Hardware Watermarking and IP Metering for IP Core Protection

Dr. Anirban Sengupta, Prof., FIET, FBCS, IEEE Senior Member
IEEE Distinguished Speaker
Associate Editor, IEEE Transactions on Consumer Electronics
Associate Editor, IEEE Transactions on Aerospace & Electronic Systems
Senior Editor, IEEE Consumer Electronics
Editor-in-Chief, IEEE VLSI Circuits & Systems Letter
Executive Committee, IEEE Computer Society Technical Committee on VLSI
Conference Chair, 37th IEEE ICCE '19, Las Vegas (USA)
Technical Chair, ISVLSI 2019, USA

Computer Science and Engineering
Indian Institute of Technology Indore, India
Web: www.anirban-sengupta.com

Consumer Electronics (CE) Hardware Protection/Security

- Consumer electronic products currently are composed of highly complex designs.
- They feature in applications such as digital signal processing (DSP), soft processors etc.
- Many DSP algorithms such as FFTs, FIR or IIR, which were previously built using application specific integrated circuits (ASICs) can be built on FPGAs with very high flexibility.
- There is plenty of High Level Synthesis (HLS) tools available in the market today e.g. HDL coder tool, Vivado HLS tool, Catapult etc.
- An HLS tool usually takes in a higher level language description, for example in C, C++ and then based on directives, translates the high level code into RTL-code which can then be synthesized into logic gates.

CE hardware mainly comprises of DSP cores/Blocks/Macro-operators (with more than 50K gates) that need Security/Protection

These DSP Cores rely on HLS

Here HLS is the key !

Courtesy: Xilinx – Vivado HLS -- https://www.xilinx.com/products/design-tools/vivado/integration/esl-design.html

Consumer Electronics (CE) Hardware Backbone

High-Level Synthesis Benefits

- Improved productivity for hardware designers Hardware designers can work at a higher level of abstraction while creating high-performance hardware.
- Improved system performance for software designers Software developers can accelerate the computationally intensive parts of their algorithms on a new compilation target, the FPGA.
- Control the high level synthesis process through optimization directives Create specific high-performance hardware implementations.
- Create multiple implementations from the C source code using optimization directives
- Explore the design space, which increases the likelihood of finding an optimal implementation.

CE hardware mainly comprises of DSP cores/Blocks/Macro-operators (some more than 50K gates) that need Security/Protection

These DSP Cores rely on HLS

Here HLS is the key !

Courtesy: Xilinx – Vivado HLS – User Guide

Complex JPEG with ~ 100K Gates

High-Level Synthesis of DSP core, Multimedia Cores etc (several examples….)

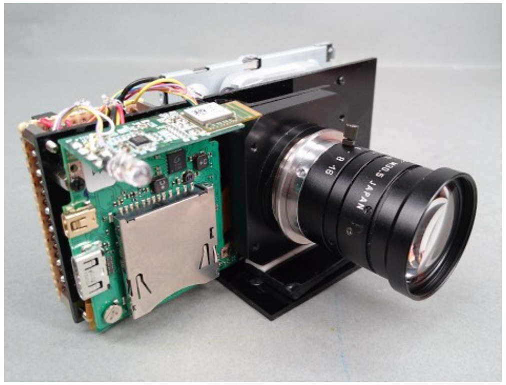
- Digital IIR Butterworth filter
- FIR filter
- DCT and IDCT
- FFT Algorithm
- Low Pass Filter, other Filters
- JPEG Compression and Decompression
- Haar Wavelet Transformation for Image Compression

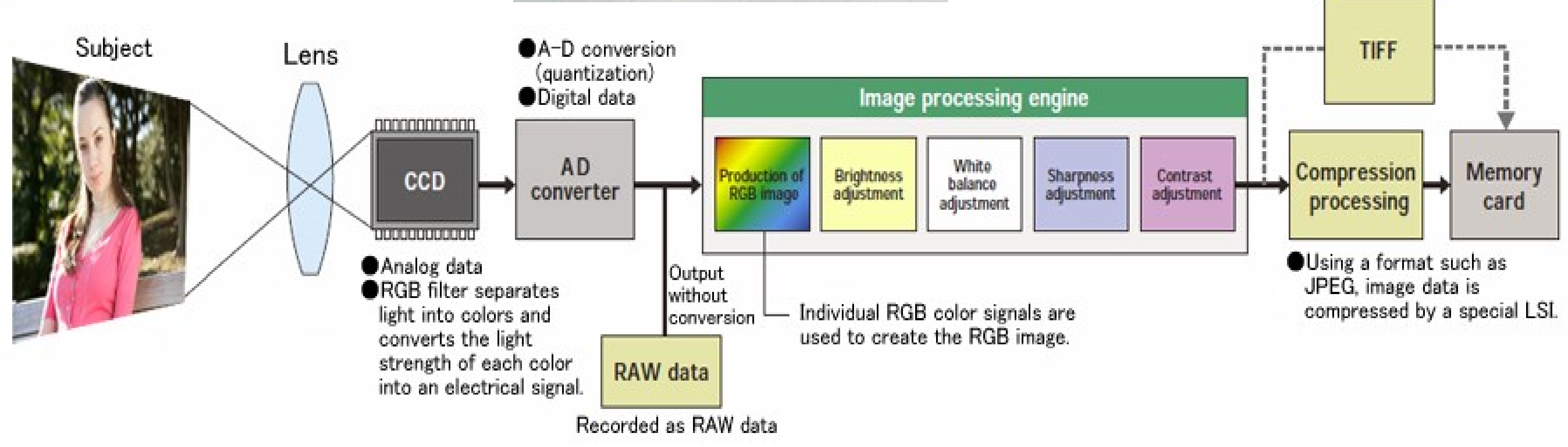
These DSP Cores rely on HLS

Starting from RTL/gate level is not a good idea !

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.





●A-D conversion (quantization)
●Digital data

●Analog data
●RGB filter separates light into colors and converts the light strength of each color into an electrical signal.

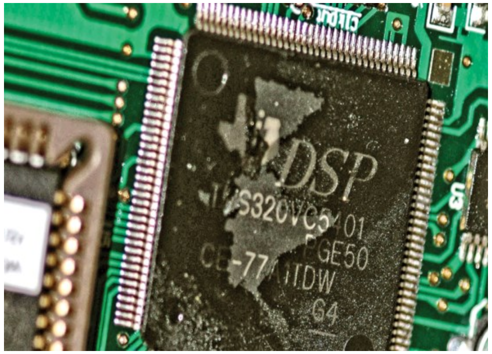
Recorded as RAW data

Individual RGB color signals are used to create the RGB image.

●Using a format such as JPEG, image data is compressed by a special LSI.

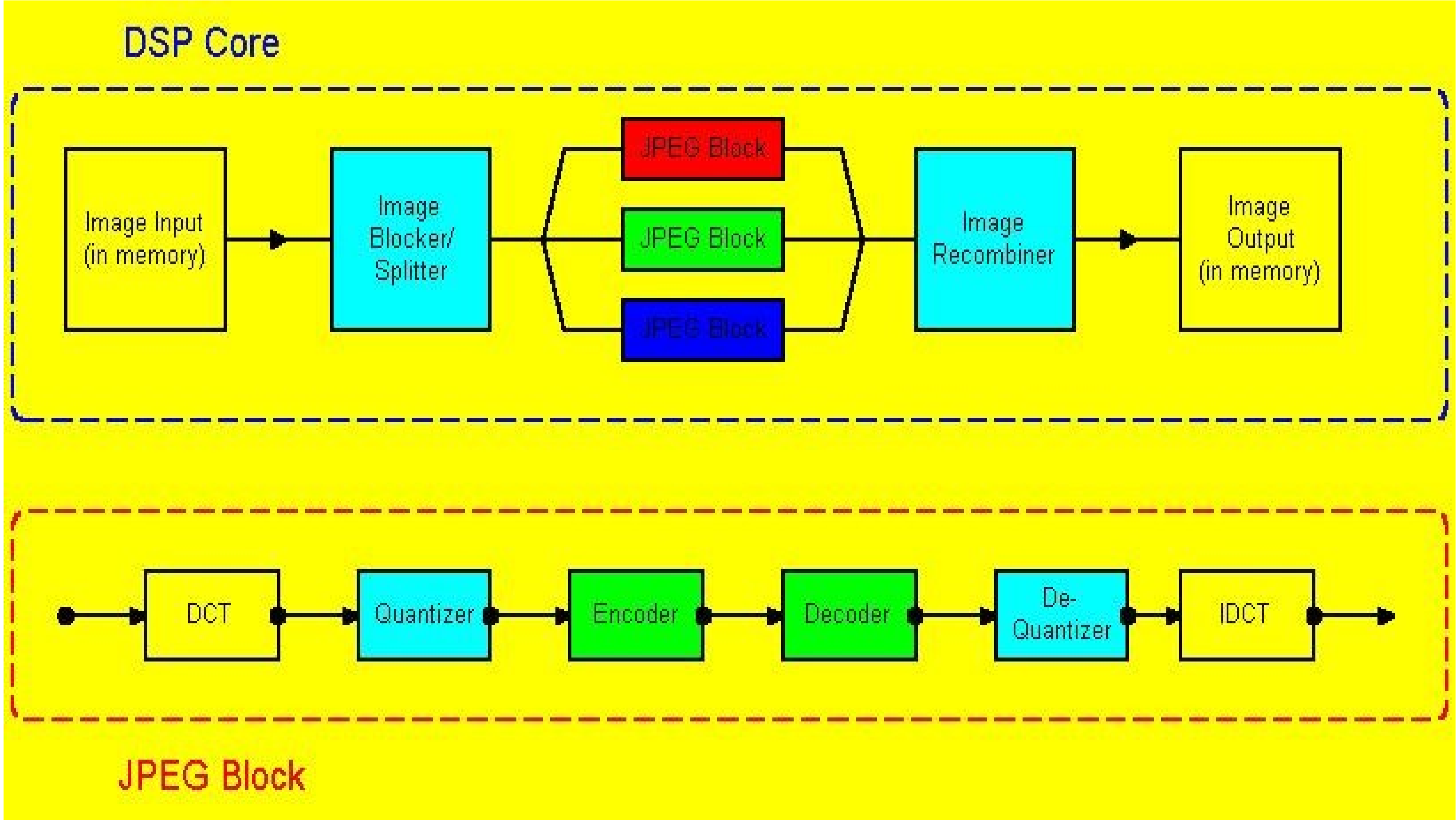
Example of DSP Core in Digital Camera

- ✓ Video cameras take analog light falling on a sensor and convert it to digital. After it's been converted to digital, you can manipulate it — you can adjust the colors, the brightness, you can sharpen or blur it. There are a wealth of things you can do easily with a digital signal.
- ✓ But when you're recording video, if the video questions aren't figured out every 30th of a second, 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.

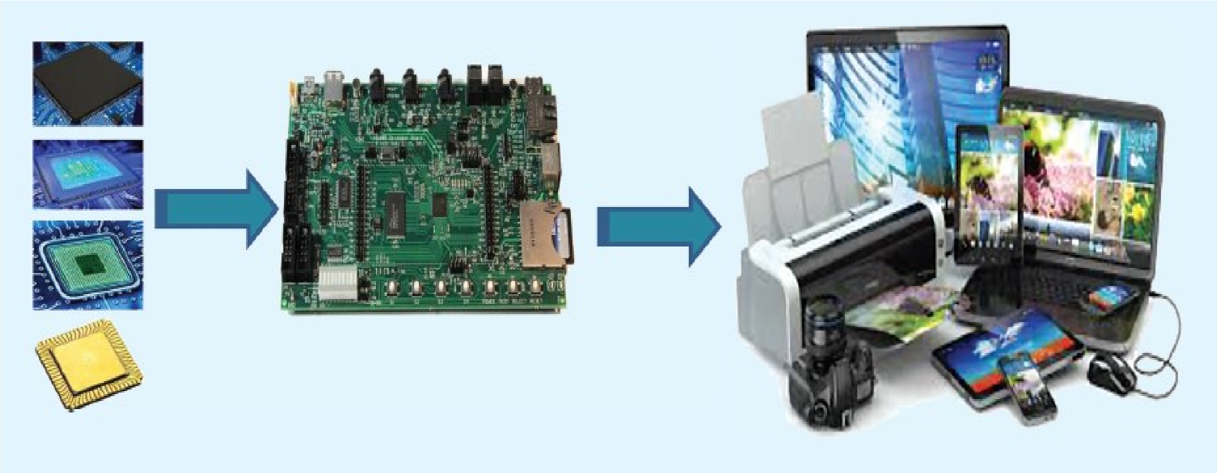


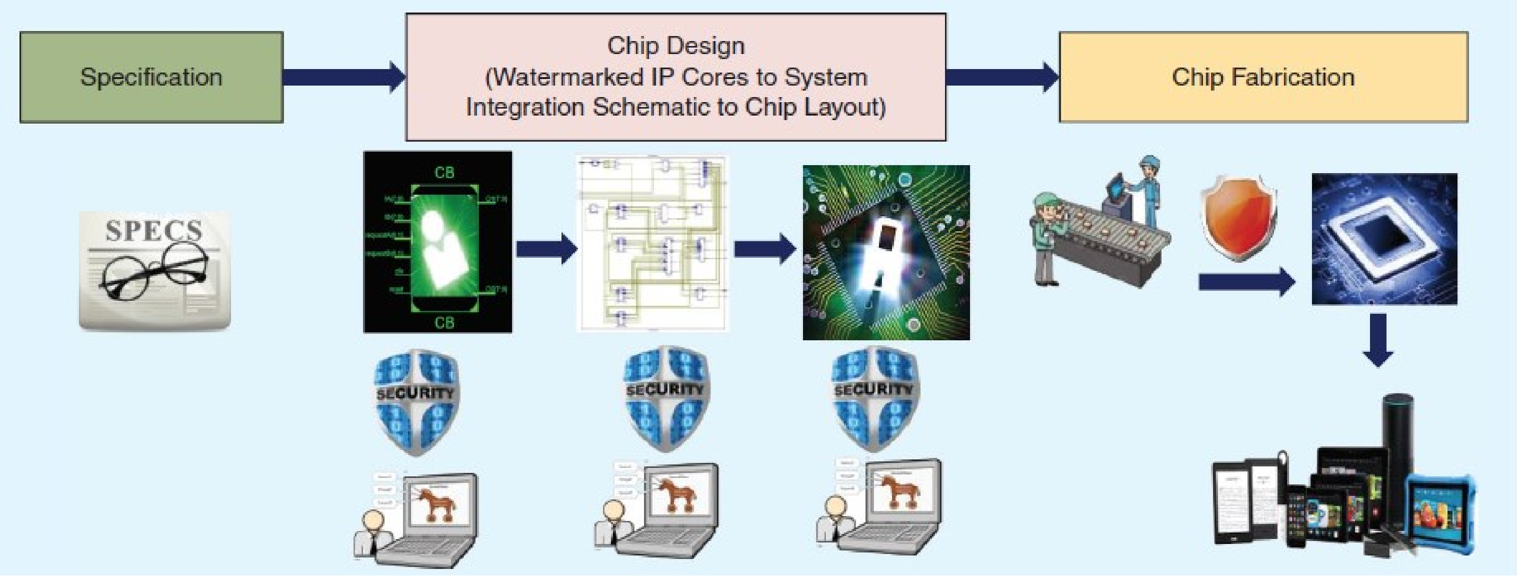
Nikon EXPEED, a system on a chip including an image processor, video processor, digital signal processor (DSP) and a 32-bit microcontroller controlling the chip

Example of DSP Core in Digital Camera



CE Device Design Flow



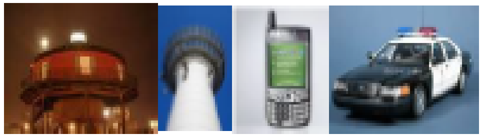


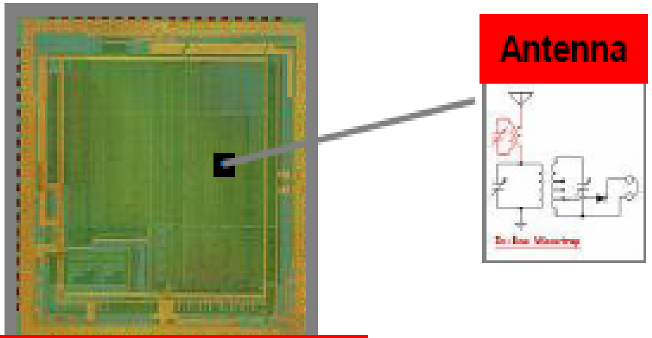
Specification

Chip Design
(Watermarked IP Cores to System Integration Schematic to Chip Layout)

Chip Fabrication

A. Sengupta et. al "Hardware Vulnerabilities and its Effect on CE Devices: Design-for-Security against Trojan", IEEE Consumer Electronics, 2017

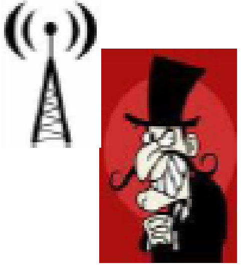




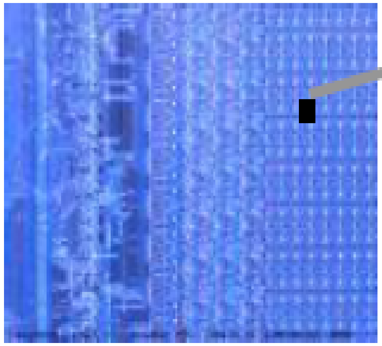
Antenna

Untrusted Hardware

- Adversary can send and receive secret information.
- Adversary can disable the chip, blowup it, send wrong processing data, etc.



- Adversary can place an Antenna on the fabricated chip.

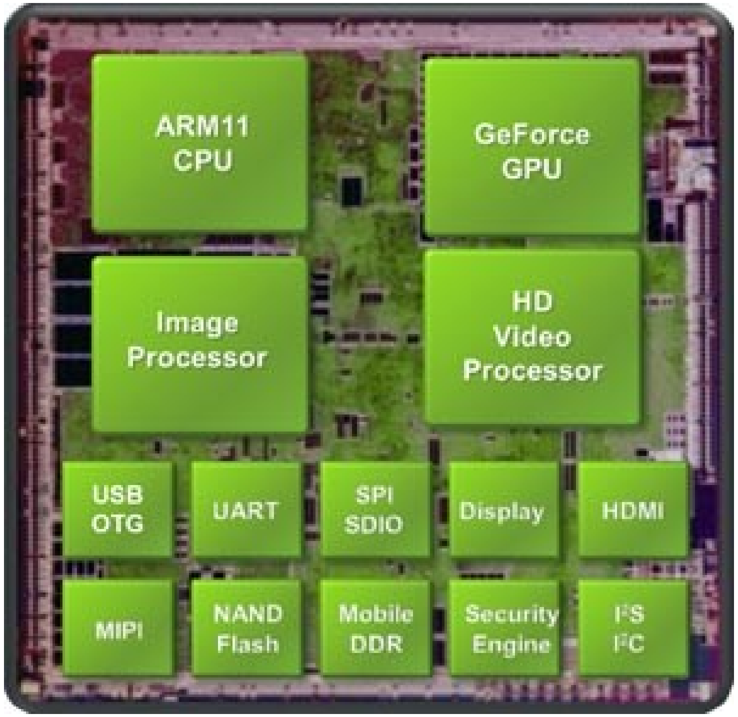


Counter

Finite state machine (FSM)

Intellectual Property (IP) Core …

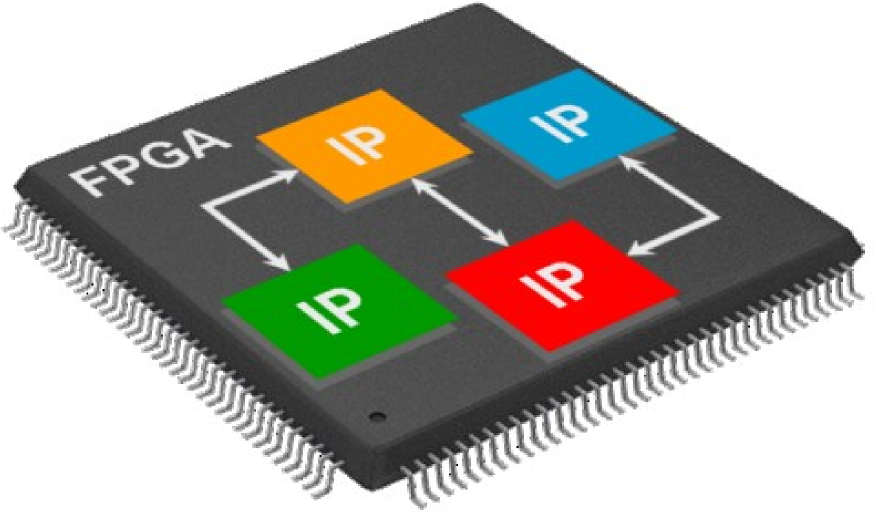
- Consumer Electronics is realized as SoC for low-power, low-cost and high performance requirements.
- Consumer Electronics SoC design challenges include:
  – Lower Cost, Lower Design Cost, and Shorter Time-to-Market



- IP cores based system design is used to meet the challenges
- IP cores (often supplied by third party vendors)
  - Maximize design productivity, minimize design time

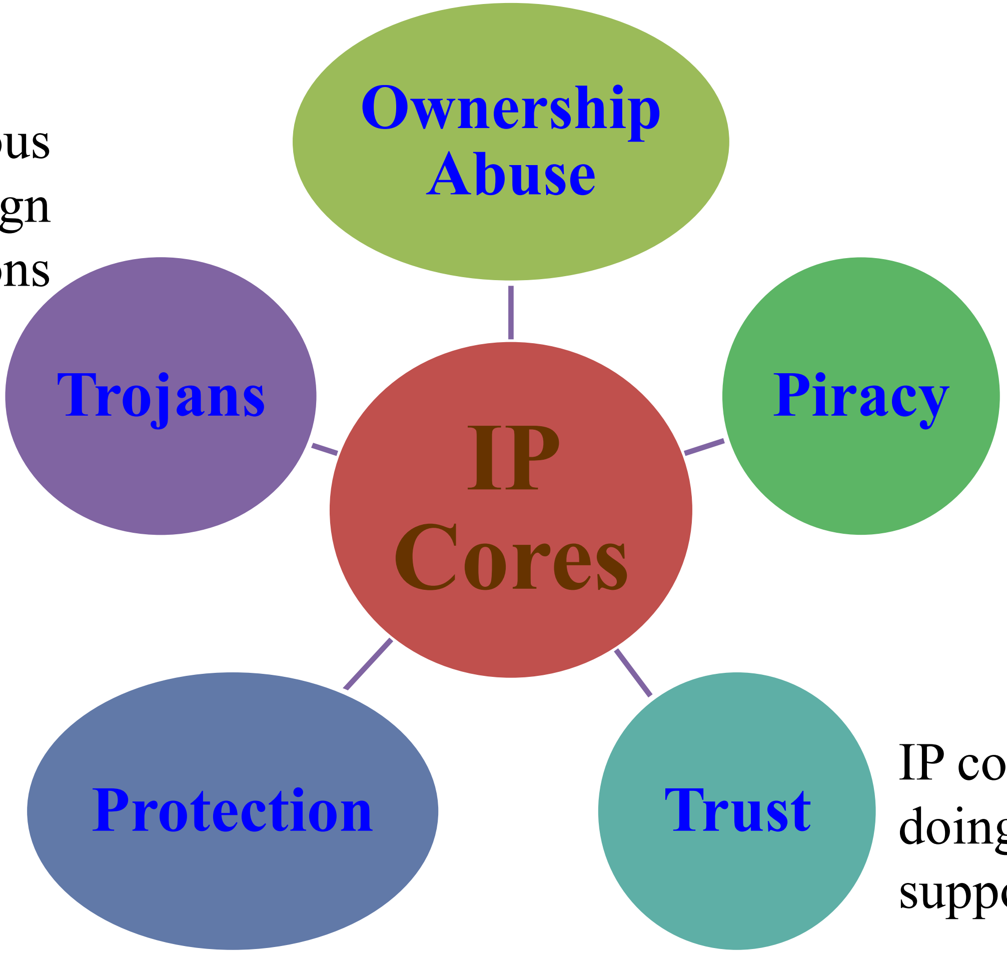
Intellectual Property (IP) Core

- An IP Core is a reusable unit of logic, block, component, cell, or layout design that is developed for licensing to multiple vendors to use as building blocks in different system designs.



A. Sengupta "Cognizance on Intellectual Property: A High-Level Perspective", **IEEE Consumer Electronics**, 2016

IP Core – Selected Issues/Challenges



IP Cores

Ownership Abuse

Trojans

Malicious design modifications

Piracy

Piracy by fraudulent means or reverse engineering

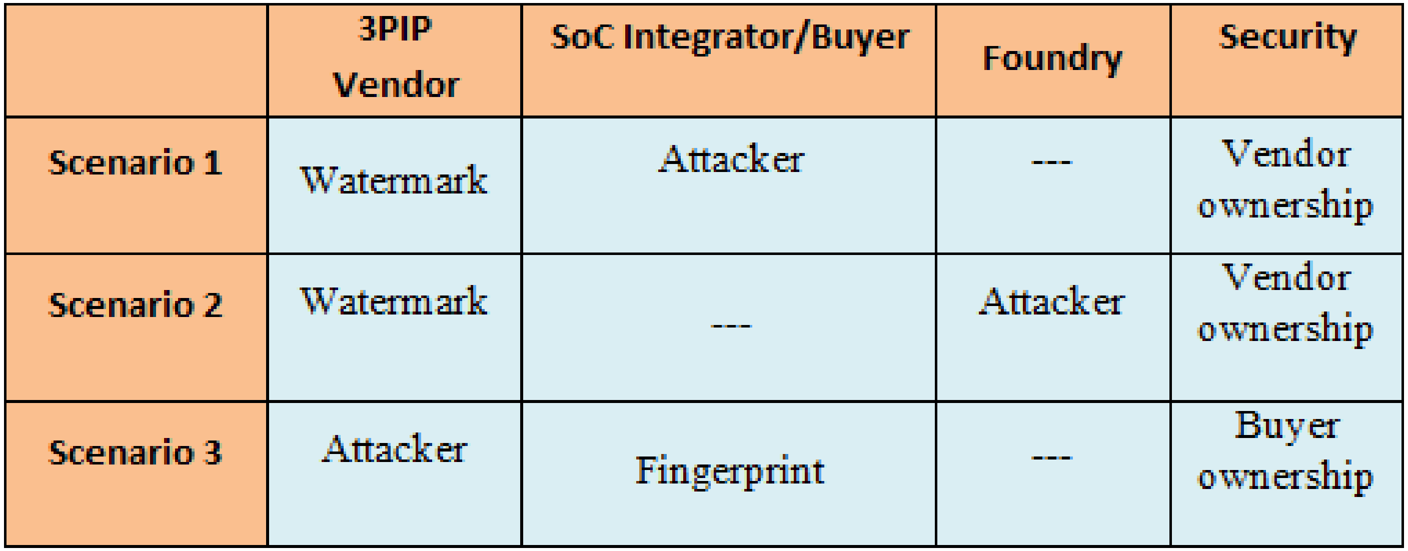
Protection

Trust

IP core is really doing what it supposed to do

A. Sengupta "Protection of IP-Core Designs for CE Products", **IEEE Consumer Electronics**, 2015

IP Threat Models: Type 1

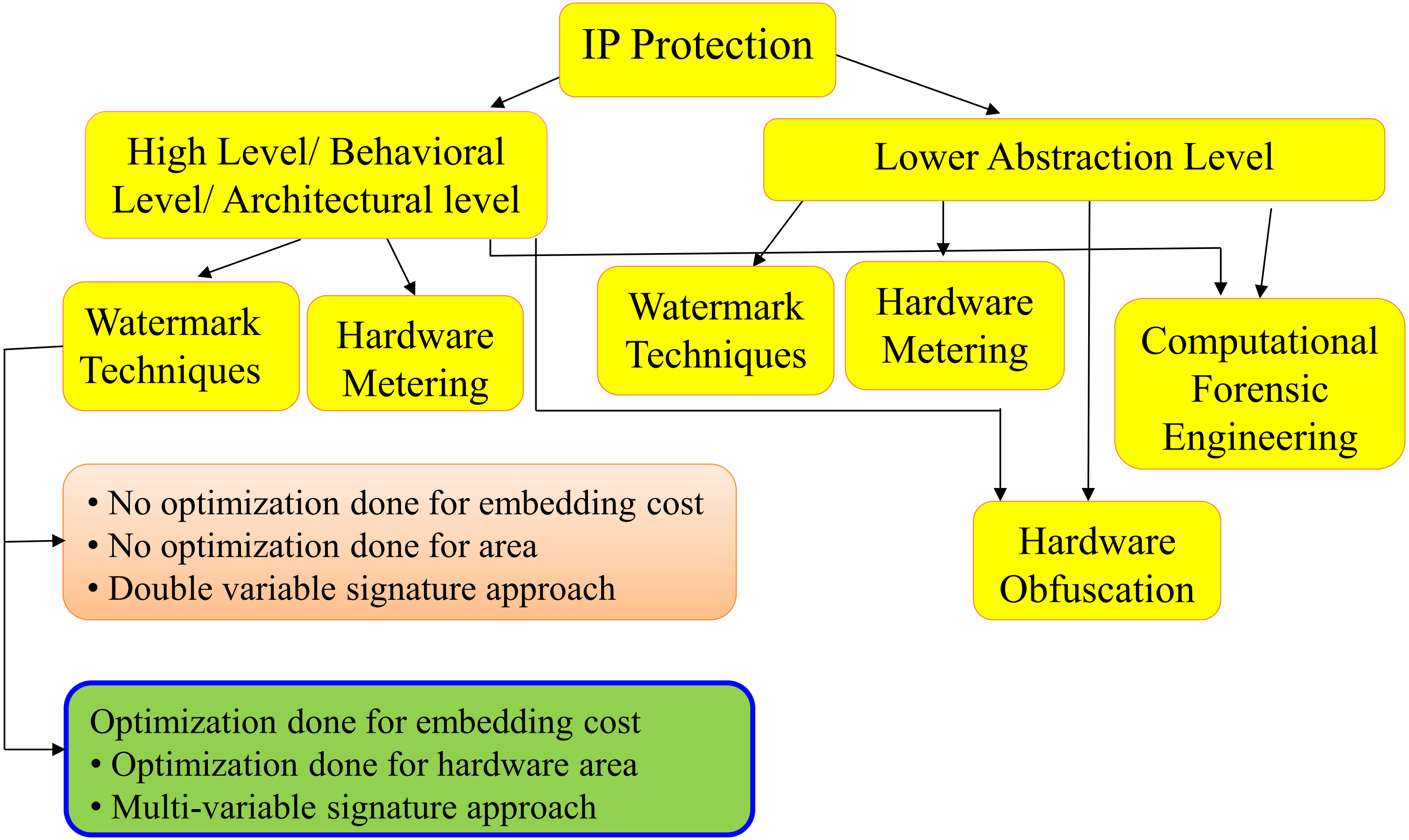


	3PIP Vendor	SoC Integrator/Buyer	Foundry	Security
Scenario 1	Watermark	Attacker	---	Vendor ownership
Scenario 2	Watermark	---	Attacker	Vendor ownership
Scenario 3	Attacker	Fingerprint	---	Buyer ownership

Typical attacks related to IP Piracy

A. Sengupta "Hardware Vulnerabilities and its Effect on CE Devices: Design-for-Security against Trojan", **IEEE Consumer Electronics**, 2017

IP Protection



IP Protection

High Level/ Behavioral Level/ Architectural level

Lower Abstraction Level

Watermark Techniques

Hardware Metering

Watermark Techniques

Hardware Metering

Computational Forensic Engineering

Hardware Obfuscation

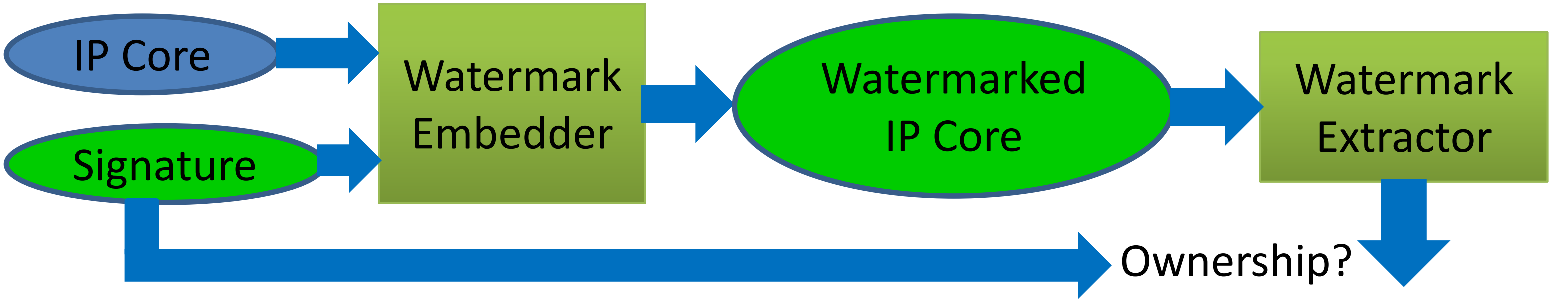
- No optimization done for embedding cost
- No optimization done for area
- Double variable signature approach

Optimization done for embedding cost
- Optimization done for hardware area
- Multi-variable signature approach

A. Sengupta et. al "Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis" , **IEEE Access Journal**, 2016

Watermarking for Hardware IP Protection

- A watermark is a signature of the owner embedded in a IP core.



- A watermark:
  - should be capable to identify the owner/creator of the design
  - should be robust and difficult to remove
  - should be resilient against attacks like: ghost signature and tampering
  - should have minimal embedding cost to obtain the watermarked design
  - should be embedded in the IP design with minimal computation effort
  - should be easy to detect signature for an entity who has full knowledge of the signature encoding rule

A. Sengupta et. al “Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)**, 2017

Properties of Watermark Generated

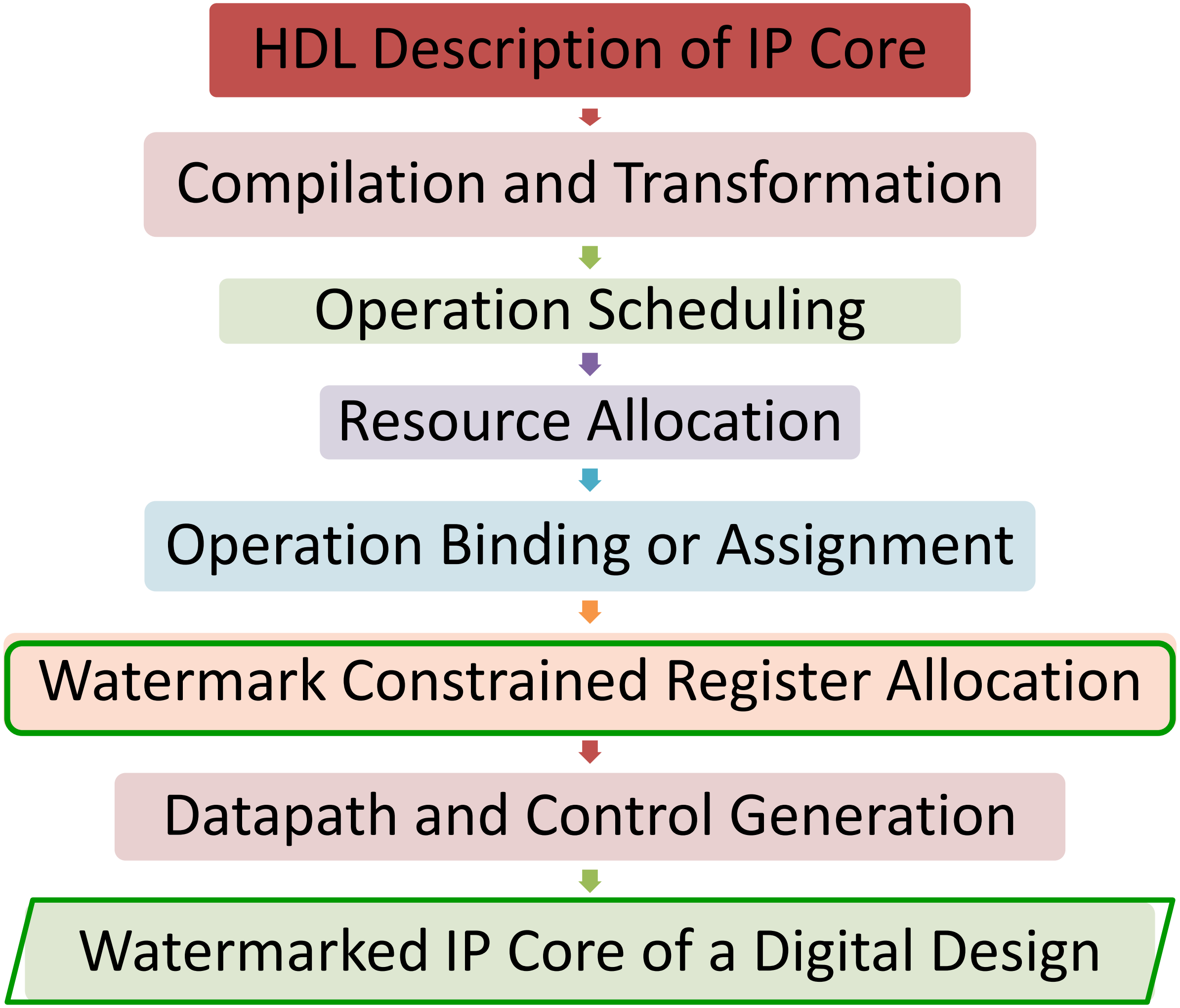
- Minimization of embedding cost
  - A solution is generated through PSO-driven exploration which considers minimization of hardware area and latency
- Resiliency against attacks
  - Generated watermark is based on multi-variable (4 variables) signature encoding therefore, it is resilient against attacks
- Fault Tolerance
  - The watermarking constraints are distributed throughout the design
- Watermark creation time and signature detection time
  - Time taken to embed a watermark is less

Watermark – At High-Level – Prior Works

- Limited literature on watermarking for IP protection at the high-level or behavioral synthesis phase of IP design cycle.
- Hong [1]: A combination of 0 and 1 is used to encode signature in the form of adding additional edges in the colored interval graph during HLS.
- Drawbacks of existing works:
    - signature is susceptible to attacks/compromise, if encoding rule of both the variable is known.
    - watermark has high embedding cost and high storage overhead.
- To advance the state-of-the art, a cost optimal watermark based on robust multi-variable signature encoding during HLS for reusable IP core protection is presented.

A. Sengupta et. al "Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis" , **IEEE Access Journal**, 2016

High-Level Synthesis Flow for IP Protection – A Simplified View



HDL Description of IP Core

Compilation and Transformation

Operation Scheduling

Resource Allocation

Operation Binding or Assignment

Watermark Constrained Register Allocation

Datapath and Control Generation

Watermarked IP Core of a Digital Design

A. Sengupta et. al “Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)** 2017

High-Level Synthesis of DSP core, Multimedia Cores etc (several examples….)

- **Example: Digital IIR Butterworth filter**

$$H(z) = \frac{Y(z)}{X(z)} = \left(\frac{16.5171z^3 + 49.5513z^2 + 49.5513z + 16.5171}{70.83z^3 + 31.1205z^2 + 27.2351z + 2.948}\right)$$
$$= \left(\frac{0.2332 + 0.4664z^{-1} + 0.4664z^{-2} + 0.2332z^{-3}}{1 + 0.4394z^{-1} + 0.3845z^{-2} + 0.0416z^{-3}}\right)$$

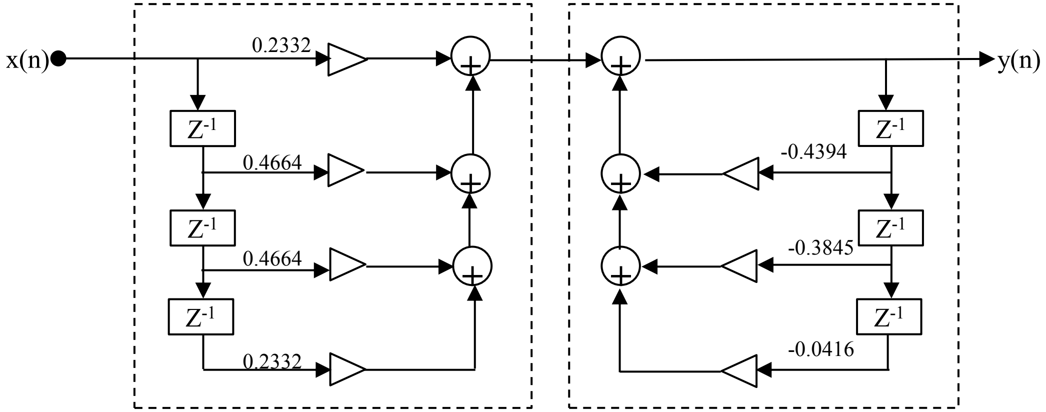
- **Example: FIR filter**

$$y(n) = \sum_{i=0}^{M} h_i * x(n-i)$$

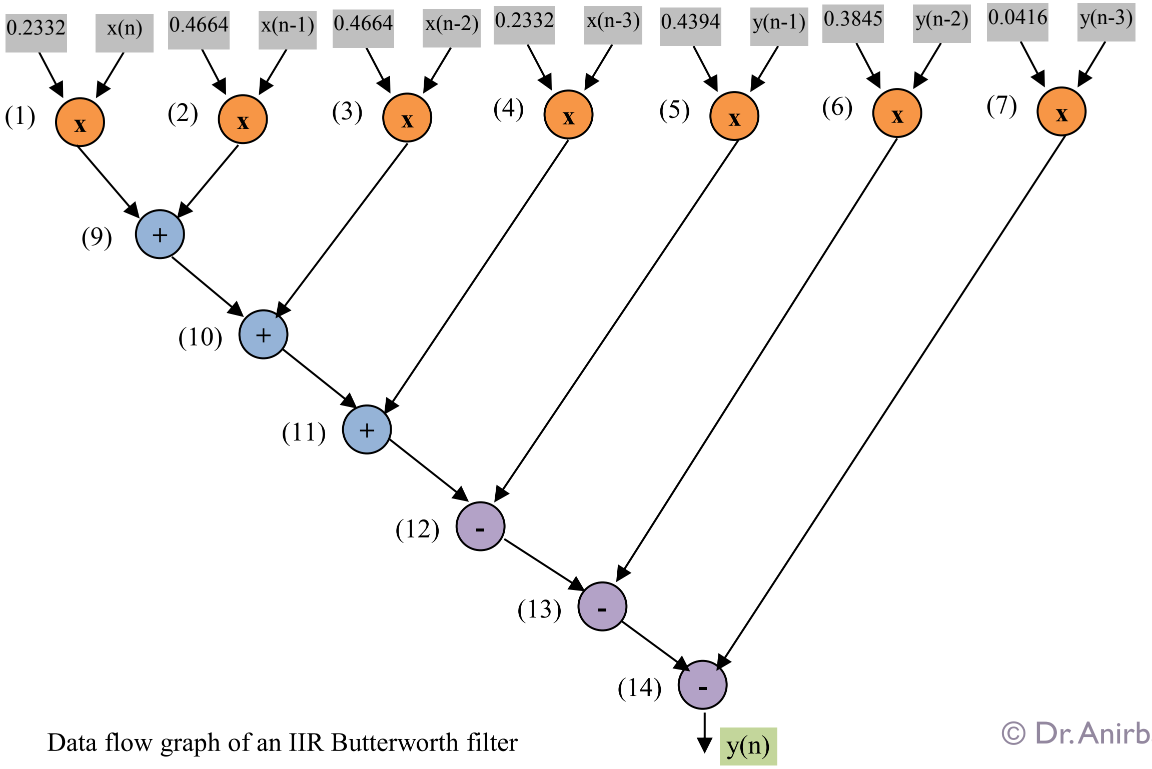
$$y(7) = h_0 * x(7) + h_1 * x(6) + h_2 * x(5) + h_3 * x(4) + h_4 * x(3) + h_5 * x(2) + h_6 * x(1) + h_7 * x(0)$$

- **Example: DCT and IDCT**
- **Example: FFT Algorithm**
- **Example: Low Pass Filter, other Filters**
- **Example: JPEG Compression and Decompression**
- **Example: Haar Wavelet Transformation for Image Compression**

DSP core- Digital IIR Butterworth filter



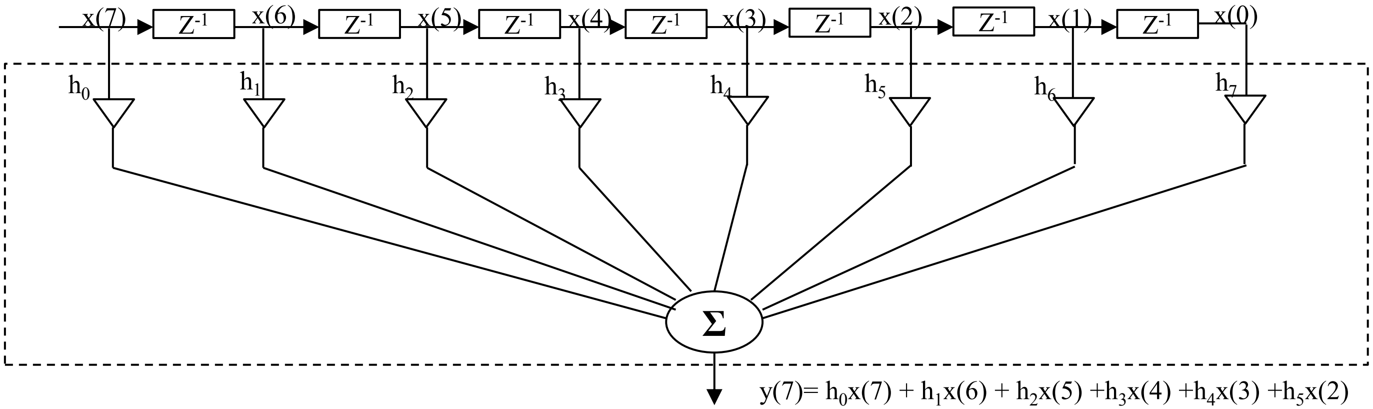
Block diagram of an IIR Butterworth filter



Data flow graph of an IIR Butterworth filter

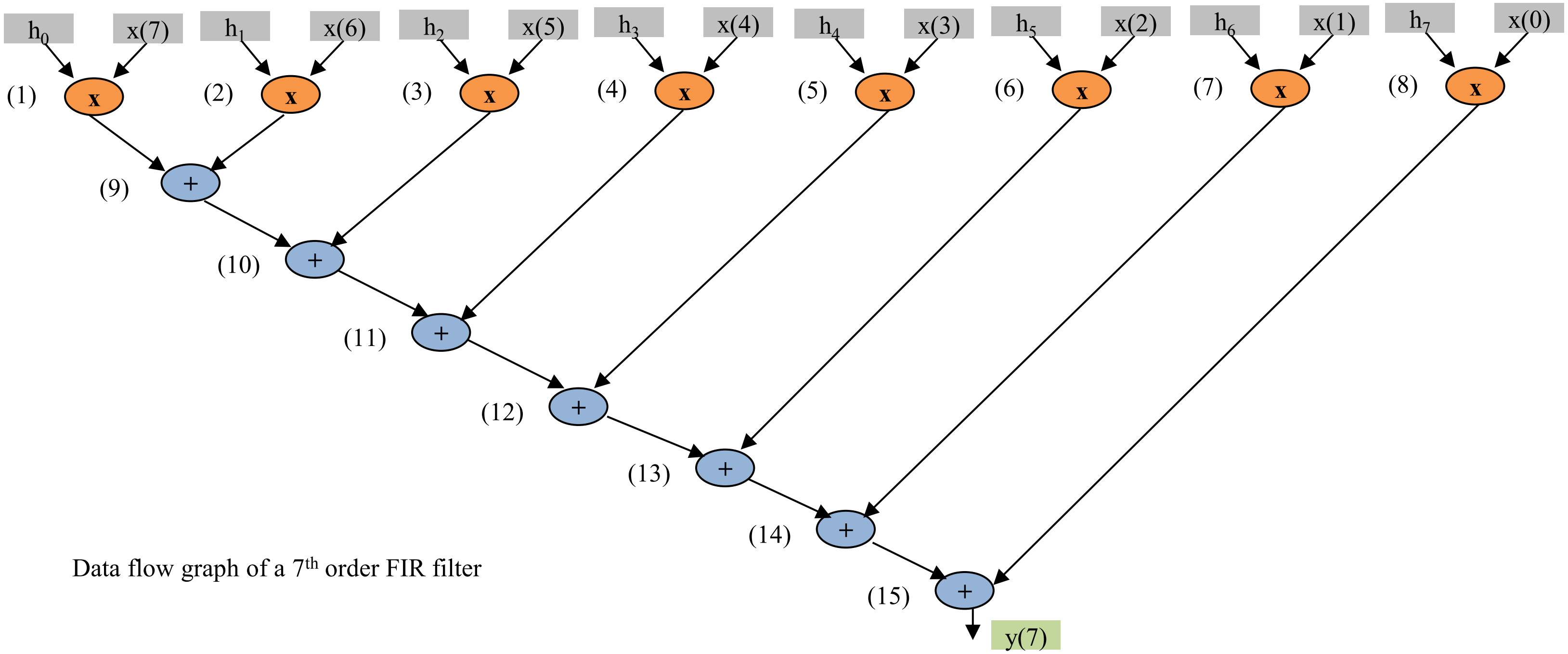
© Dr. Anirban Sengupta, IIT Indore

DSP core- FIR filter



$y(7)= h_0x(7) + h_1x(6) + h_2x(5) +h_3x(4) +h_4x(3) +h_5x(2) +h_6x(1) + h_7x(0)$

Block diagram of a 7th order FIR filter



Data flow graph of a 7th order FIR filter

A. Sengupta et al "Smart Electronic Systems for Consumer Electronics", **IEEE Transactions on Consumer Electronics,** 2018

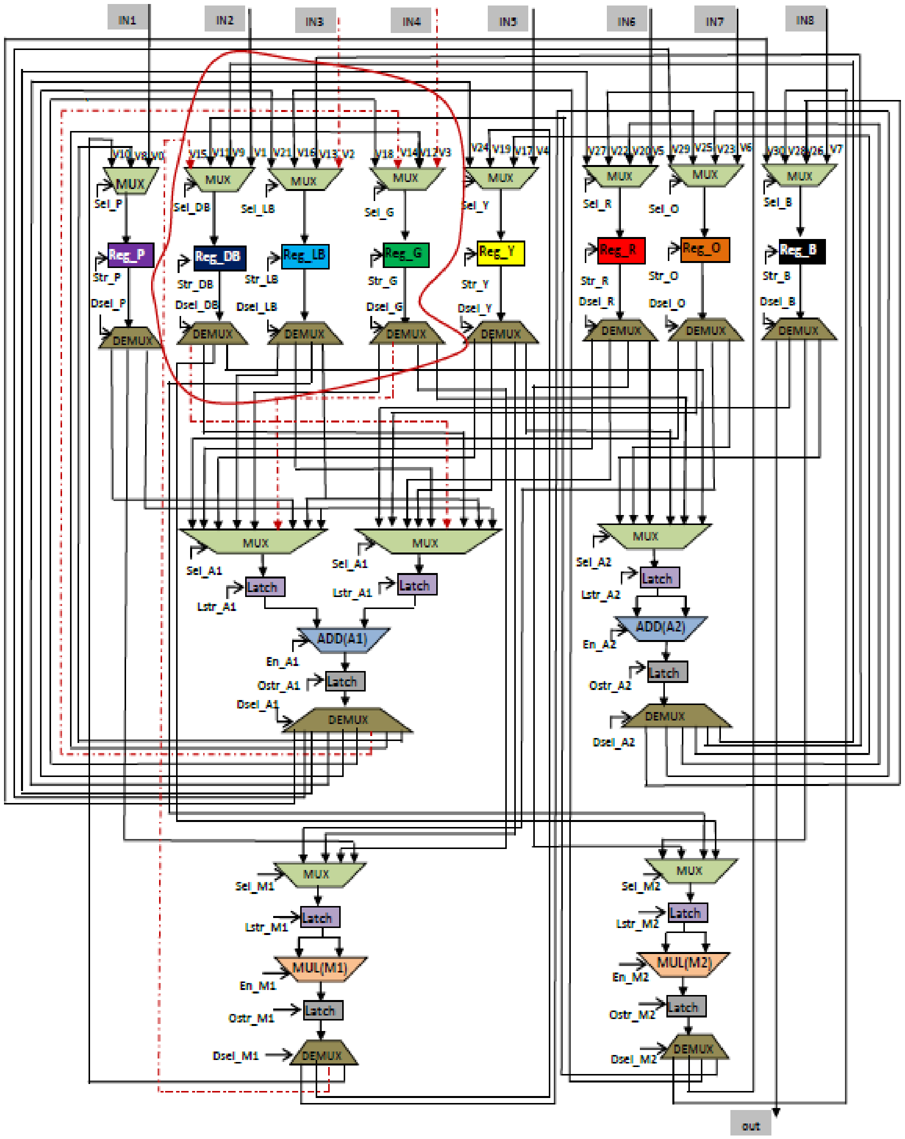
Watermarking …

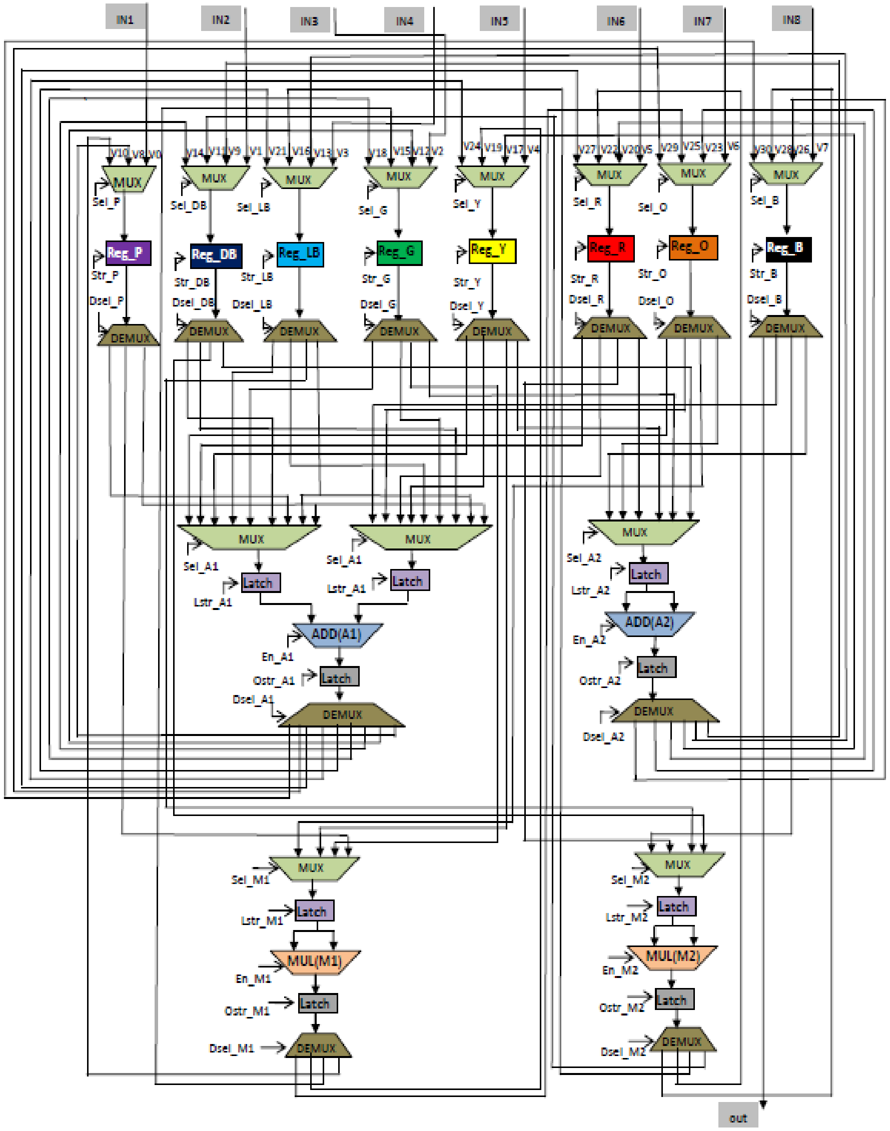
Process for embedding watermark in the design

- Schedule the CDFG based on resource configuration provided.
- Create the colored interval graph to find the minimum number of registers required for allocation.
- Generate a controller based on colored interval graph.
- Sort storage variables as per their number in increasing order.
- Generate a desired signature in the form of random combination of a tuple comprising of (*i, I, T, !*). Each variable of the generated signature maps onto a certain edge pair:
  - i = encoded value of edge with node pair as (prime, prime)
  - I = encoded value of edge with node pair as (even, even)
  - T = encoded value of edge with node pair as (odd, even)
  - ! = encoded value of edge with node pair as (0, any integer)

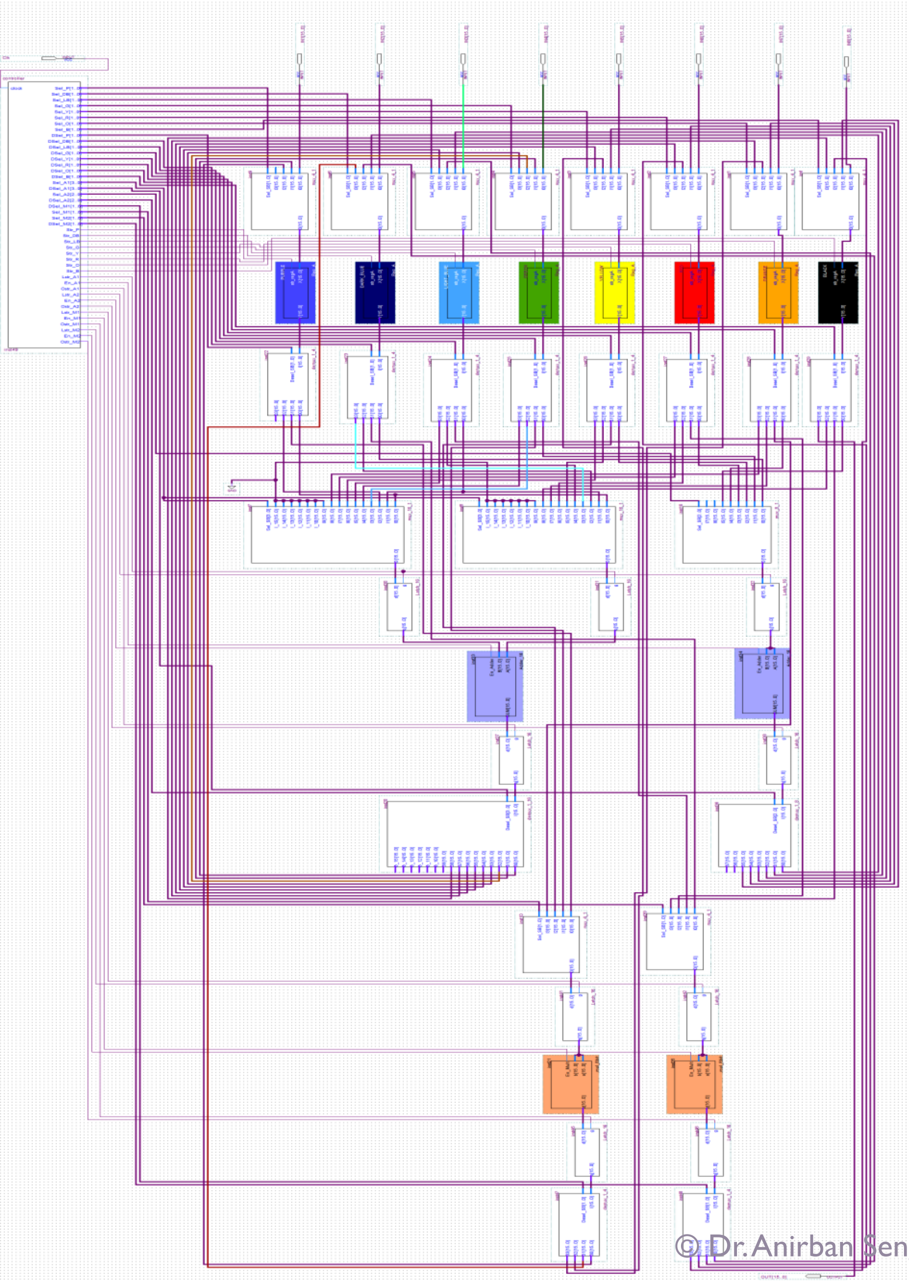
A. Sengupta et. al “Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)**, 2017

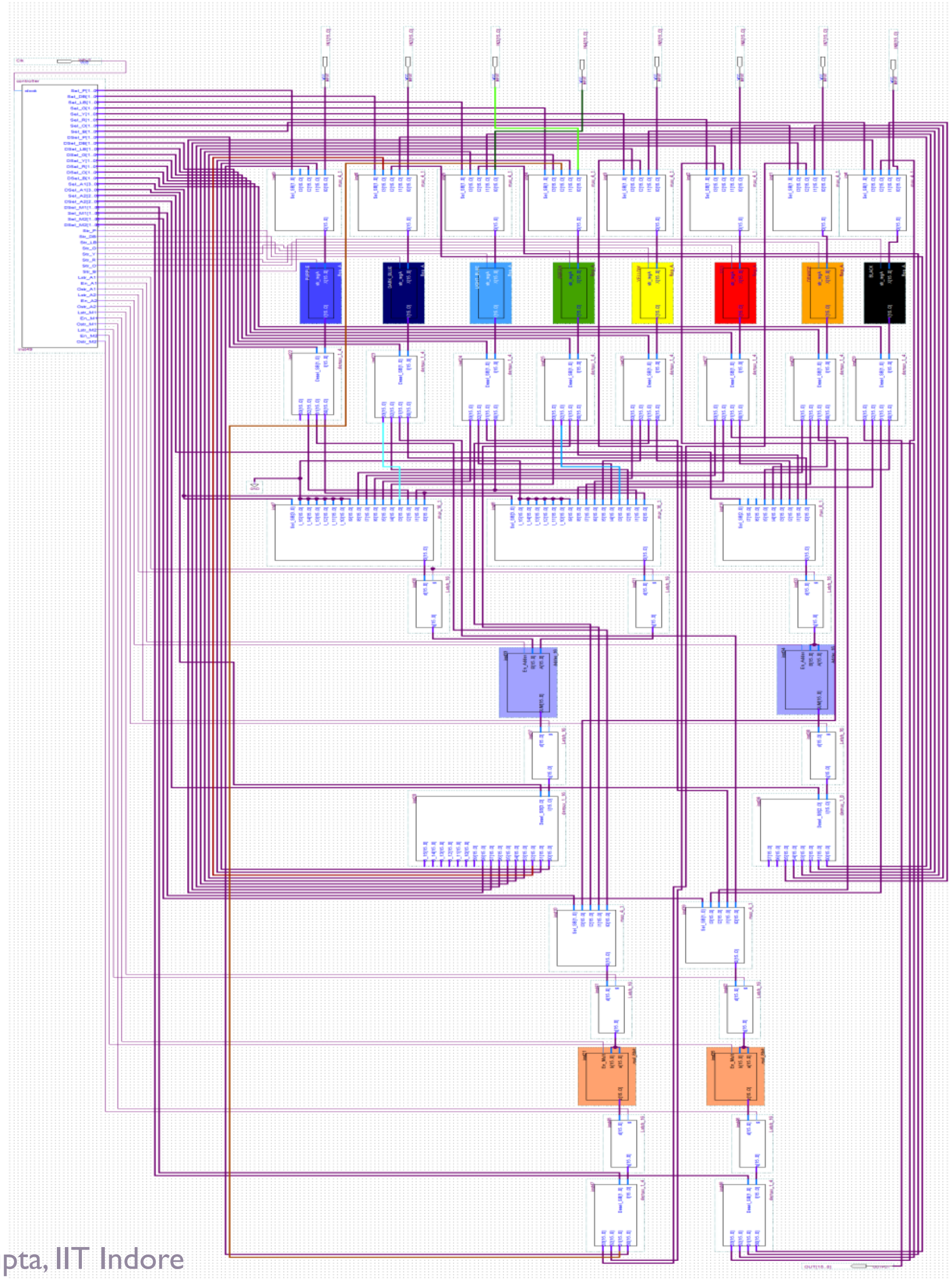
Another DSP Core: Watermarked FIR Vs Non-Watermarked FIR





Watermarked FIR Vs Non-Watermarked FIR at RTL (Altera Quartus)

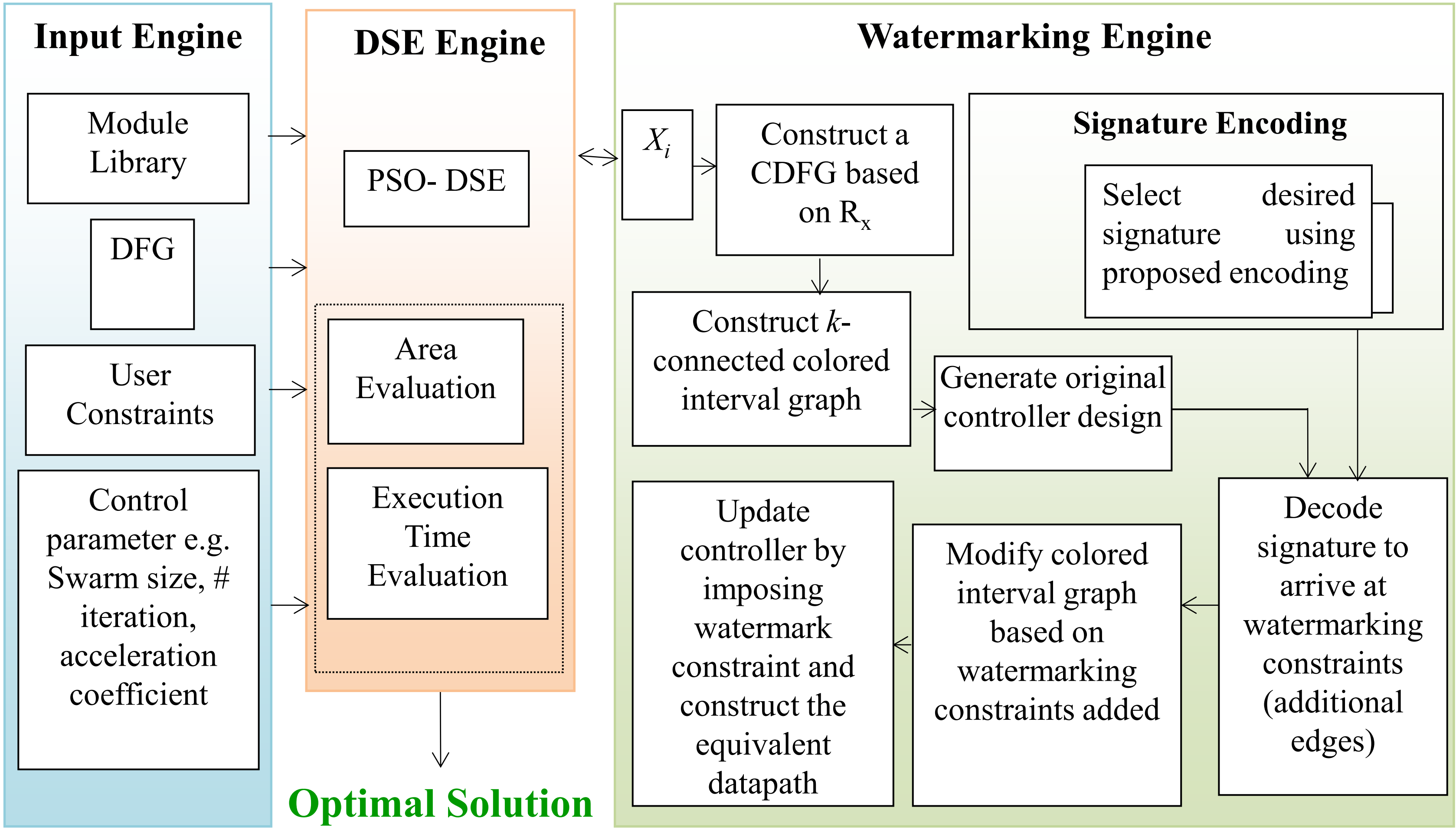




Motivation for Design Space Exploration (DSE) of Optimal Watermark

- Every solution impacts the latency and hardware area in a different way.
- Choosing a solution without performing trade-off affects the latency and area of the final IP core design.
- Before deciding a solution for inserting a watermark that yields lowest cost, many factors have to be considered.
- DSE process helps in identifying an optimal watermarked solution, which satisfies the user specified upper bounds of latency and hardware area as well as ensures that a low cost solution is found.

Particle Swarm Optimization (PSO) driven DSE for Optimal Watermark



Input Engine
Module Library
DFG
User Constraints
Control parameter e.g. Swarm size, # iteration, acceleration coefficient
DSE Engine
PSO- DSE
Area Evaluation
Execution Time Evaluation
Optimal Solution
Watermarking Engine
X_i
Construct a CDFG based on R_x
Construct *k*-connected colored interval graph
Generate original controller design
Signature Encoding
Select desired signature using proposed encoding
Decode signature to arrive at watermarking constraints (additional edges)
Modify colored interval graph based on watermarking constraints added
Update controller by imposing watermark constraint and construct the equivalent datapath

A. Sengupta et. al "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)**, 2017

Optimization Methodology

- Problem Formulation
  - Given a control data flow graph (CDFG), determine, optimal watermarked solution (X_i) = N(R_1), N(R_2),…N(R_D)

with minimum Hybrid $Cost(A_T, L_T)$

$$C_f(X_i) = W_1 \frac{L_T - L_{cons}}{L_{\max}} + W_2 \frac{A_T - A_{cons}}{A_{\max}}$$

Subjected to: $A_T \le A_{cons}$, $L_T \le L_{cons}$, and

w is # of watermarking constraint generated corresponding to a signature

A_T *and* L_T are area and delay of watermarked solutions

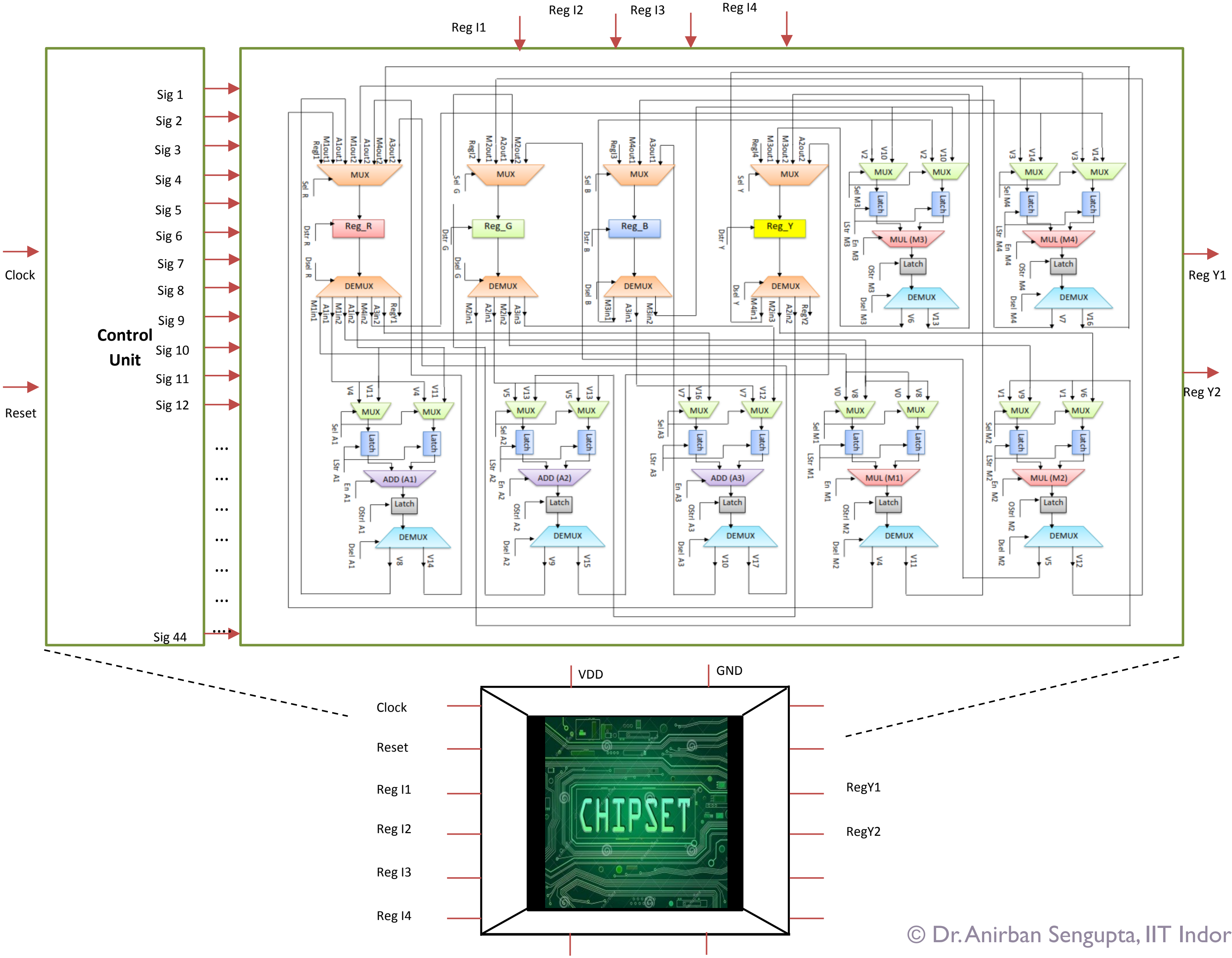
A_{max} *and* L_{max} correspond to solutions with maximum area and delay in the design space

W_1, W_2 are the user defined weights, e.g. both 0.5 for equal weightage

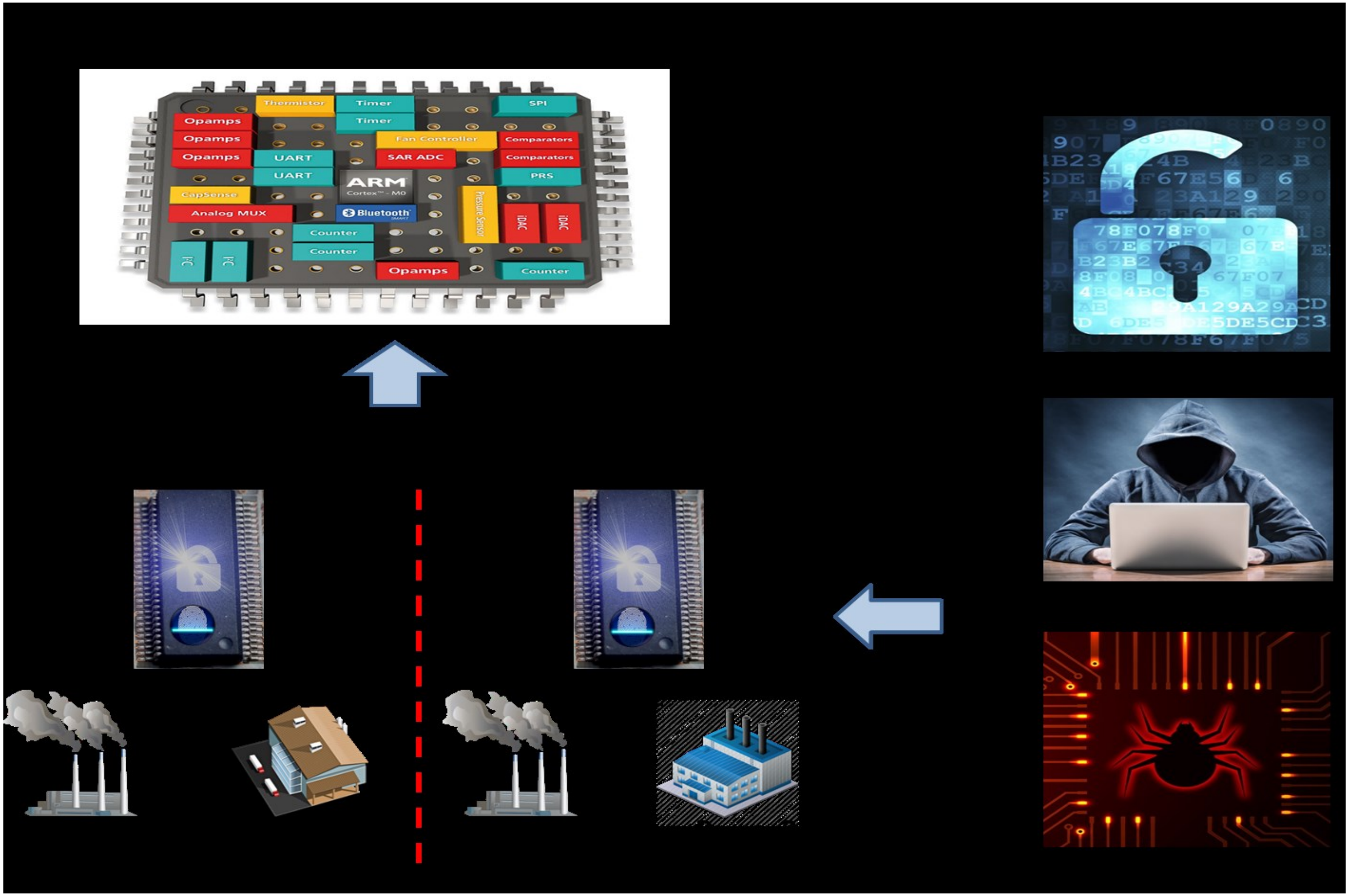
$N(R_D)$ is the number of a resource type R_D

A. Sengupta et. al "Low Cost Security Aware High Level Synthesis Methodology", **IET Journal on Computers & Digital Techniques (CDT)**, 2016

Final watermarked (anti-piracy aware) IP chipset: Another DSP ore



Symmetrical IP Core Protection



A. Sengupta et. al "Low Overhead Symmetrical Protection of Reusable IP Core using Robust Fingerprinting and Watermarking during High Level Synthesis", **Elsevier Journal on Future Generation Computer Systems**, 2017

Motivation of symmetrical protection

- From the IP providers' standpoint, embedding watermark is not enough to discourage piracy and unauthorized redistribution, the buyer's legal ownership of a given piece of IP must symmetrically be protected as well.
- The IP provider desires the ability to trace a dishonest buyer from unauthorized resold copies of the IP. It is crucial for IP provider to distribute IPs with the same functionality but different appearance to different users.
- Symmetric protection of the provider's and buyer's rights is afforded by a fingerprinting methodology, whereby the IP provider fingerprints and delivers to each buyer a unique copy of functionally identical IP.

The main challenge in IP fingerprinting is how to implement the same IP, functionality-wise, in many different ways to accommodate the potential IP user market. **Therefore, we require fingerprinting process that can provide a number of distinct versions of the same IP core with a reasonable amortized design effort.**

Courtesy: Q. Gang, M. Potkonjak, "Intellectual Property Protection in VLSI Designs: Theory and Practice", Springer Science & Business Media, 2007.

Symmetrical IP Core Protection

- What is symmetrical IP core protection?
  - Seller and watermark.
  - Buyer and fingerprint.
- Why symmetrical IP core protection?
  - Tracing illegally resold/redistributed copies of a reusable IP core.
  - Piracy/forgery.
  - False claim of ownership.
- Why symmetrical IP core protection during HLS?
  - To meet the time to market demand.
  - Performance optimization.
  - Protects higher level as well as lower level designs.

A. Sengupta et. al "Low Overhead Symmetrical Protection of Reusable IP Core using Robust Fingerprinting and Watermarking during High Level Synthesis", **Elsevier Journal on Future Generation Computer Systems**, 2017

Desired properties of signature

- Low embedding cost overhead
- Resiliency against attacks
- Fault tolerance
- Adaptability to any CAD Tool
- Signature creation and detection time
- Preserve correctness and functionalities

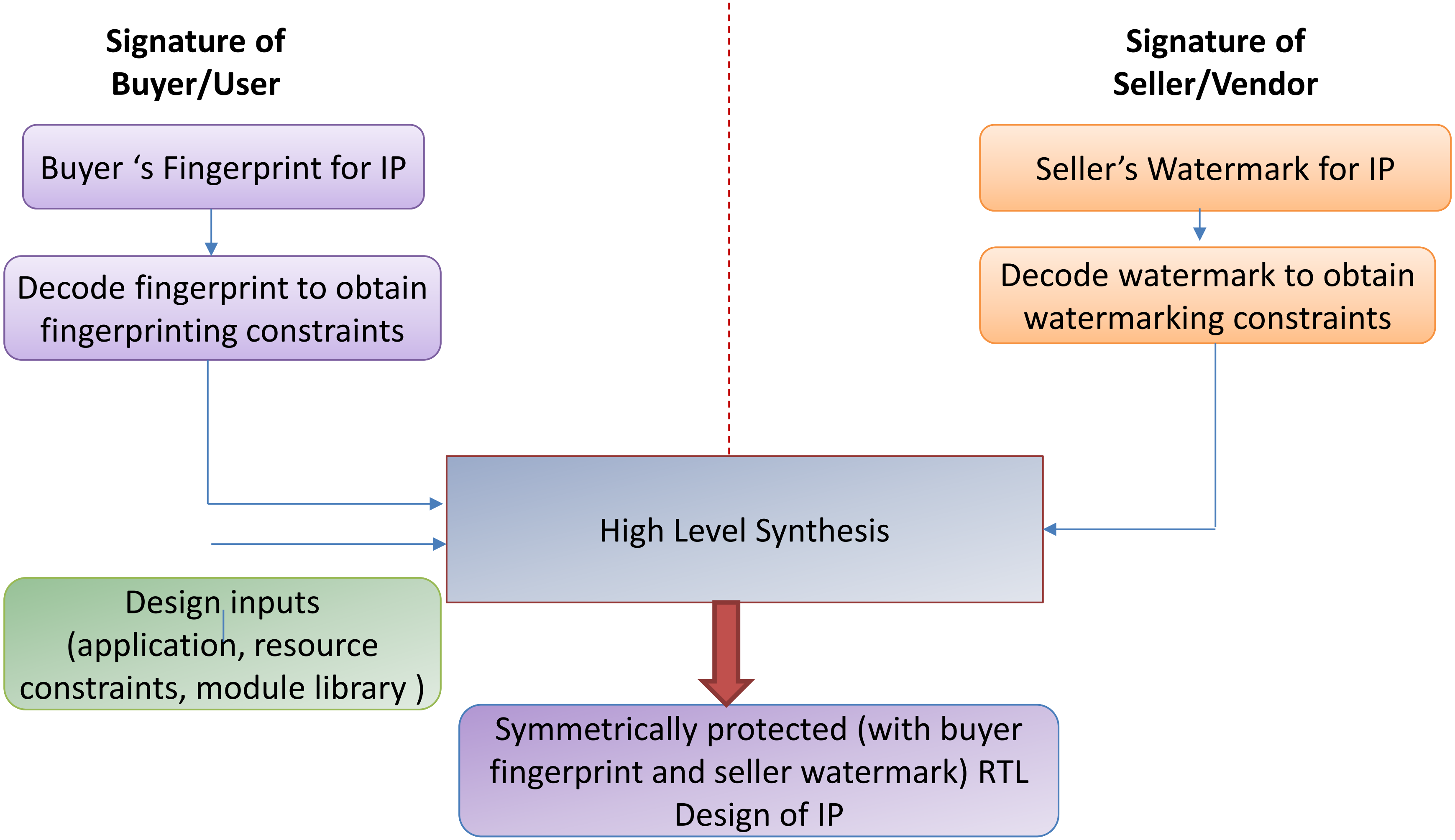
A. Sengupta et. al "Low Overhead Symmetrical Protection of Reusable IP Core using Robust Fingerprinting and Watermarking during High Level Synthesis", **Elsevier Journal on Future Generation Computer Systems**, 2017

Solution: Symmetrical IP Core

- Proposes multi-variable fingerprinting methodology during scheduling and register allocation phases of HLS.
- Proposes symmetrical IP core protection methodology first-time during HLS.
- Proposes symmetrical IP core protection with extremely low design overhead.
- Offers higher robustness, lower embedding cost, fault tolerance and faster signature encoding/decoding.

A. Sengupta et. al "Low Overhead Symmetrical Protection of Reusable IP Core using Robust Fingerprinting and Watermarking during High Level Synthesis", **Elsevier Journal on Future Generation Computer Systems**, 2017

Symmetrical IP core Protection

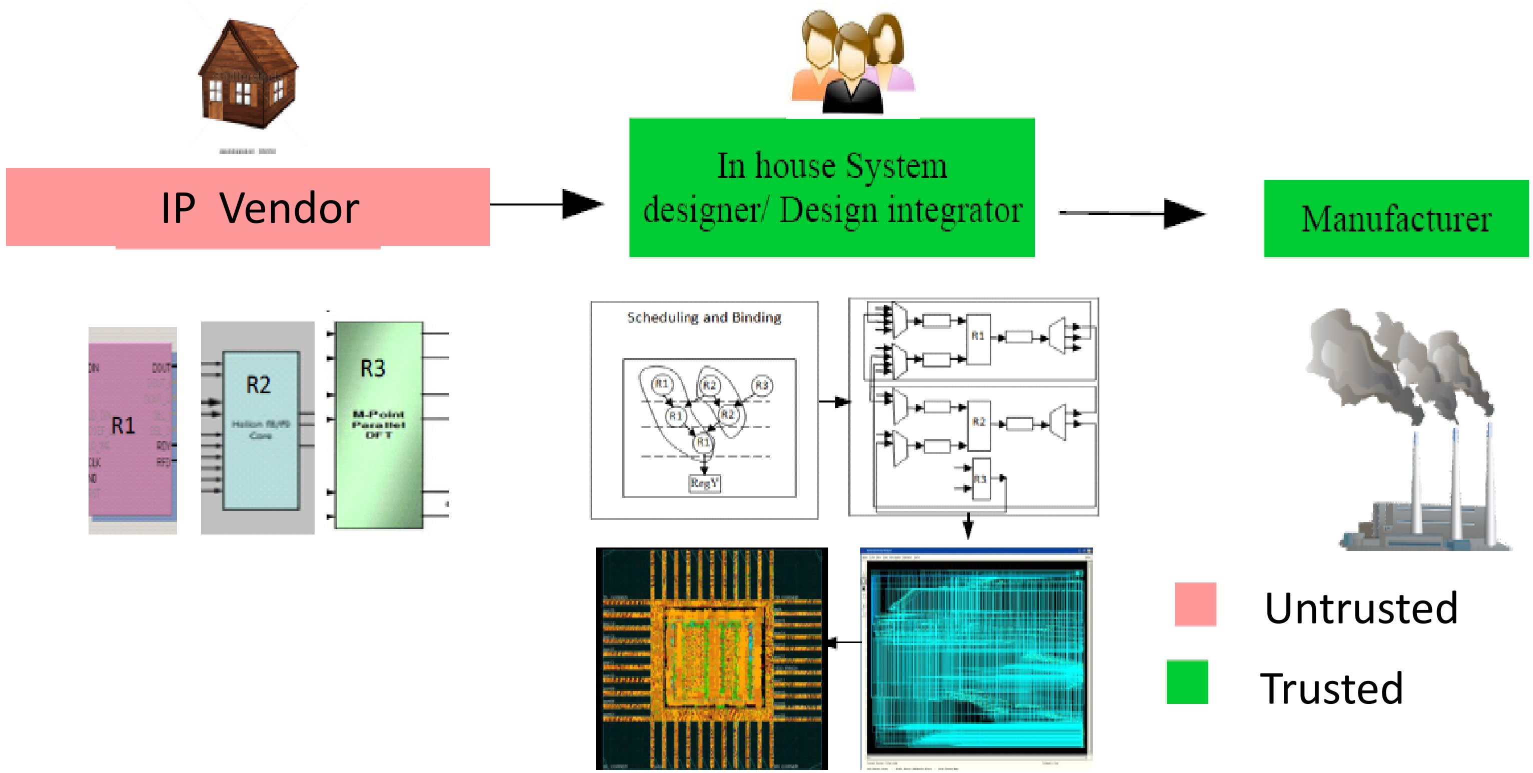

Signature of Buyer/User
Signature of Seller/Vendor
Buyer ‘s Fingerprint for IP
Seller’s Watermark for IP
Decode fingerprint to obtain fingerprinting constraints
Decode watermark to obtain watermarking constraints
High Level Synthesis
Design inputs (application, resource constraints, module library)
Symmetrically protected (with buyer fingerprint and seller watermark) RTL Design of IP

A. Sengupta et al "Multi-Phase Watermark for IP Core Protection", ***Proc. 36th IEEE International Conference on Consumer Electronics (ICCE) 2018***, Las Vegas, Jan 2018

IP Core design flow

- Due to globalization of design supply chain, possibility of intervention and attacks on IP cores is on the rise

  → mandates protection of IP cores from piracy/counterfeiting even at early stage of design flow



IP Vendor

In house System designer/ Design integrator

Manufacturer

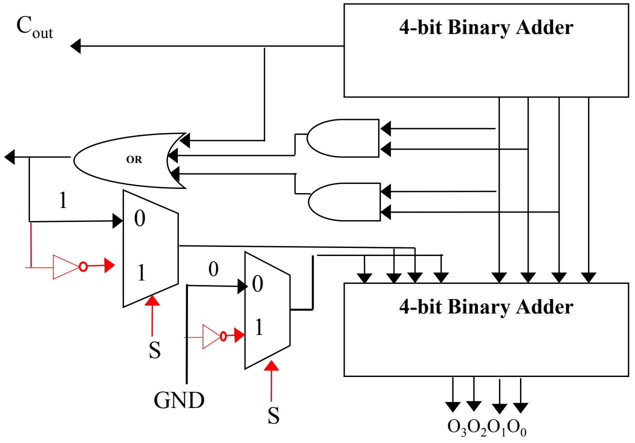
🟥 Untrusted

🟩 Trusted

A. Sengupta et. al "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor during High Level Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)**, 2016

IP Trojan: Security

- What is a Trojan?
  - Malicious modification of an IC.
  - Trigger and payload.
  - External activation (antennas or sensors) or internal activation (FSM or counters).
- What are the different types of Trojan?
  - rare value triggered
  - time-triggered
- How a Trojan can be inserted?
  - Through third party IP (3PIP) cores.



BCD Adder

- How to achieve Trojan secure design?
  - Dual Modular Redundant (DMR) schedule during HLS.

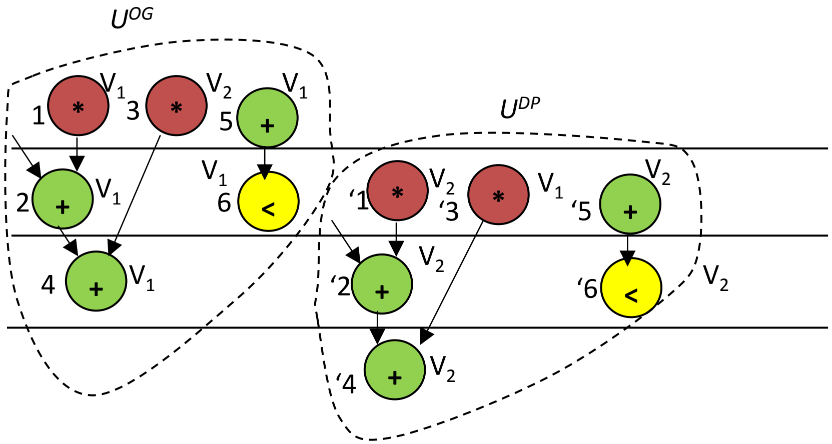
A. Sengupta et. al Low cost optimized Trojan secured schedule at behavioral level for single & Nested loop control data flow graphs, **Elsevier VLSI Integration**, 2016

IP core Trojan Detection Rules

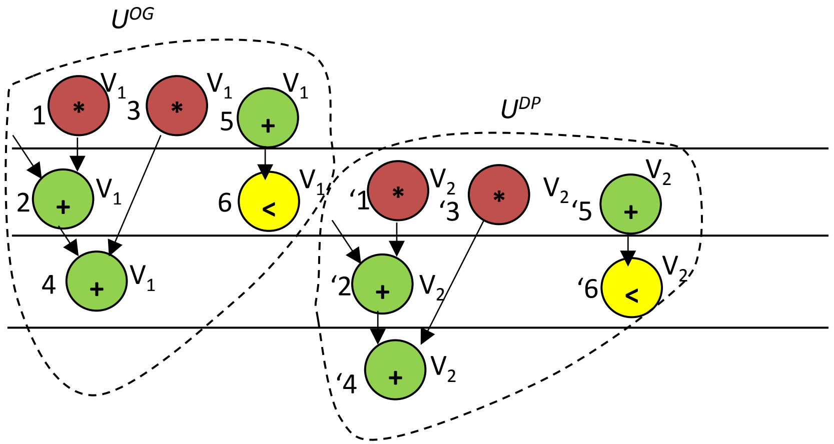
- **Rule 1**: Vendor allocation procedure (Type 1): A_v = 00
  - Alternate vendor assignment to operations in control step of a unit.
  - Similar operations of both U^{OG} and U^{DP} being assigned to different vendors.
- **Rule 2**: Vendor allocation procedure (Type 2): A_v = 01
  - All operations of a specific unit being assigned to resources of same vendor type.
  - Similar operations of both original unit (U^{OG}) and duplicate unit (U^{DP}) being assigned to different vendors.
- **Rule 3**: Vendor allocation procedure (Type 3): A_v = 10
  - All operations within critical path of a specific unit being strictly assigned to a vendor type while all operations of non critical path through alternate vendor type.
  - Operations of critical path of U^{OG} and U^{DP} are assigned to distinct vendors.
  - Similar operations of non critical path in both U^{OG} and U^{DP} being assigned to different vendors.
- **Rule 4**: Vendor allocation procedure (Type 4): A_v = 11
  - Alternate vendor assignment to operations belonging to subsequent unrolled loop iterations within a unit.
  - Similar operations of unrolled loop iteration in both U^{OG} and U^{DP} assigned to different vendors.

A. Sengupta et. al "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor during High Level Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)**, 2016

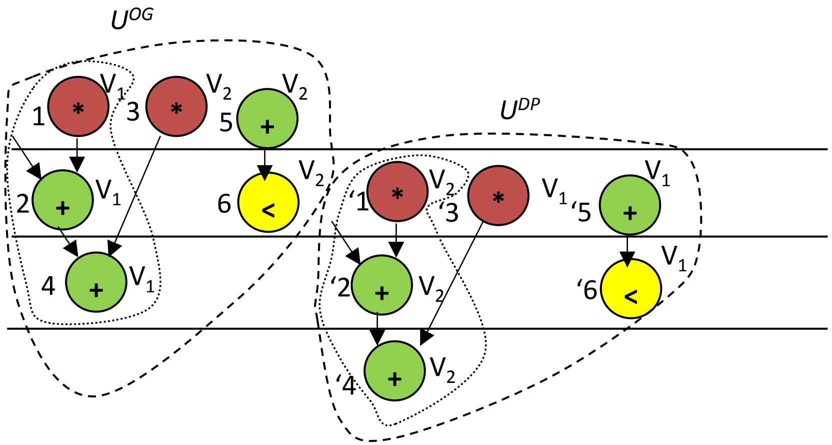
Example to Secure an IP core



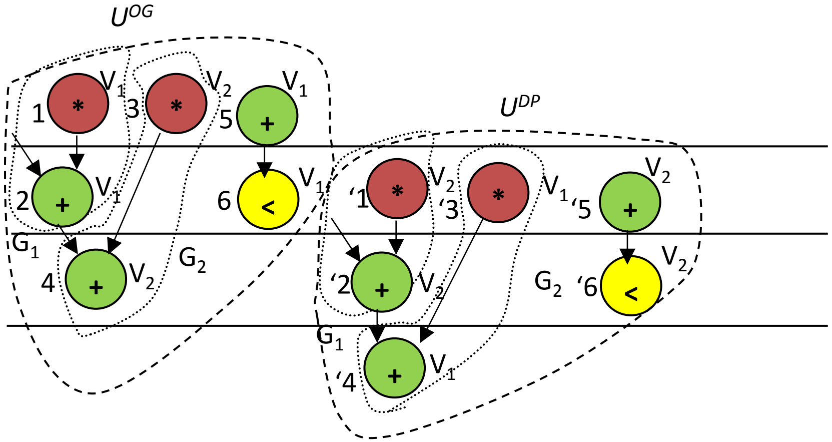
Scheduling and Binding of FIR for X_i = 2(+), 2(*), 2(<), U=2, I=4
based on Vendor Allocation Mode A_v = 00;
T_E^{DMR} = 45080 ns and A_T^{DMR} = 13064 au



Scheduling and Binding of FIR for X_i = 2(+), 2(*), 2(<), U=2, I=4
based on Vendor Allocation Mode A_v = 01;
T_E^{DMR} = 43080 ns and A_T^{DMR} = 17996 au



Scheduling and Binding of FIR for X_i = 2(+), 2(*), 2(<), U=2, I=4
based on Vendor Allocation Mode A_v = 10;
T_E^{DMR} = 45080 ns and A_T^{DMR} = 13064 au



Scheduling and Binding of FIR for X_i = 2(+), 2(*), 2(<), U=2, I=4
based on Vendor Allocation Mode A_v = 11;
T_E^{DMR} = 45070 ns and A_T^{DMR} = 15096 au

A. Sengupta et. al "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor during High Level Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD)**, 2016

References

- Sengupta, D. Roy, and S. P. Mohanty, “Triple-phase watermarking for reusable IP core protection during architecture synthesis,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 37, no. 4, pp. 742– 755, Apr. 2018.
- A. Sengupta, E. R. Kumar, and N. P. Chandra, “Embedding digital signature using encrypted-hashing for protection of DSP Cores in CE,” IEEE Trans. Consum. Electron., vol. 65, no. 3, pp. 398–407, Aug. 2019.
- M. Rathor and A. Sengupta, “IP core steganography using switch based key-driven hash-chaining and encoding for securing DSP kernels used in CE systems,” IEEE Trans. Consum. Electron., vol. 66, no. 3, pp. 251–260, Aug. 2020.
- A. Sengupta et al., “DSP design protection in CE through algorithmic transformation based structural obfuscation,” IEEE Trans. Consum. Electron., vol. 63, no. 4, pp. 467–476, Nov. 2017.
- A. Sengupta, D. Kachave, and D. Roy, “Low cost functional obfuscation of reusable IP cores used in CE hardware through robust locking,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 38, no. 4, pp. 604–616, Apr. 2019.
- A. Sengupta, S. Bhadauria, and S. P. Mohanty, “Embedding low cost optimal watermark during high level synthesis for reusable IP core protection,” in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), Montreal, QC, Canada, May 2016, pp. 974–977.
- Anirban Sengupta, Saumya Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis", IEEE Access, Volume:4, Issue: 99, pp. 2198 - 2215, May 2016
- Anirban Sengupta, Saumya Bhadauria, Saraju P Mohanty "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor during High Level Synthesis", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 36, Issue: 4, April 2017, pp. 655 – 668
- 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
- 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
- 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