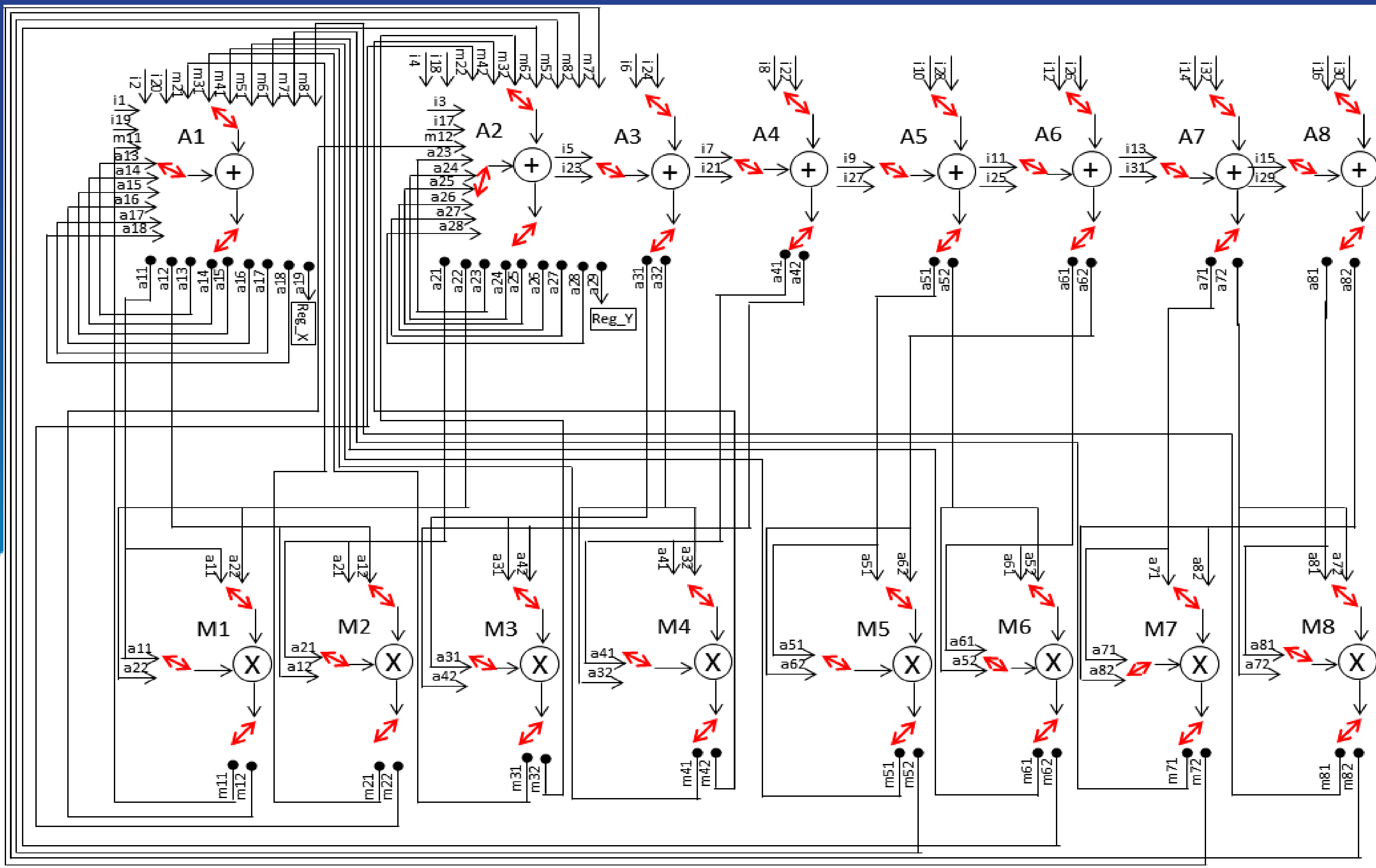


Obfuscation for fault Secured DSP Designs

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

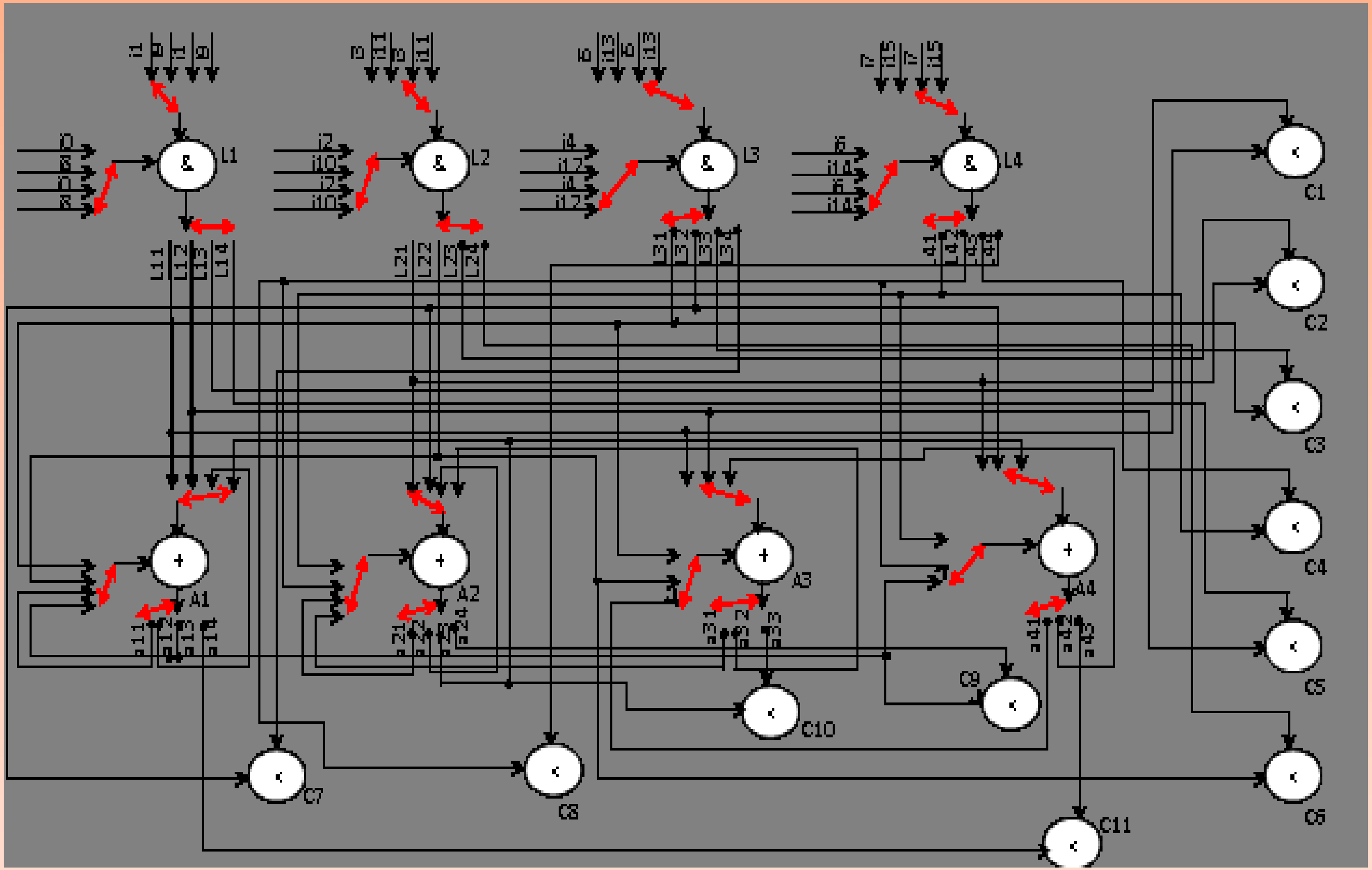
Non-obfuscated DSP circuit of a FIR filter with normal fault security



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

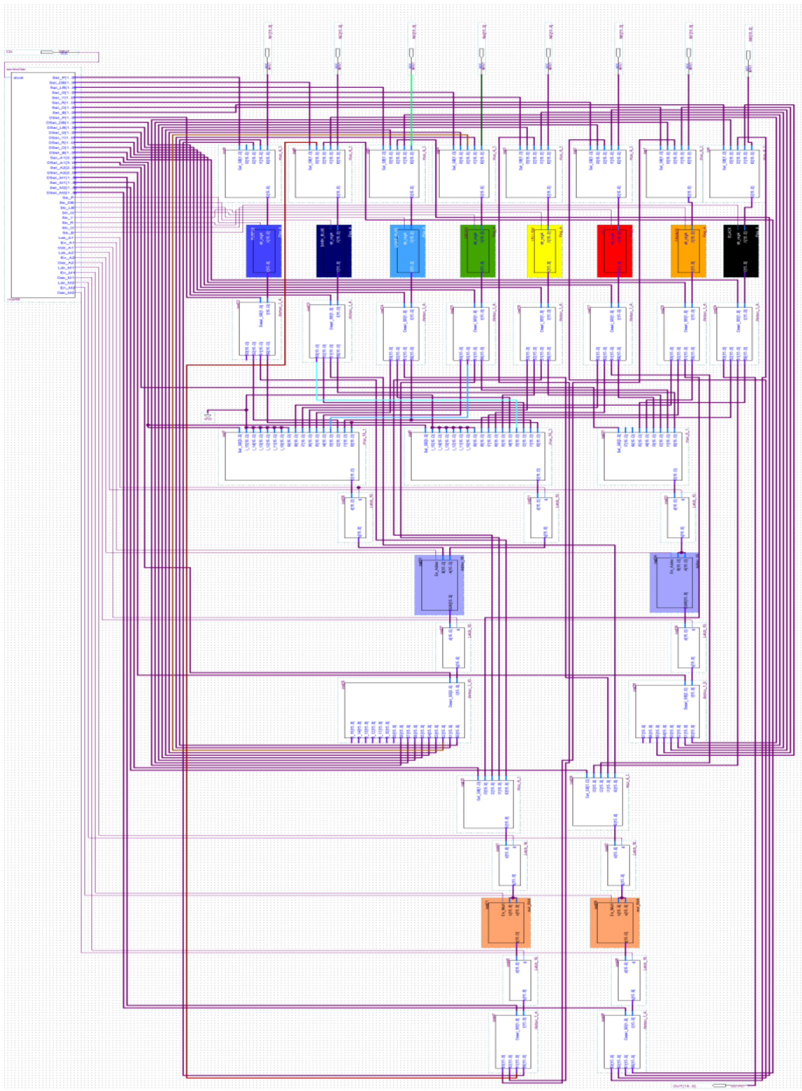
IEEE

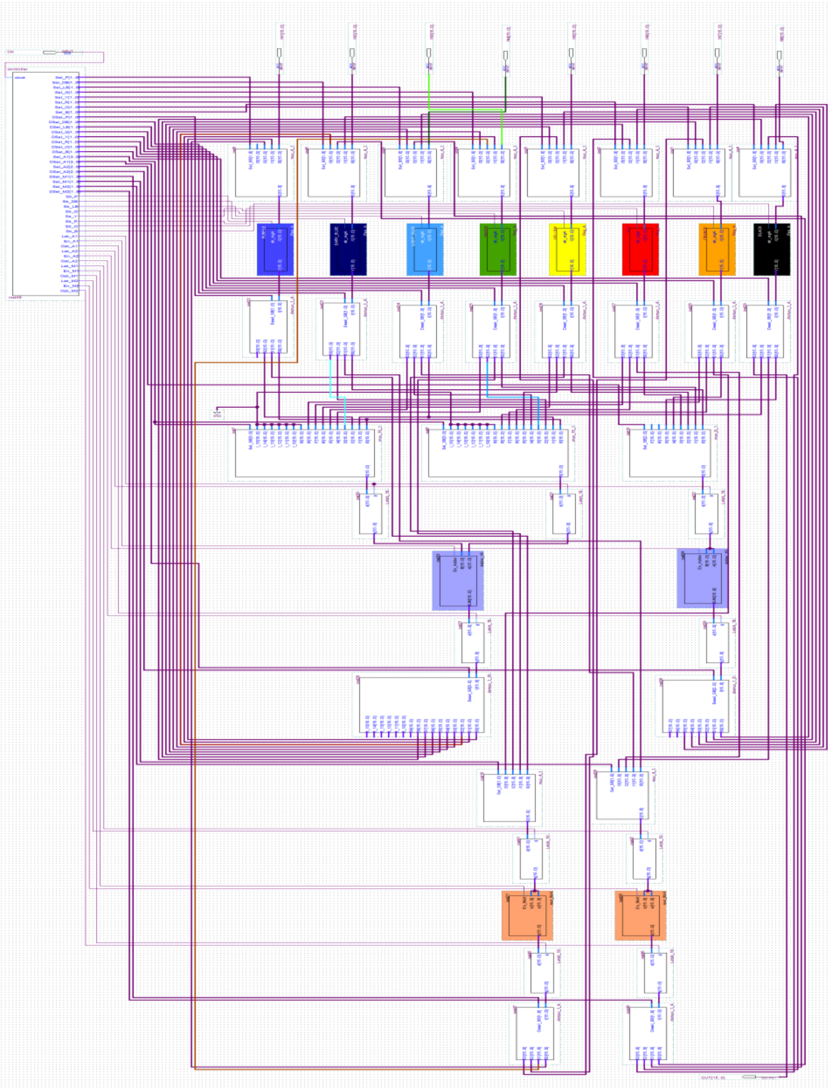
Obfuscated Design of fault secured FIR filter



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

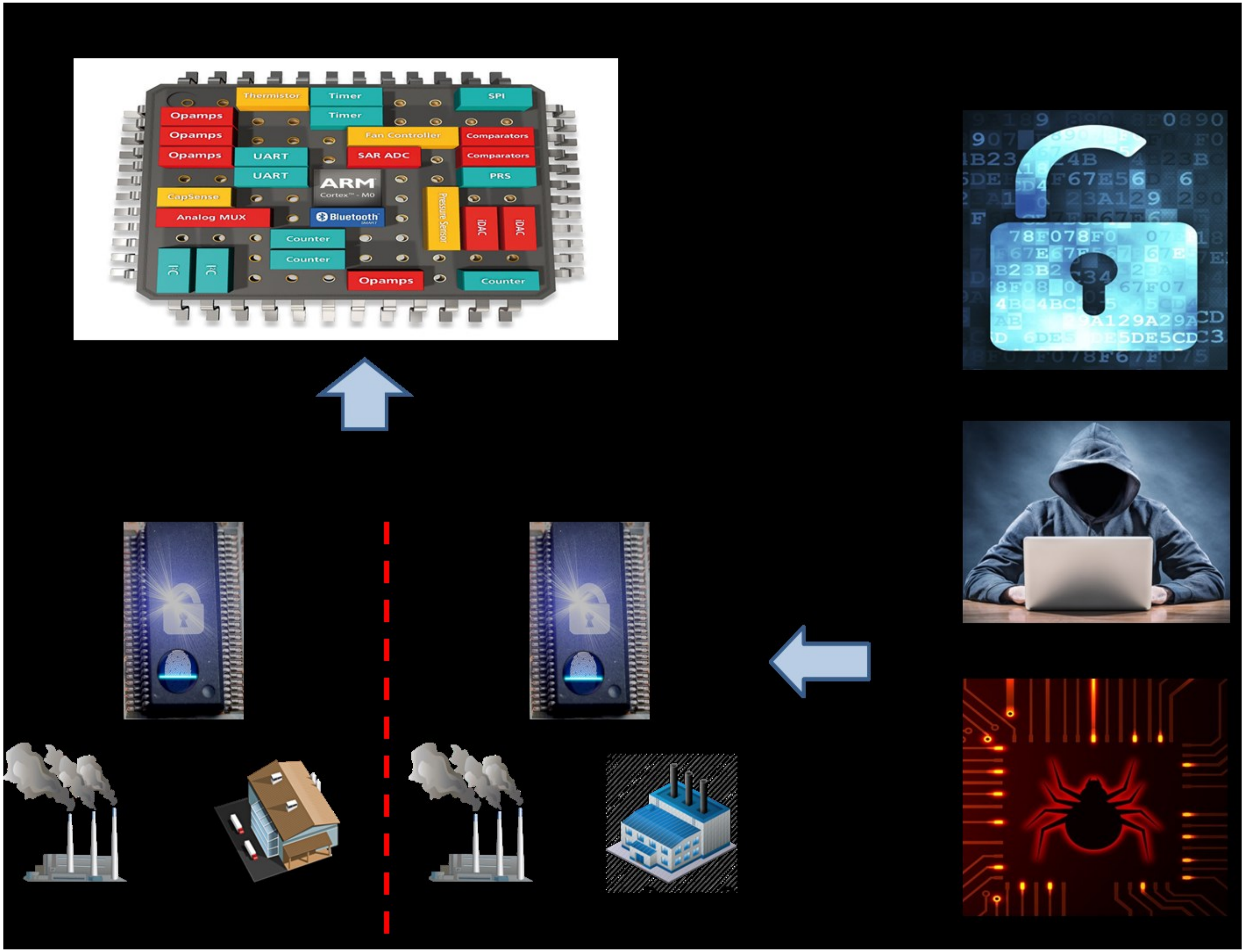
Watermarked FIR Vs Non-Watermarked FIR at RTL



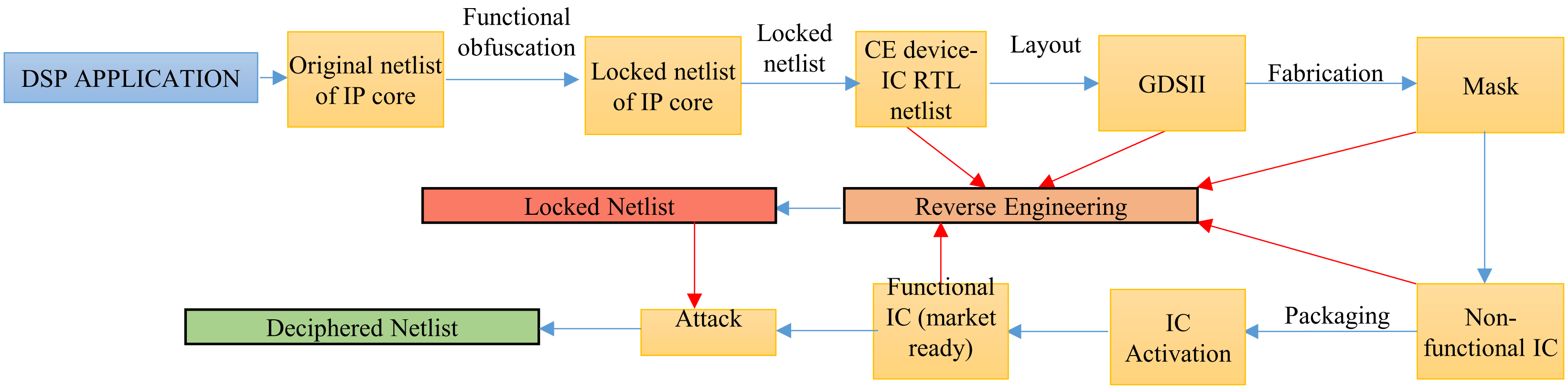


Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** Volume: 37, Issue: 4, April 2018, pp. 742 - 755

Symmetrical IP Core Protection



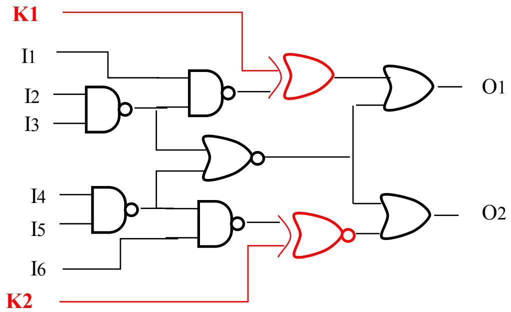
How Hardware of a CE device can be compromised ?



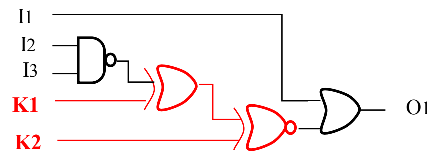
- Reverse engineering (RE) of a DSP core is a process of gaining the complete understanding of its **functionality**, **design** and **structure**.
- However, RE can be used for dishonest intention such as **overbuilding**, **piracy**, or **counterfeiting** a DSP core or inserting a **hardware Trojan**.

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

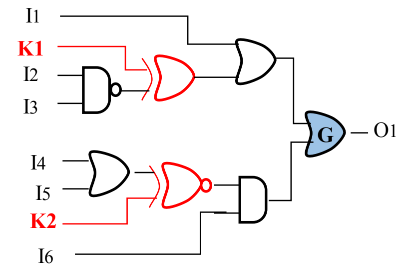
Possible Threat Scenarios



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.

Cont…

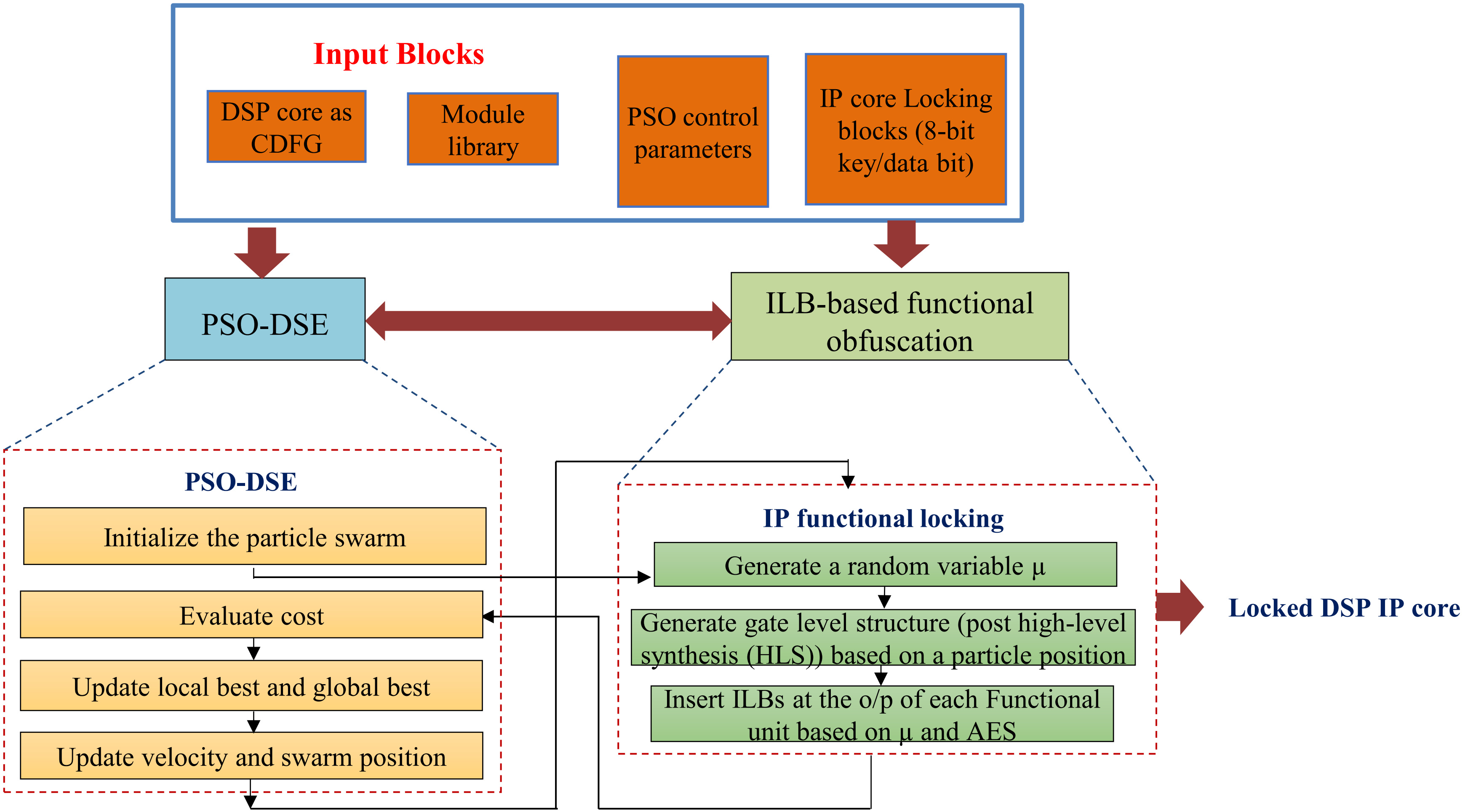
2. **IP Piracy and Trojan attack:** IP piracy attacks and Trojan insertion attacks aims to identify correct key to understand functionality of an IP. Further, Trojans are required to be inserted at safe places thus an attacker has to understand the correct functionality.
3. **Removal attack:** Removal attack identifies all the key-gates from a locked netlist and removes them to obtain an unlocked circuit. Unlocked circuit can be resold illegally to make a profit or Trojan logic can be inserted at safe places.
4. **SAT attack:** SAT attack algorithm formulates a SAT formula and then the SAT solver generates an assignment to distinguishing input pattern (DIP). After the DIP is formed, it is then fed to the activated functional IC and correct output is observed. This distinguishing input/output pair can be used to eliminate the wrong key combinations, till no new one is found.

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

Low-cost functional obfuscation



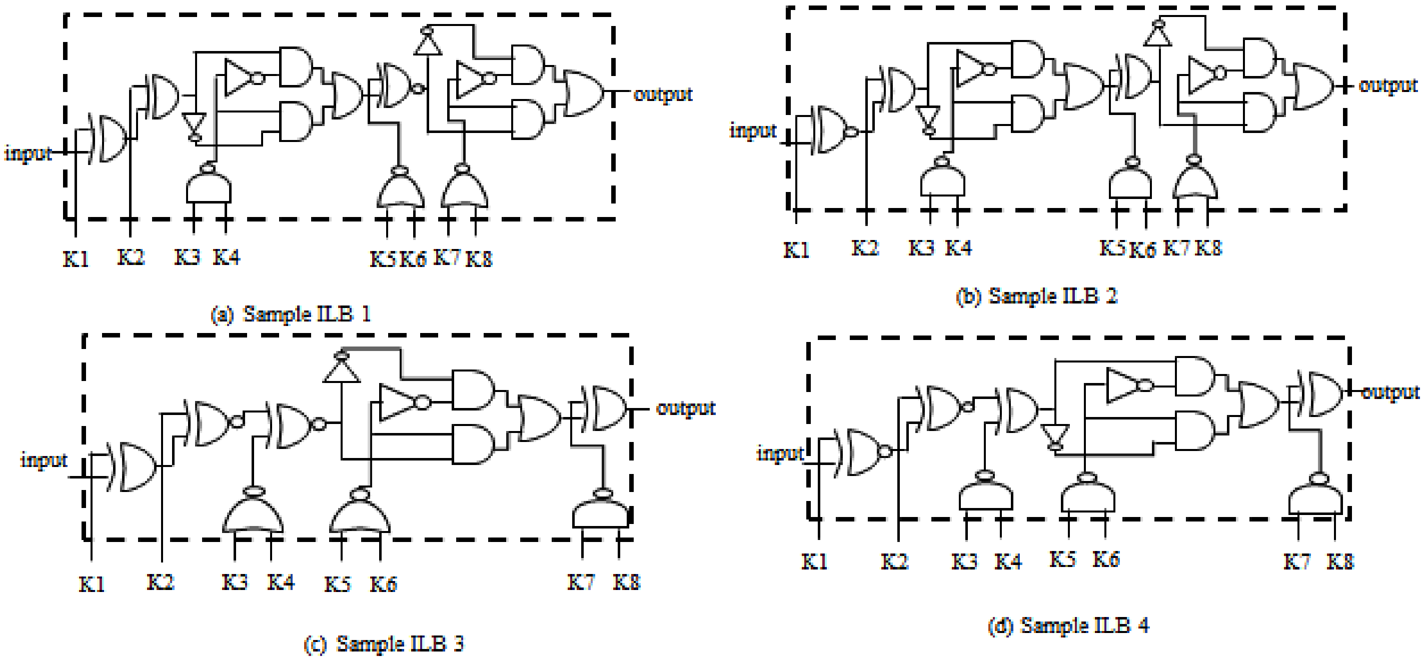
Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** 2019

What is needed?

- A novel enhanced locking approach with lightweight AES for functional obfuscation of DSP IP cores.
- A novel approach for designing several IP logic obfuscation blocks that includes strong security feature.
- Generates a low cost obfuscated netlist through PSO-driven optimization framework.
- Enhancement in security in terms of strength of obfuscation.

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

Proposed IP core locking blocks (ILBs)



- Each ILB consist of **8-bit key** value inserted into **each bit of output** data.
- ILBs are designed using the **different combination** of AND, NAND, NOT, XOR and XNOR gates.
- Structures of ILB depend on the key values.
- Innumerable **different structures** of ILBs with the **same area** is possible.

Insertion technique of ILB

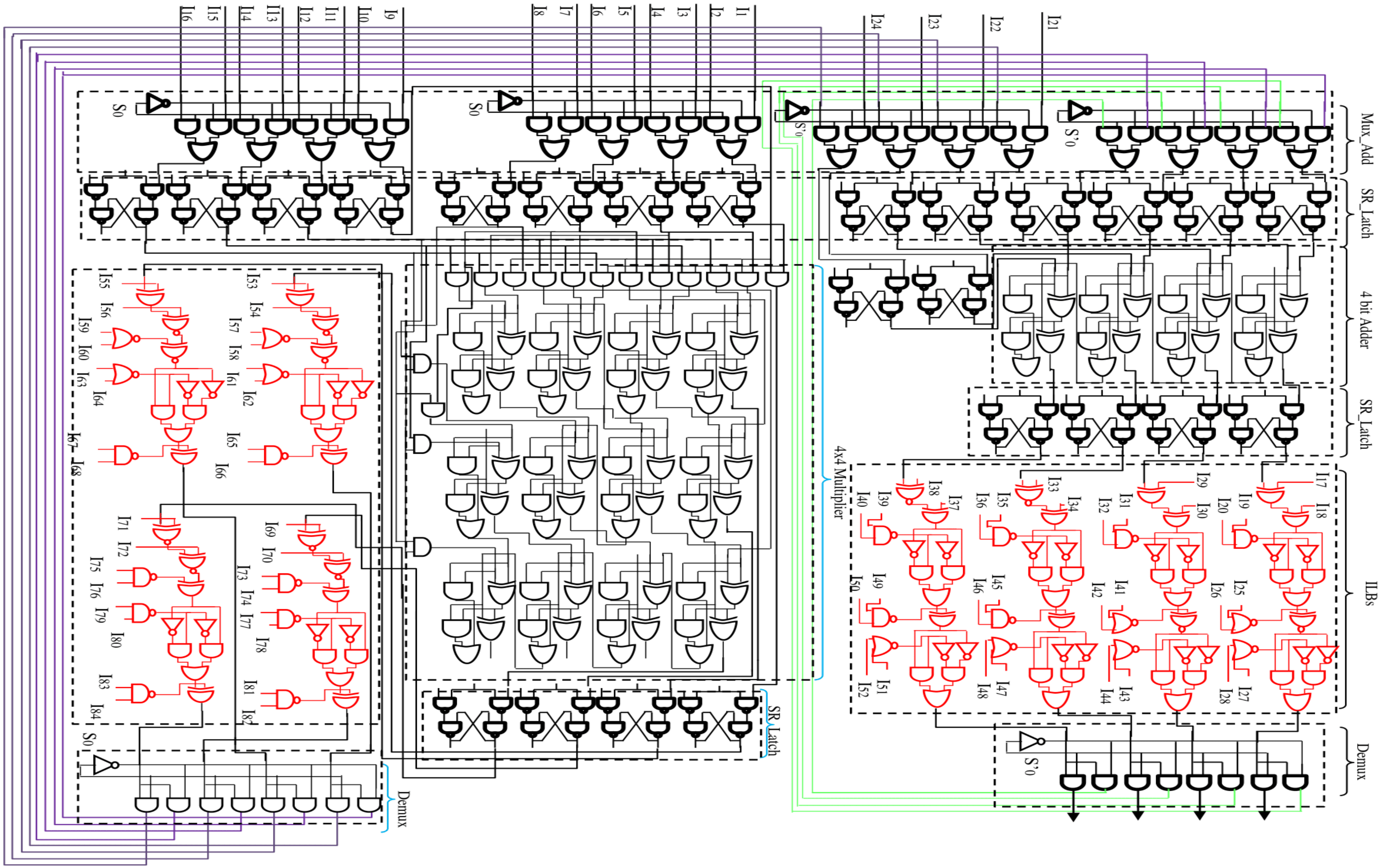
1. Generate a random integer number ‘μ’ (through PSO-DSE process) such that:

$$1 \leq \mu \leq T_{ILB}$$

   T_{ILB} = the total number of ILB structure/template available to insert in the design (we used T_{ILB} = 4).

2. Perform post high-level synthesis to obtain gate level datapath structures.
3. Insert ILB in each output data bit of functional unit based on ‘μ’ value.
4. Same ILB must be inserted ‘μ’ times into the design.
5. After ‘μ’ repetition next ILB from T_{ILB} is selected.
6. Continue this process until all the output data bits of functional units are connected to ILBs.

Obfuscated gate structure of 4-bit FIR



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.

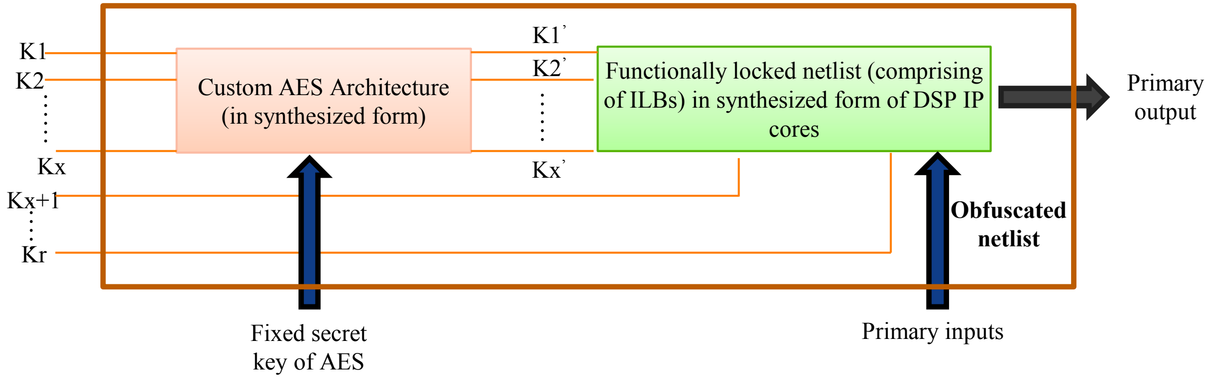
- **Prohibiting key gate isolation:** Proposed ILBs are a combination of multiple key gates dependent on each other thus ensuring no-isolation among key inputs. Hence, impedes an attacker's attempt to sensitize key without knowing/controlling key-bits.

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.

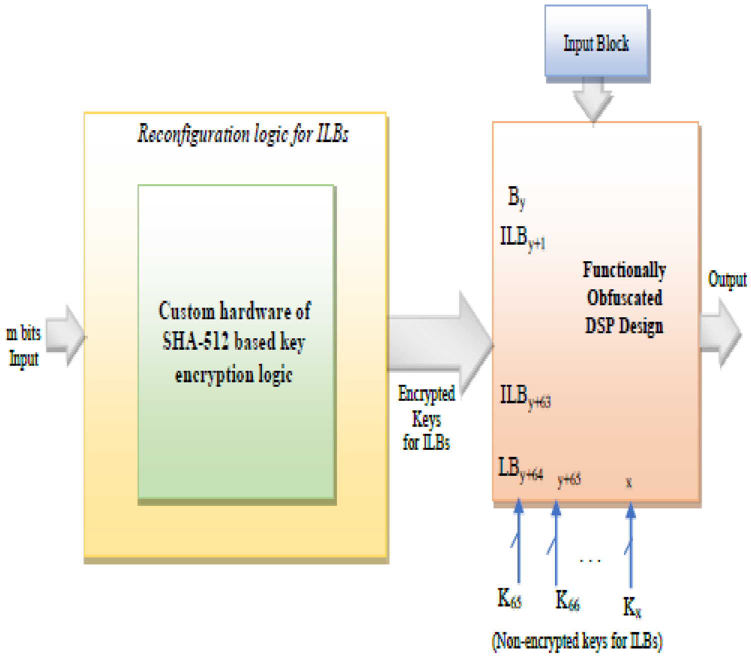
Cont...



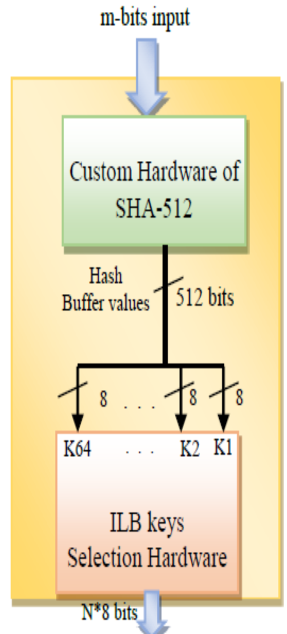
- **Resiliency against SAT attack:** Custom lightweight AES block with fixed secret key is integrated to a sub-set of functional locking blocks in the obfuscated netlist to prevent an attacker from determining the inputs from its output.

- **Resiliency against ILB removal attack:** Subset of ILB structures are re-configured depending on the AES encrypted output. Number of possibilities also increases with the number of key-inputs fed to ILBs through AES. Therefore, the attacker would not be able to identify the reconfigured ILB structures.

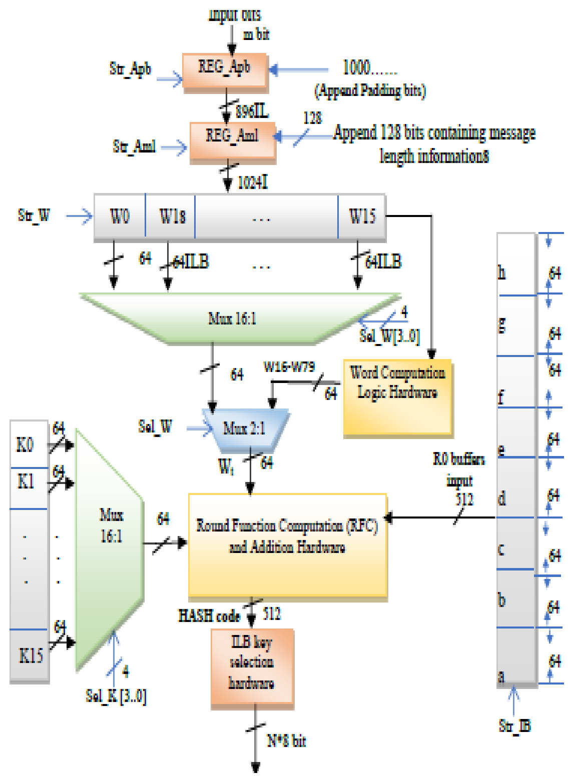
Reconfiguring locking logic using SHA-512 based key encryption hardware



.Overview of encrypted keys generated for ILB reconfiguration using SHA-512 based key encryption hardware



Block diagram of key encryption logic for reconfiguring ILB structure

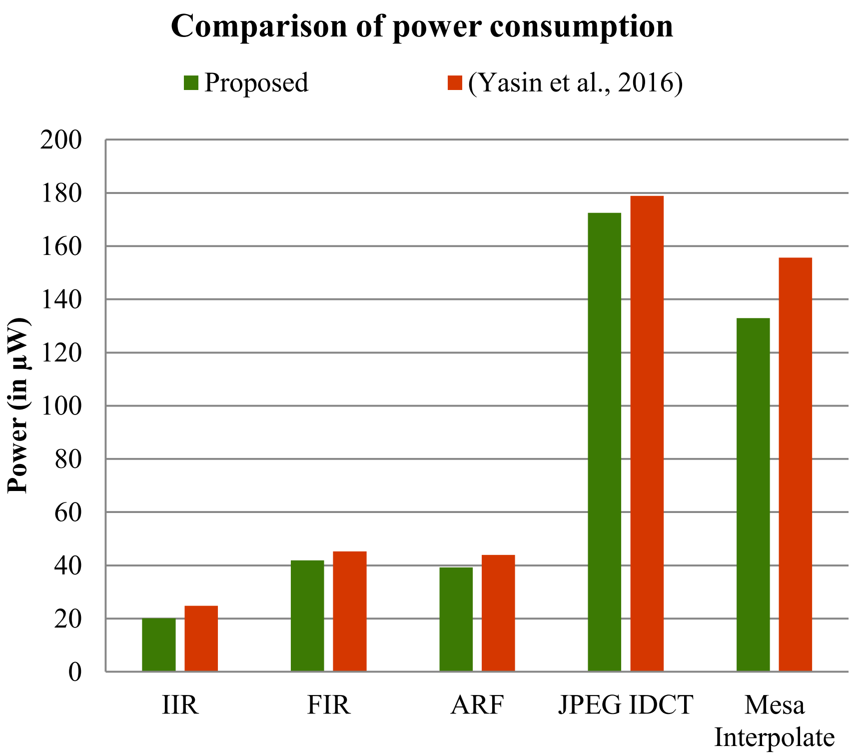


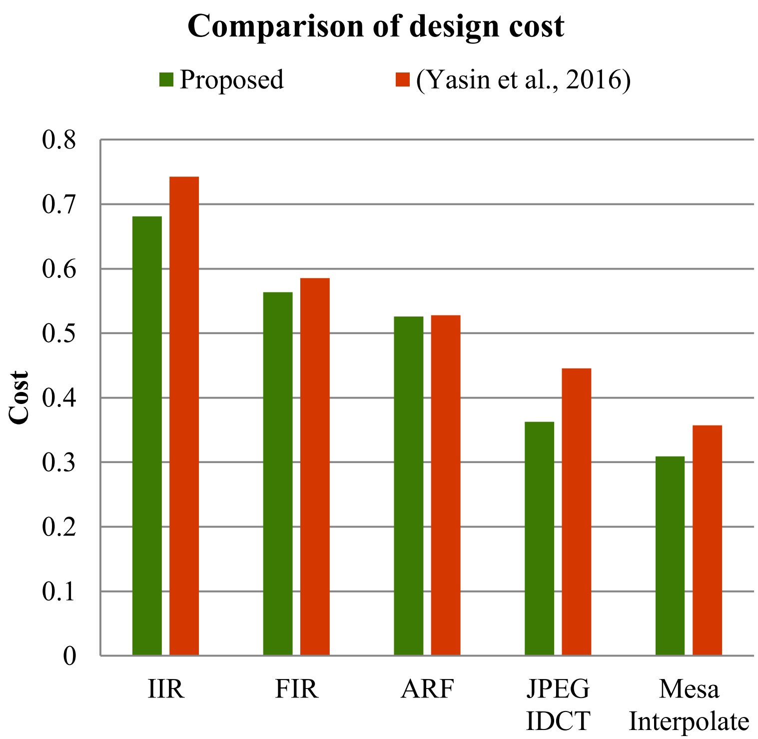
Anirban Sengupta, Mahendra Rathor "Security of Functionally Obfuscated DSP core against Removal Attack using SHA-512 based Key Encryption Hardware", **IEEE Access**, 2019

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

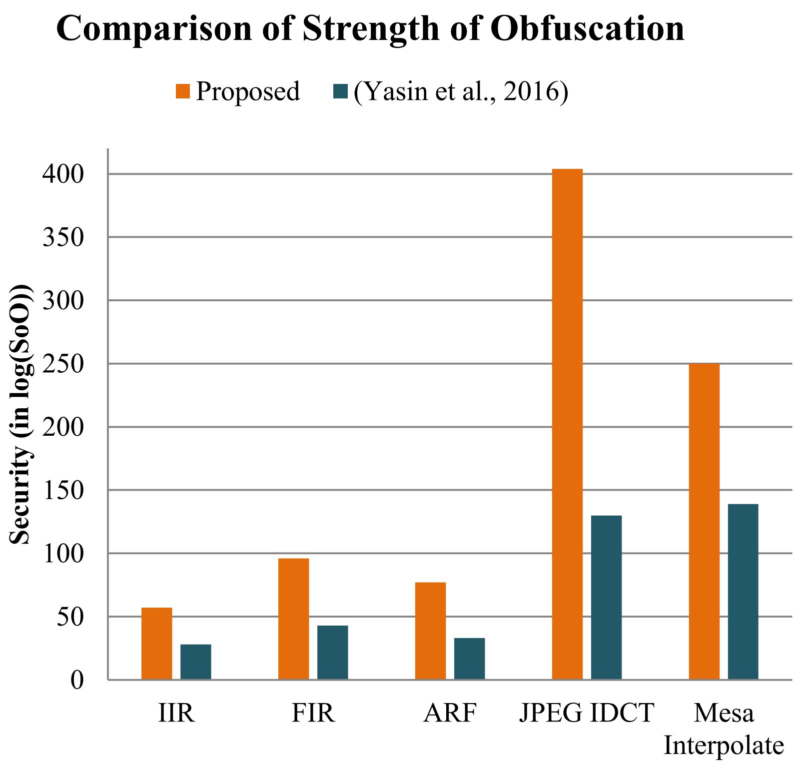
IEEE

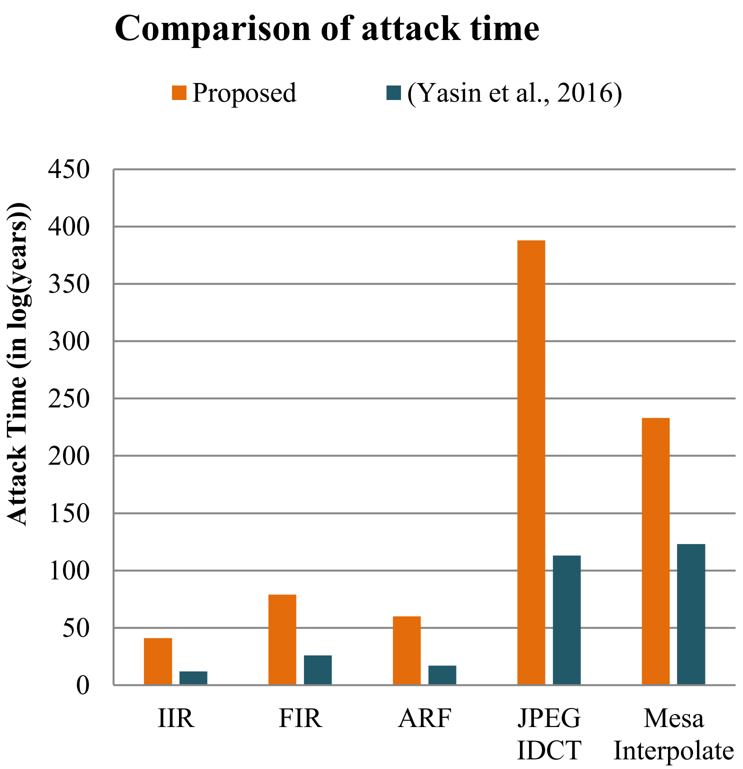
Result (comparative study)





Result (comparative study)





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, Mahendra Rathor, "IP Core Steganography using Switch based Key-driven Hash-chaining and Encoding for Securing DSP kernels used in CE Systems", IEEE Transactions on Consumer Electronics (TCE), 2020
- Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", IEEE Transactions on Consumer Electronics (TCE) , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 – 515
- https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool
- Anirban Sengupta, Rahul Chaurasia, Tarun Reddy "Contact-less Palmprint Biometric for Securing DSP Coprocessors used in CE systems", IEEE Transactions on Consumer Electronics (TCE) , Volume: 67, Issue: 3, August 2021, pp. 202-213
- Rahul Chaurasia, Aditya Anshul, Anirban Sengupta "Palmprint Biometric vs Encrypted Hash based Digital Signature for Securing DSP Cores Used in CE systems", IEEE Consumer Electronics (CEM) , Volume: 11, Issue: 5, September 2022, pp. 73-80
- 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, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", IEEE Transactions on Very Large Scale Integration Systems , Vol 28, Issue: 9, 2020, pp. 1979-1992
- Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", IEEE Transactions on Consumer Electronics (TCE), Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

Conclusion

The future of CE system / IoT design / CPS design / Autonomous vehicle design is Energy-Security Tradeoff !

Thank You