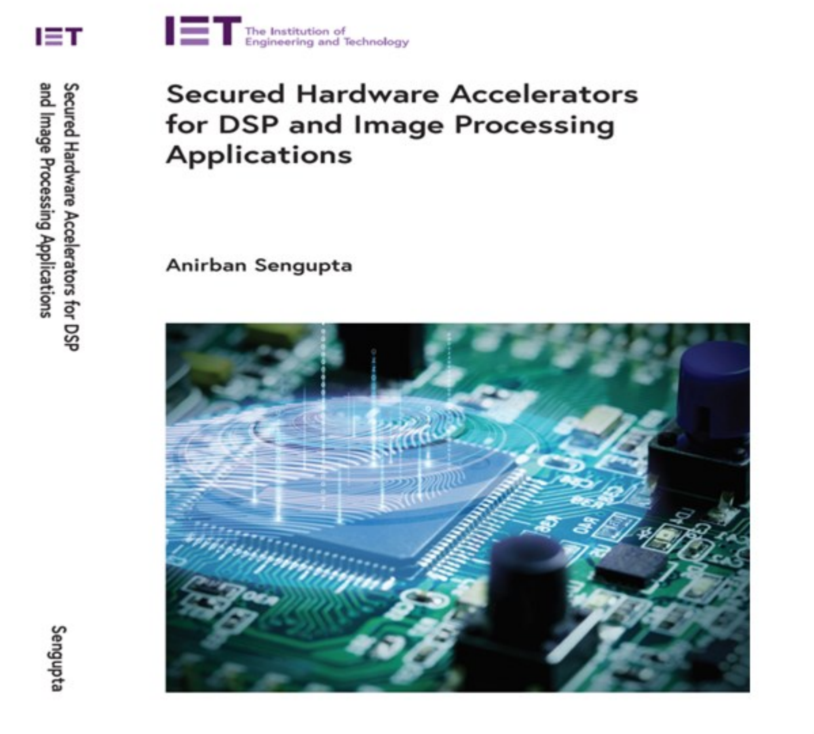
Amrita Vishwa Vidyapeetham, Kerala

Nov 30, 2022

Hardware Security and IP Core Protection (IPP)

DR. ANIRBAN SENGUPTA, ASSOC. PROFESSOR
FIET (UK), FBCS (UK), FIETE
IEEE Distinguished Visitor and IEEE Distinguished Lecturer
IEEE Senior Member
Board Member, IEEE Consumer Technology Society Technical Committee (TC)
Chair, IEEE Consumer Technology Society Technical Committee on Security & Privacy (TC-SPC)
Founder & Advisor, IEEE Consumer Technology Society- MP Chapter
Advisor, Executive Comm.- IEEE Computer Society MP Section
Former Chair, IEEE Computer Society Technical Committee on VLSI (TC-VLSI)
Former Chair, IEEE Consumer Technology Society Bombay Chapter
Deputy Editor-in-Chief, IET Computers and Digital Techniques (CDT)
Associate Editor, IEEE Transactions on VLSI (TVLSI)
Associate Editor, IEEE Transactions on Consumer Electronics (TCE)
Associate Editor, IEEE Transactions on Aerospace & Electronic Systems (TAES)
Former Editor-in-Chief, IEEE VLSI Circuits & Systems Letter (IEEE Computer Society TCVLSI)
Computer Science and Engineering
Indian Institute of Technology Indore
Email: asengupt@iiti.ac.in
Web: http://www.anirban-sengupta.com

BOOKS


IET The Institution of Engineering and Technology

Secured Hardware Accelerators for DSP and Image Processing Applications

Anirban Sengupta

Secured Hardware Accelerators for DSP and Image Processing Applications

Sengupta

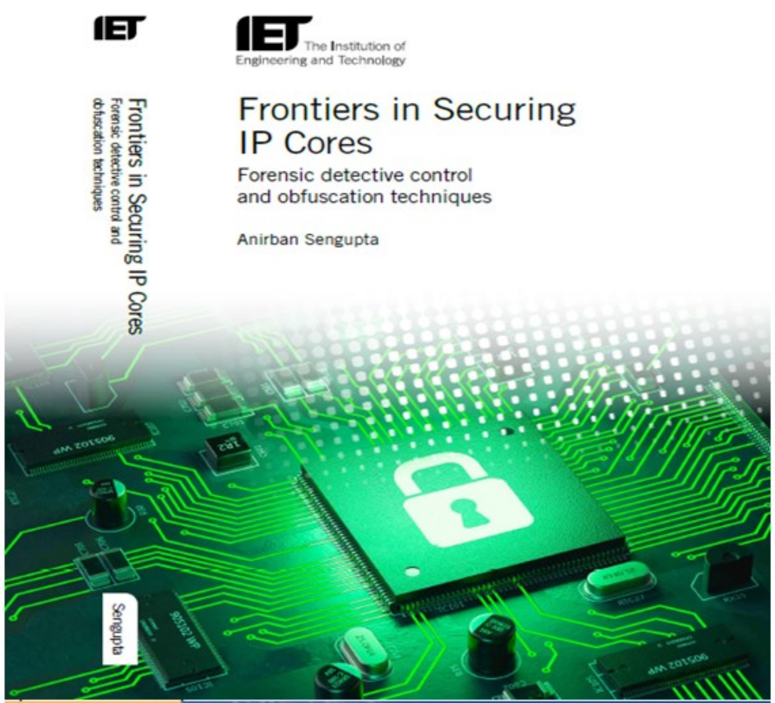
IET The Institution of Engineering and Technology

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Anirban Sengupta and Saraju P. Mohanty

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Sengupta and Mohanty


IET The Institution of Engineering and Technology

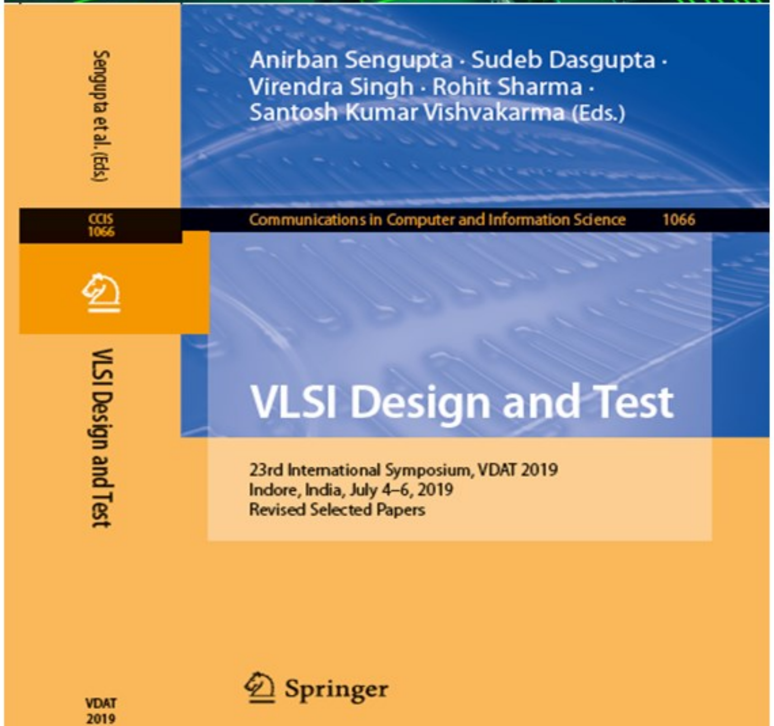
Frontiers in Securing IP Cores

Forensic detective control and obfuscation techniques

Anirban Sengupta

Frontiers in Securing IP Cores Forensic detective control and obfuscation techniques

Sengupta


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

Sengupta et al. (Eds.)

CCIS 1066

VLSI Design and Test

VDAT 2019

DR. ANIRBAN SENGUPTA

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.

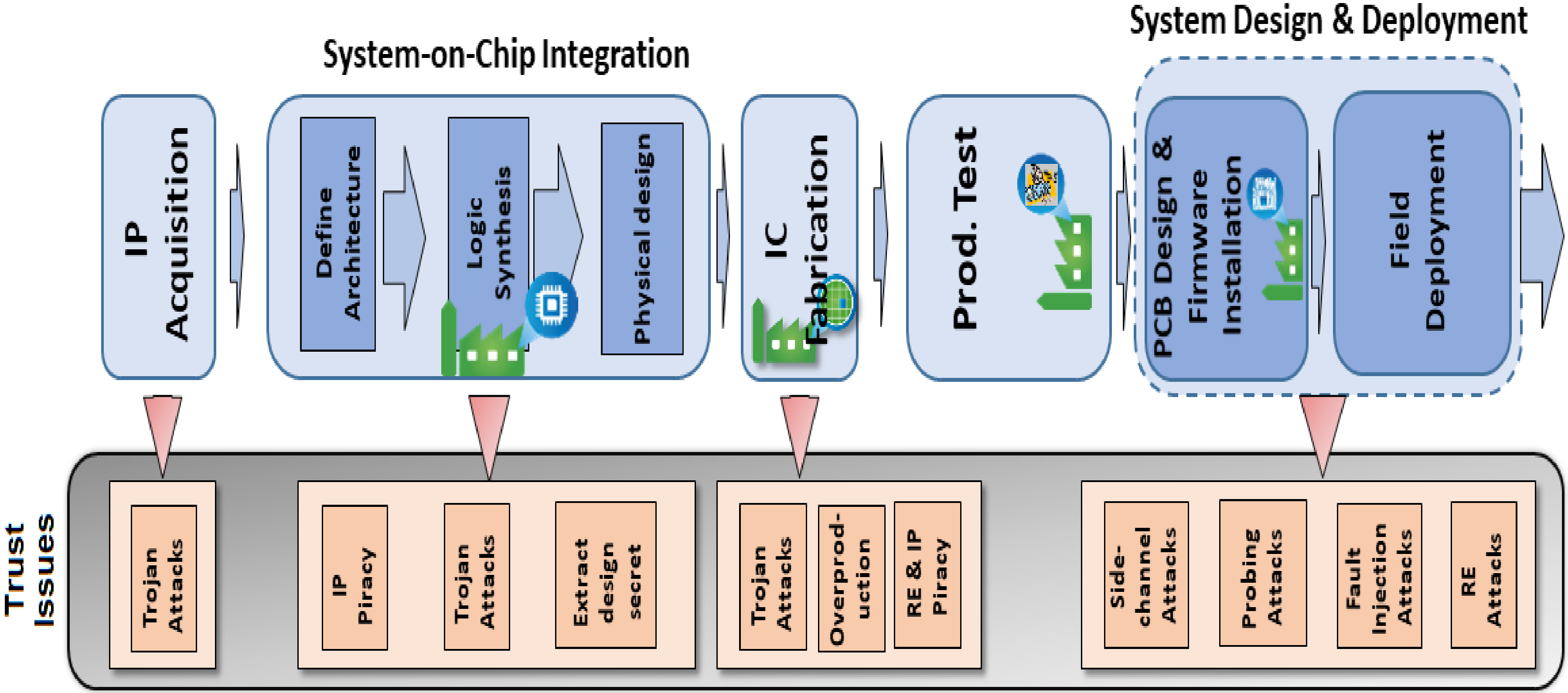
- Hardware security is broadly classified into two types: (a) authentication based approaches (b) obfuscation based approaches.

- 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 "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**, 2019

IP Core Protection and Hardware Security



System-on-Chip Integration

System Design & Deployment

IP Acquisition

Define Architecture

Logic Synthesis

Physical design

IC Fabrication

Prod. Test

PCB Design & Firmware Installation

Field Deployment

Trust Issues

Trojan Attacks

IP Piracy

Trojan Attacks

Extract design secret

Trojan Attacks

Overprod-uction

RE & IP Piracy

Side-channel Attacks

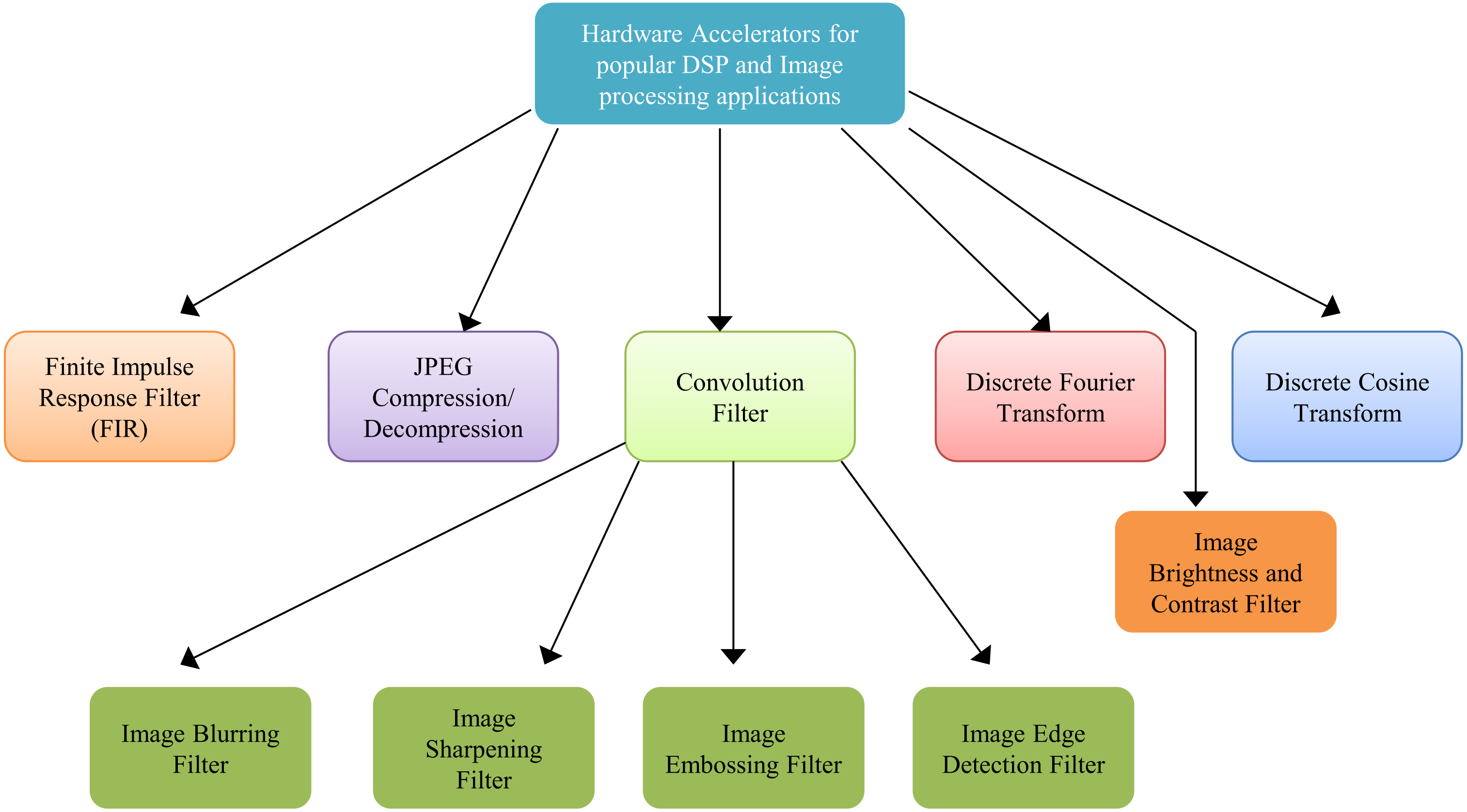
Probing Attacks

Fault Injection Attacks

RE Attacks

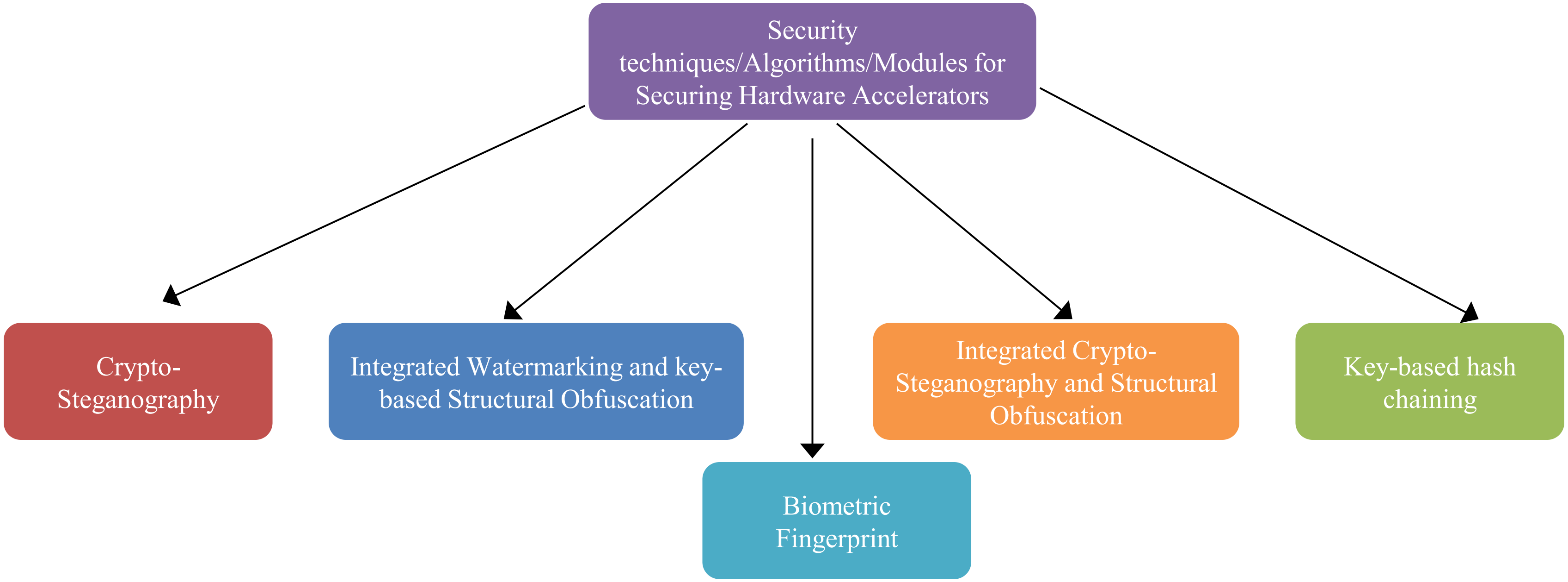
CAD for Assurance – CAD for Assurance of Electronic Systems

Hardware accelerators: Example


Hardware Accelerators for popular DSP and Image processing applications
Finite Impulse Response Filter (FIR)
JPEG Compression/ Decompression
Convolution Filter
Discrete Fourier Transform
Discrete Cosine Transform
Image Brightness and Contrast Filter
Image Blurring Filter
Image Sharpening Filter
Image Embossing Filter
Image Edge Detection Filter

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

Hardware security techniques for securing hardware accelerators



Security techniques/Algorithms/Modules for Securing Hardware Accelerators

Crypto-Steganography

Integrated Watermarking and key-based Structural Obfuscation

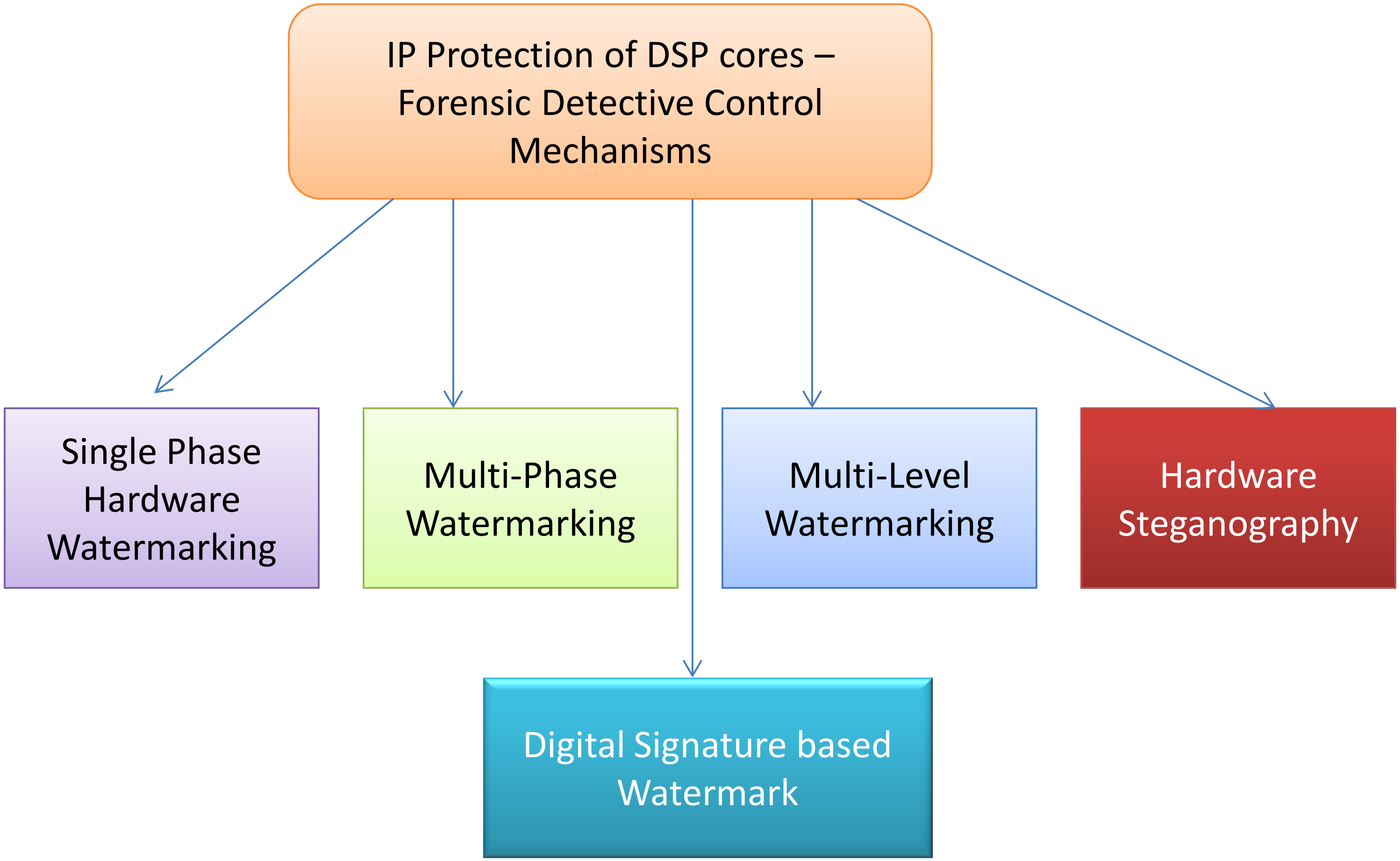
Biometric Fingerprint

Integrated Crypto-Steganography and Structural Obfuscation

Key-based hash chaining

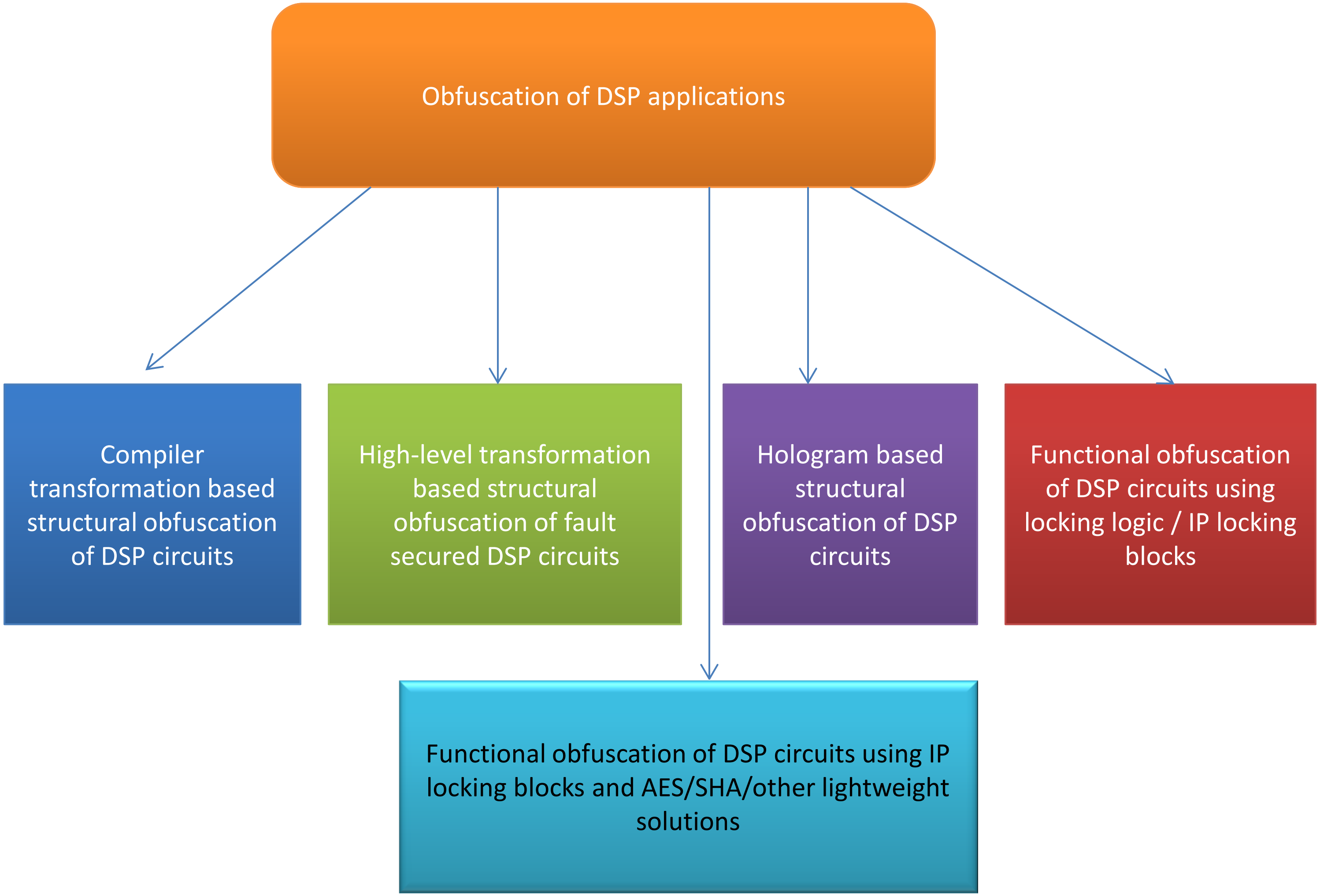
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

IP Protection of DSP cores – Forensic Detective Control Mechanisms


IP Protection of DSP cores – Forensic Detective Control Mechanisms
Single Phase Hardware Watermarking
Multi-Phase Watermarking
Multi-Level Watermarking
Hardware Steganography
Digital Signature based Watermark

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

Hardware Security of DSP applications using Obfuscation



Obfuscation of DSP applications

Compiler transformation based structural obfuscation of DSP circuits

High-level transformation based structural obfuscation of fault secured DSP circuits

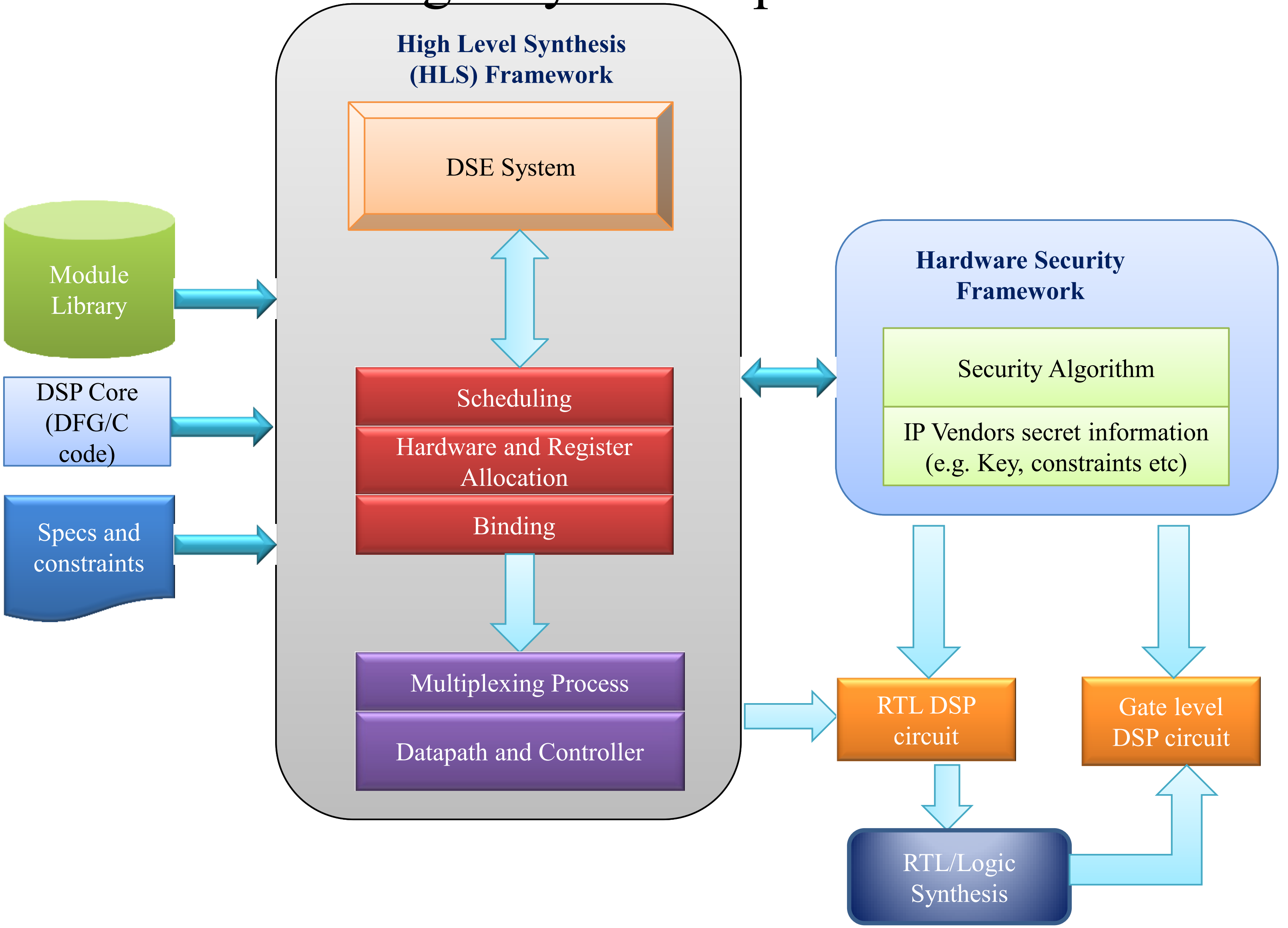
Hologram based structural obfuscation of DSP circuits

Functional obfuscation of DSP circuits using locking logic / IP locking blocks

Functional obfuscation of DSP circuits using IP locking blocks and AES/SHA/other lightweight solutions

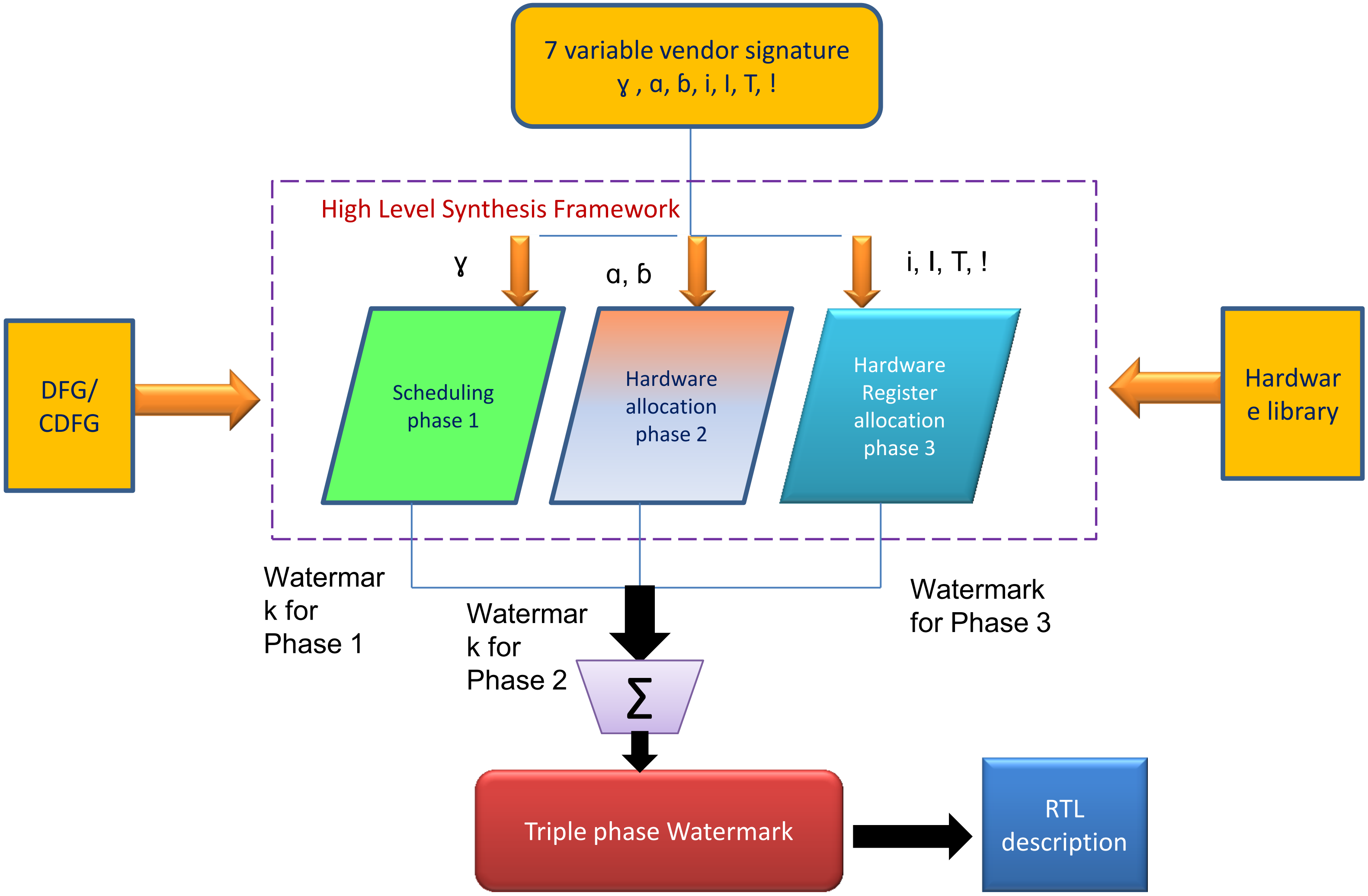
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Hardware Security Algorithms integrated with HLS and Logic Synthesis phases



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

High level overview of triple phase watermarking



7 variable vendor signature
ɣ , ɑ, ɓ, i, I, T, !

High Level Synthesis Framework

ɣ

ɑ, ɓ

i, I, T, !

DFG/
CDFG

Scheduling
phase 1

Hardware
allocation
phase 2

Hardware
Register
allocation
phase 3

Hardwar
e library

Watermar
k for
Phase 1

Watermar
k for
Phase 2

Watermark
for Phase 3

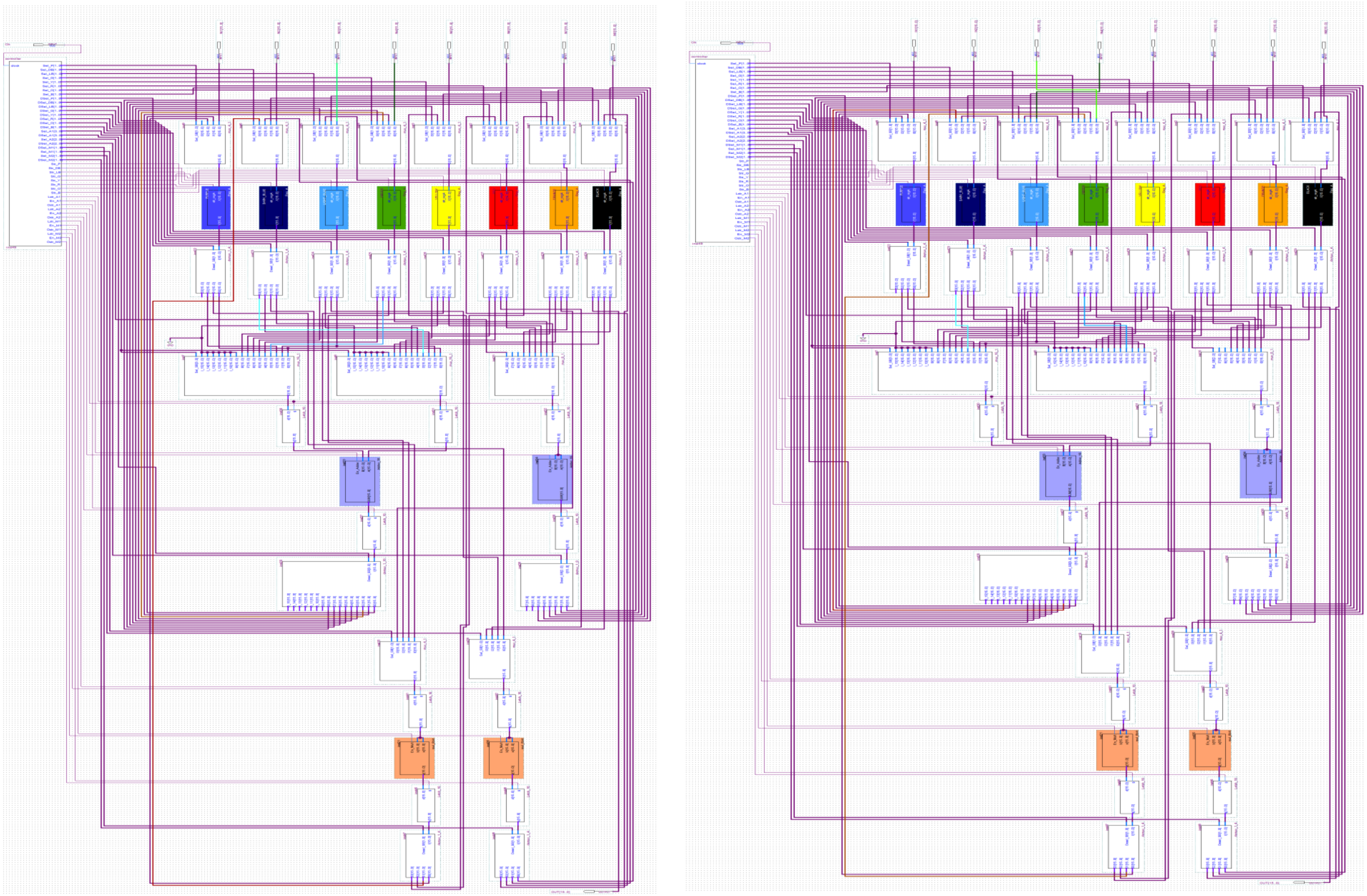
∑

Triple phase Watermark

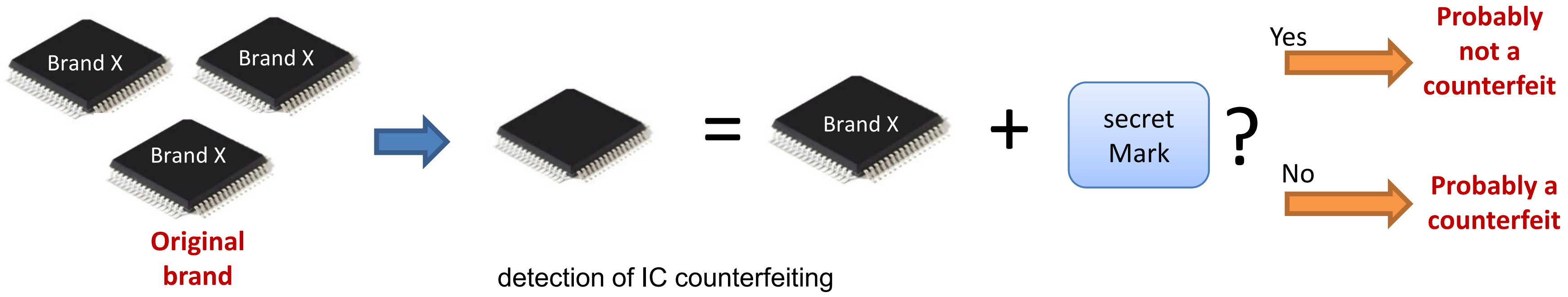
RTL
description

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

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



Brand X

Brand X

Brand X

Original brand

=

Brand X

+

secret Mark

?

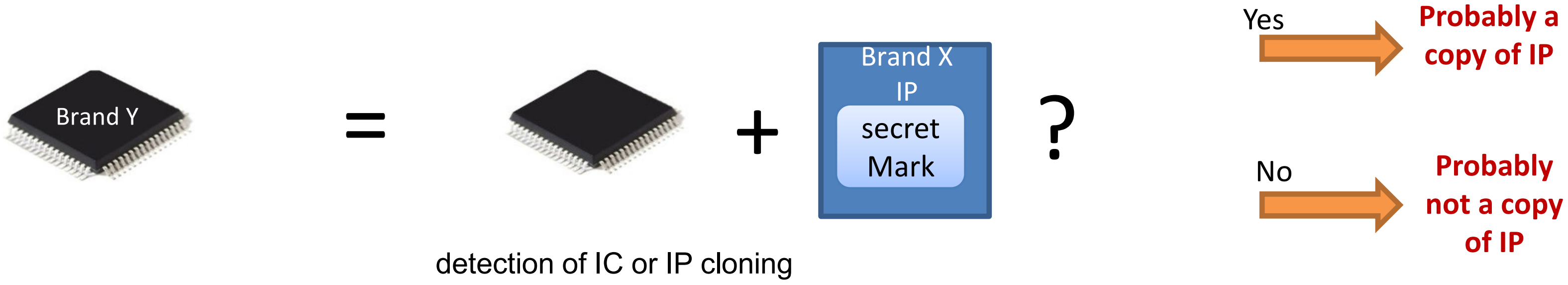
Yes

Probably not a counterfeit

No

Probably a counterfeit

detection of IC counterfeiting



Brand Y

=

+

Brand X IP

secret Mark

?

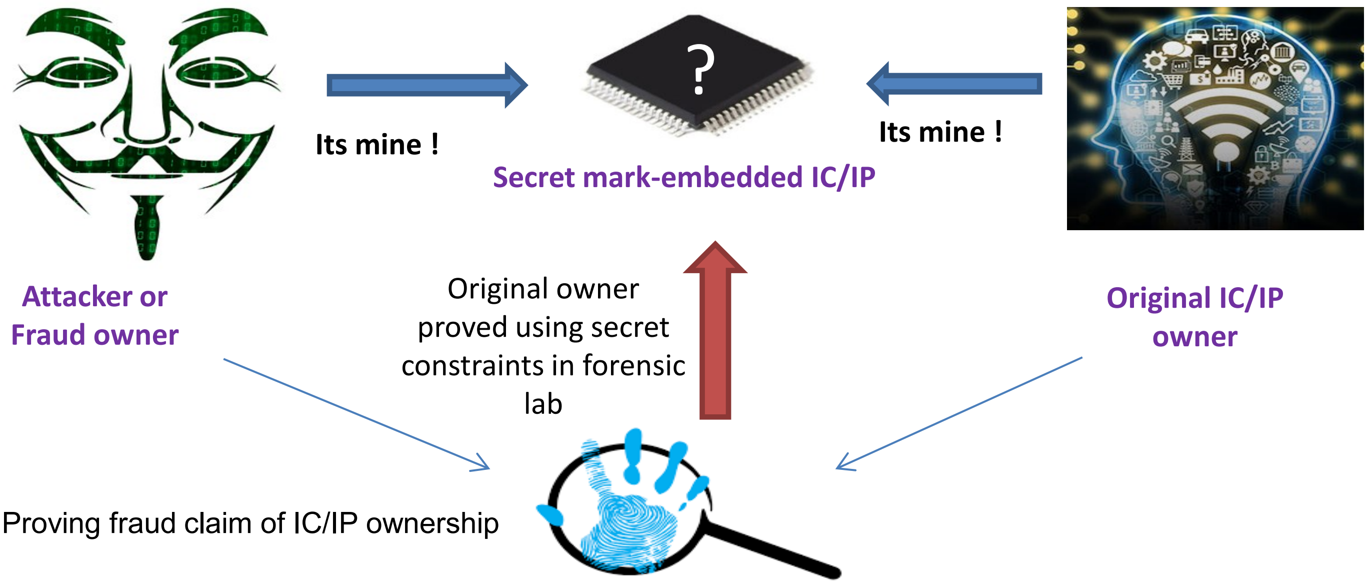
Yes

Probably a copy of IP

No

Probably not a copy of IP

detection of IC or IP cloning



Its mine !

?

Its mine !

Secret mark-embedded IC/IP

Attacker or Fraud owner

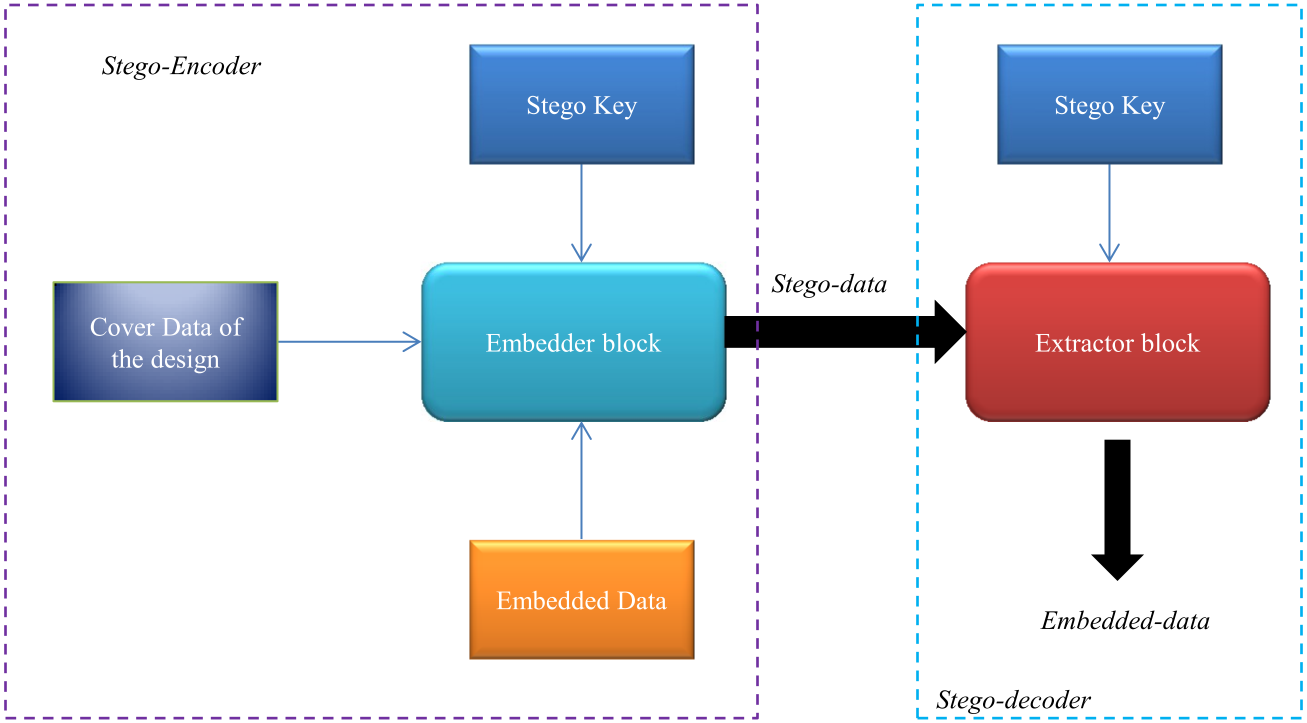
Original owner proved using secret constraints in forensic lab

Original IC/IP owner

Proving fraud claim of IC/IP ownership

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

Basic Steganography Model

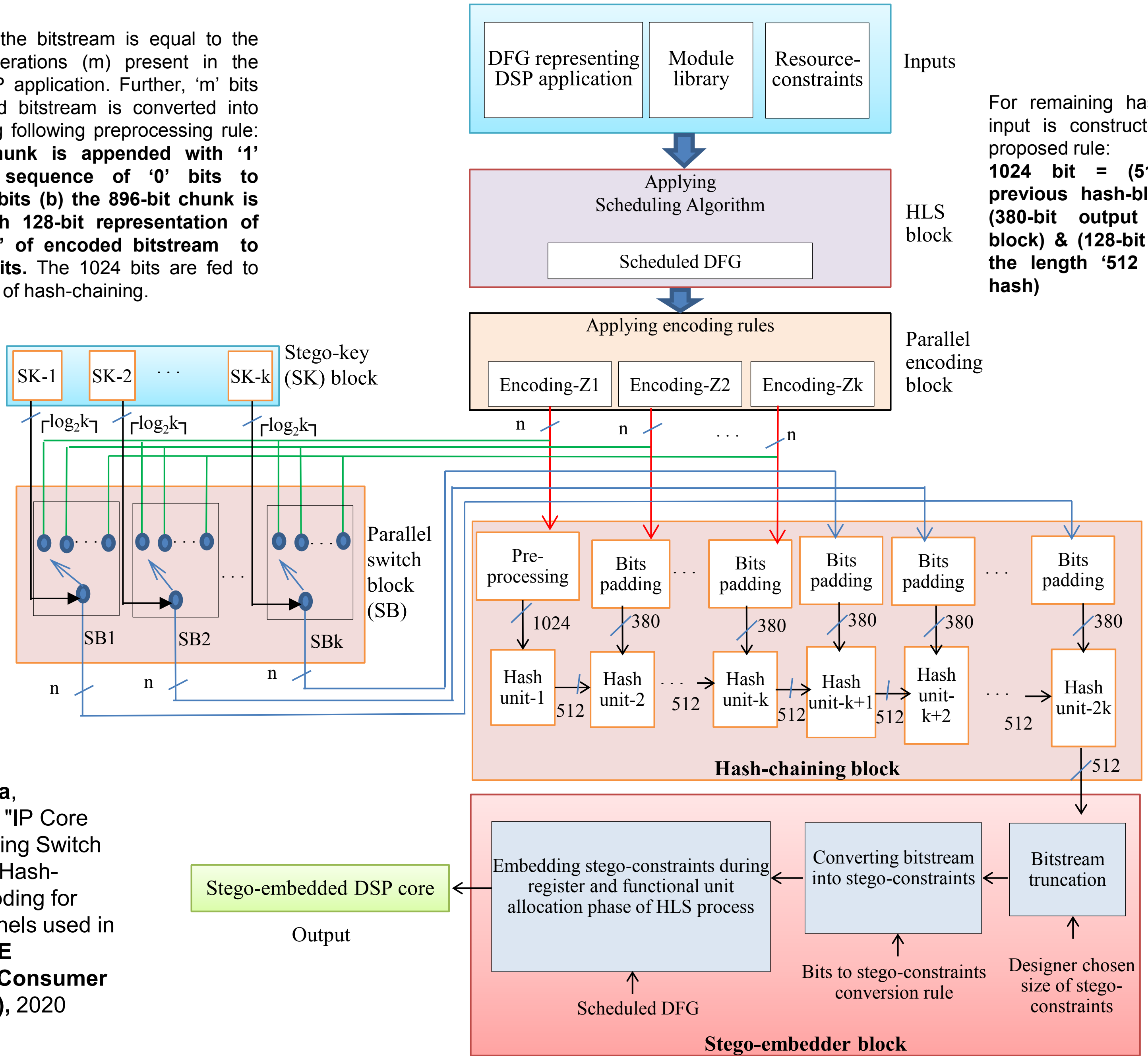


Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

Securing DSP cores using key-triggered hash-chaining based steganography

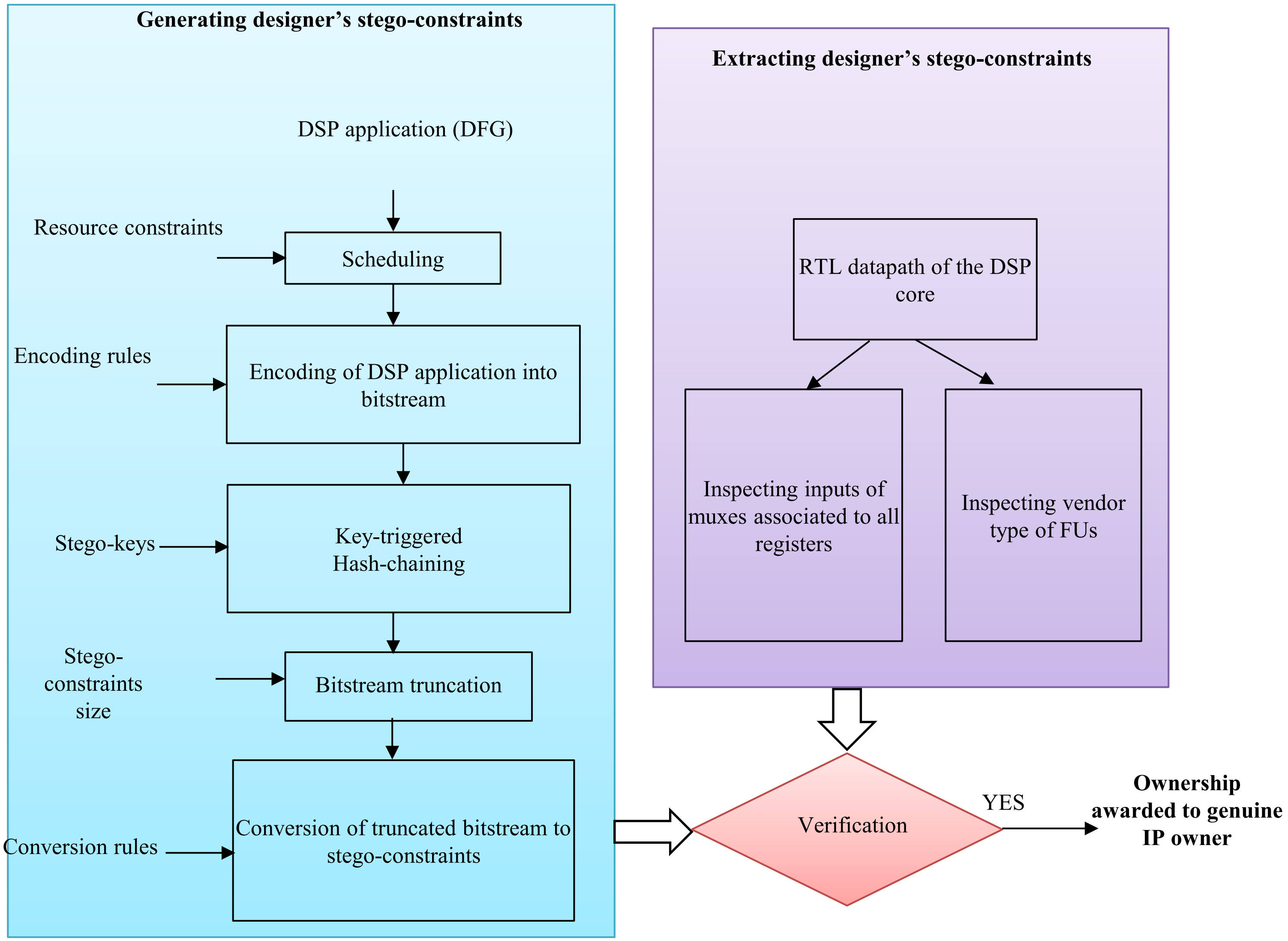
The length of the bitstream is equal to the number of operations (m) present in the respective DSP application. Further, ‘m’ bits of the encoded bitstream is converted into 1024 bits using following preprocessing rule: **(a) m-bit chunk is appended with ‘1’ followed by sequence of ‘0’ bits to generate 896 bits (b) the 896-bit chunk is appended with 128-bit representation of the length ‘m’ of encoded bitstream to obtain 1024 bits.** The 1024 bits are fed to first hash-block of hash-chaining.

For remaining hash-blocks, 1024-bit input is constructed using following proposed rule: **1024 bit = (512-bit output of previous hash-block) & “1000” & (380-bit output of bits-padding block) & (128-bit representation of the length ‘512 bits’ of previous hash)**



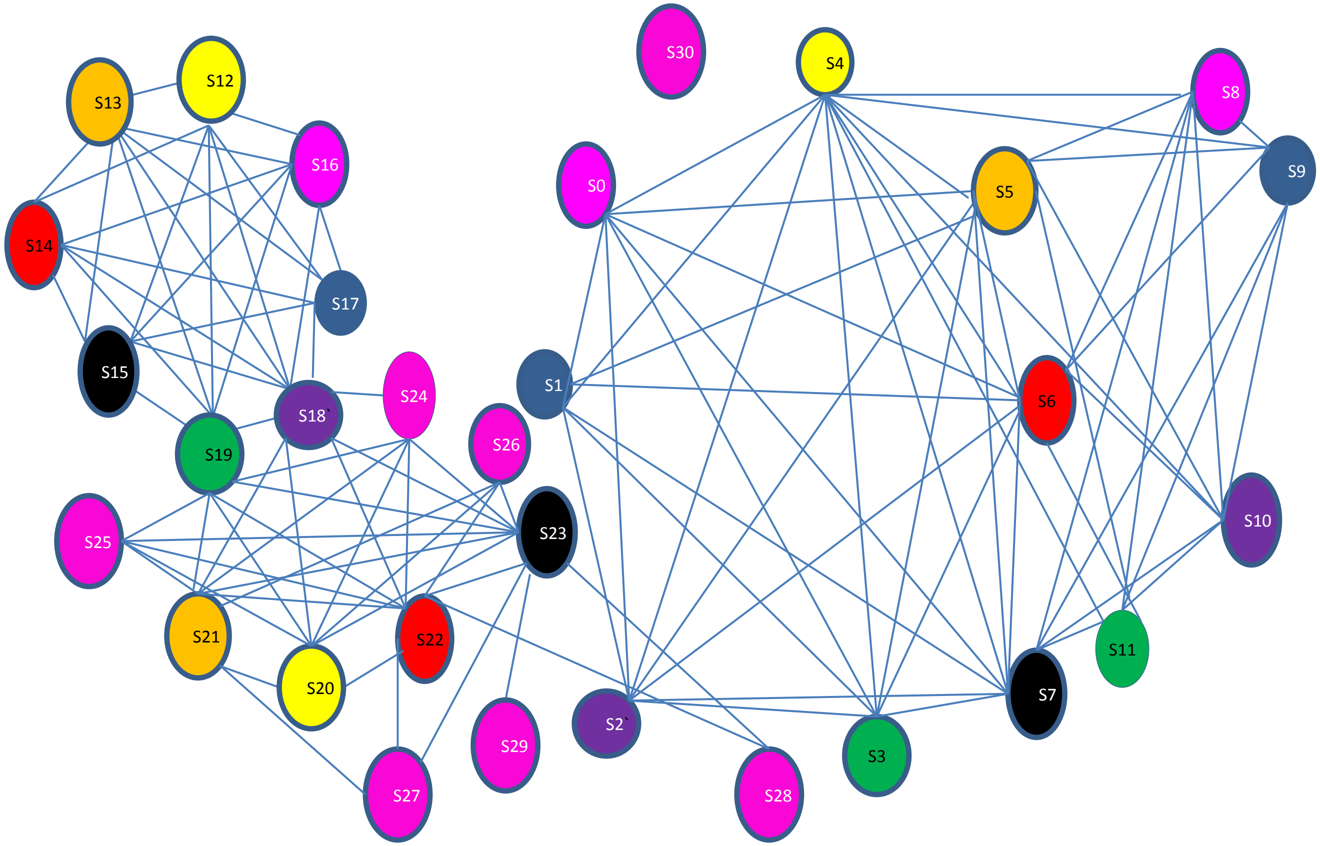
Anirban Sengupta, Mahendra Rathor, "IP Core Steganography using Switch based Key-driven Hash-chaining and Encoding for Securing DSP kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE),** 2020

Detection process of steganography

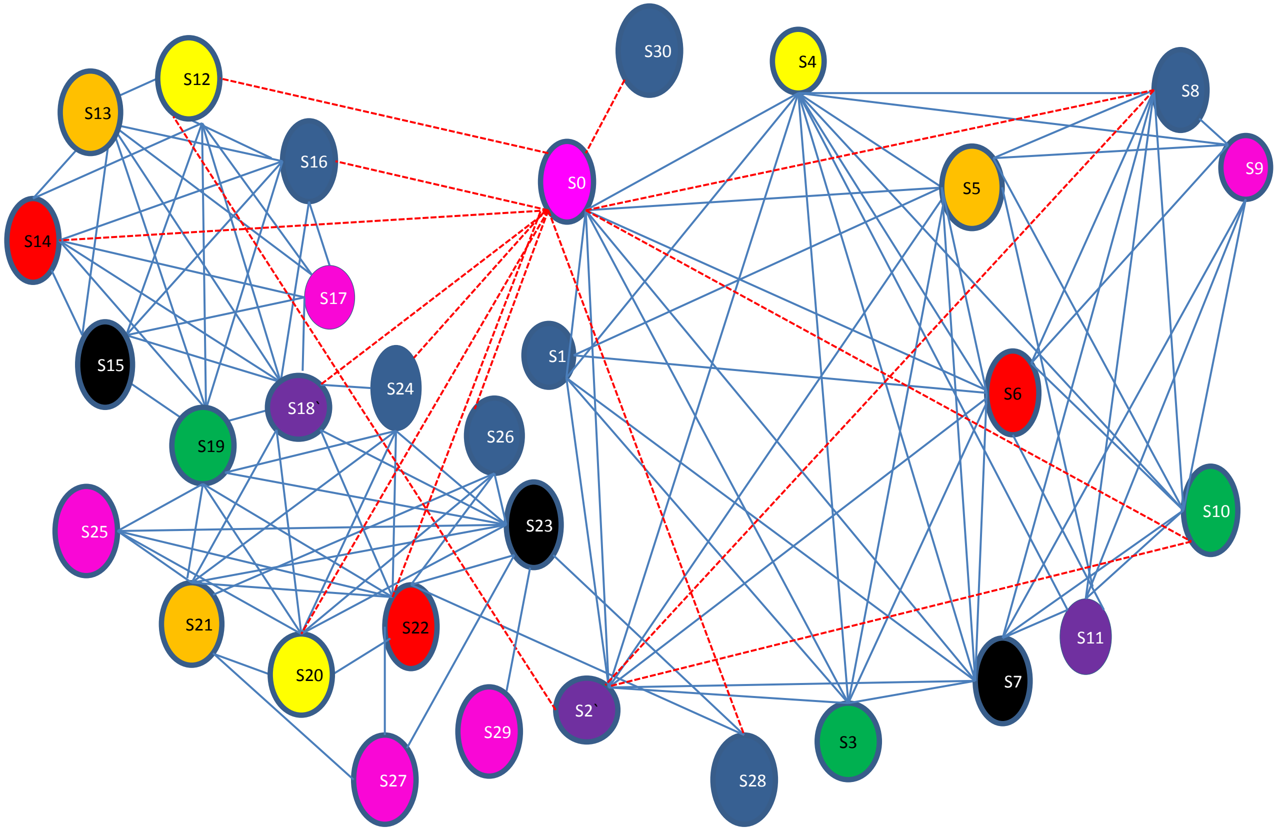

Generating designer's stego-constraints
DSP application (DFG)
Resource constraints
Scheduling
Encoding rules
Encoding of DSP application into bitstream
Stego-keys
Key-triggered Hash-chaining
Stego-constraints size
Bitstream truncation
Conversion rules
Conversion of truncated bitstream to stego-constraints
Extracting designer's stego-constraints
RTL datapath of the DSP core
Inspecting inputs of muxes associated to all registers
Inspecting vendor type of FUs
Verification
YES
Ownership awarded to genuine IP owner

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

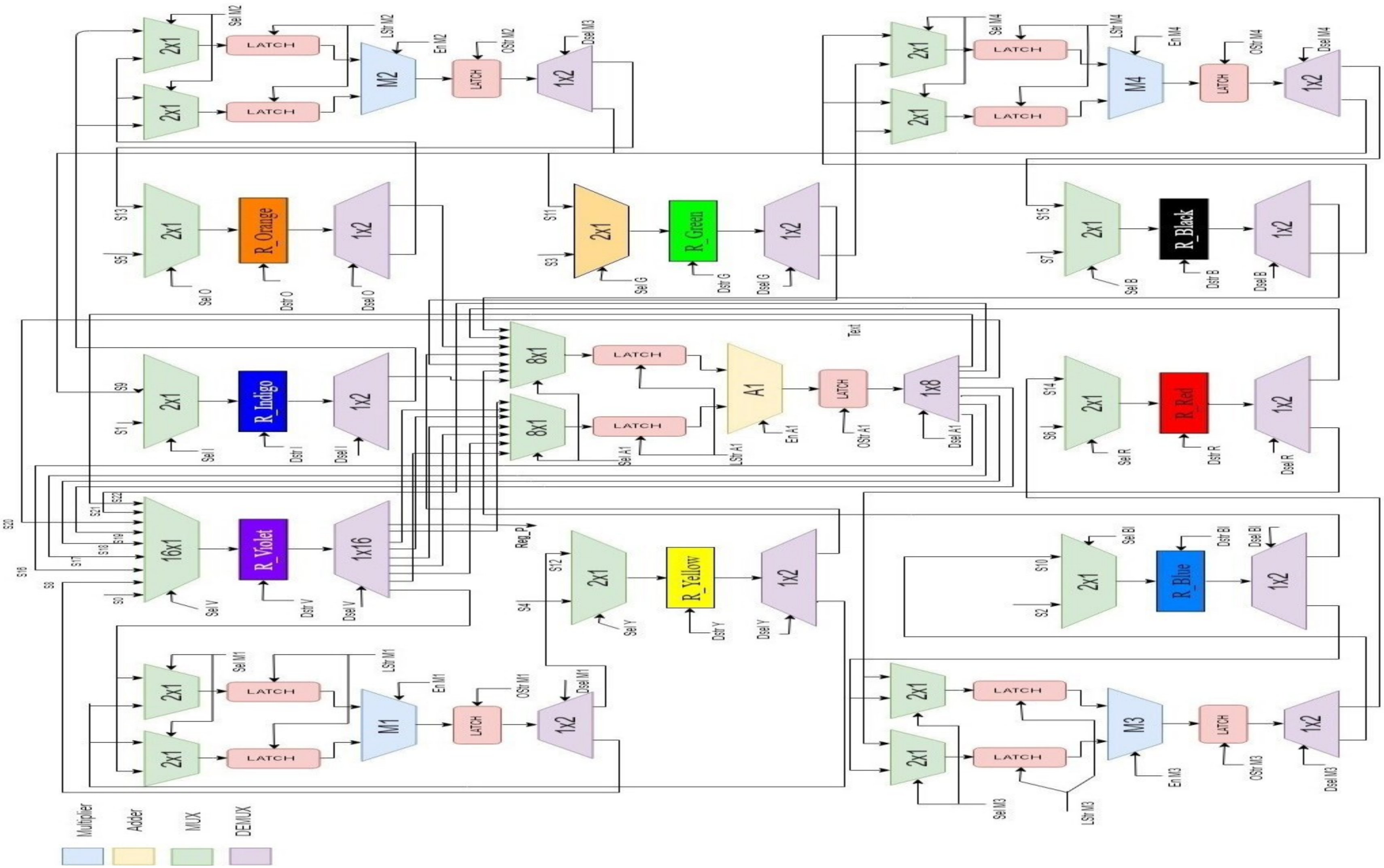
CIG of FIR filter hardware accelerator (IP core) before steganography



CIG of FIR filter hardware accelerator (IP core) after steganography

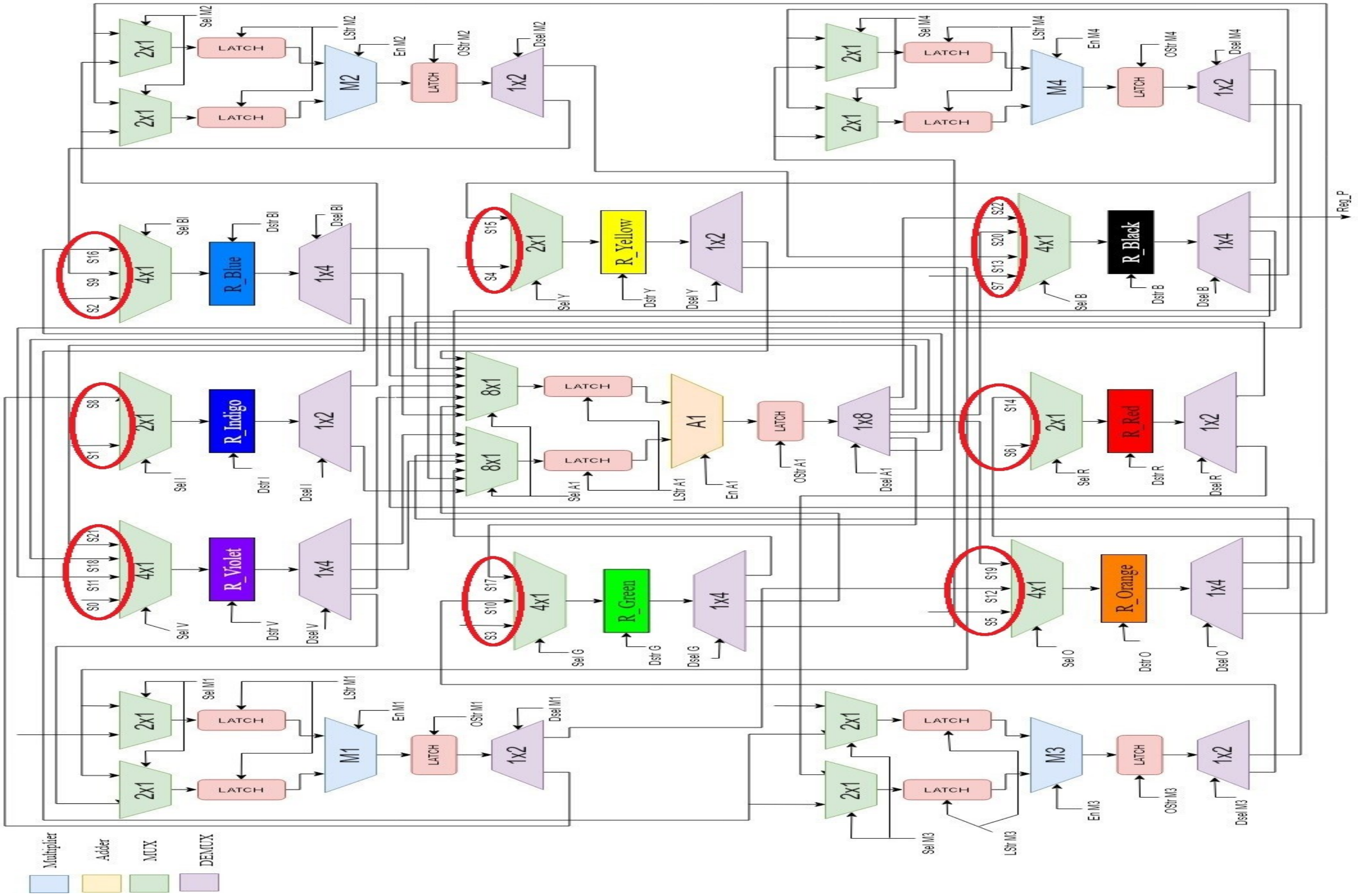


RTL datapath of 8-point DCT before



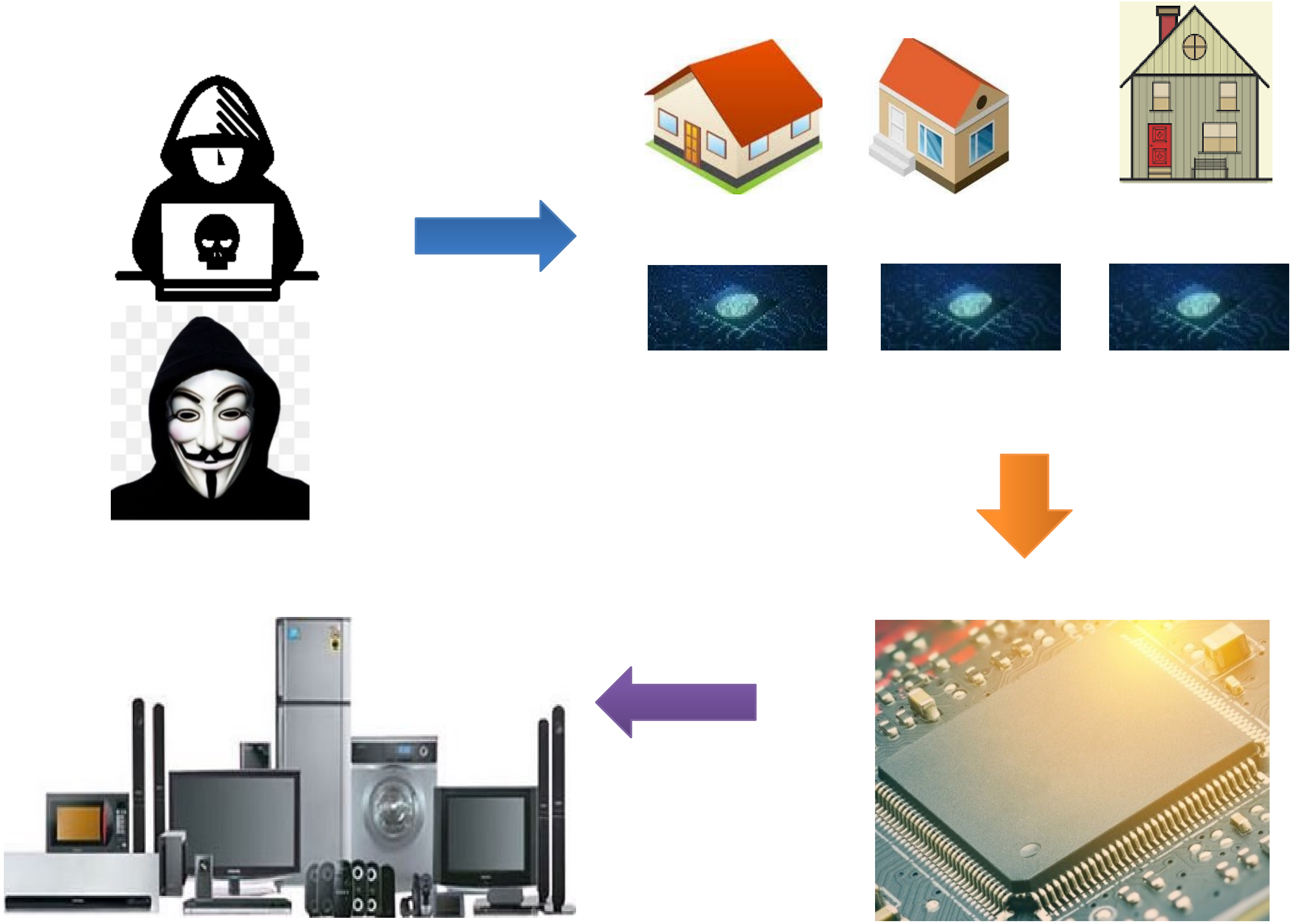
Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

RTL datapath of 8-point DCT **after** Steganography



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

IP core protection using Digital Signature

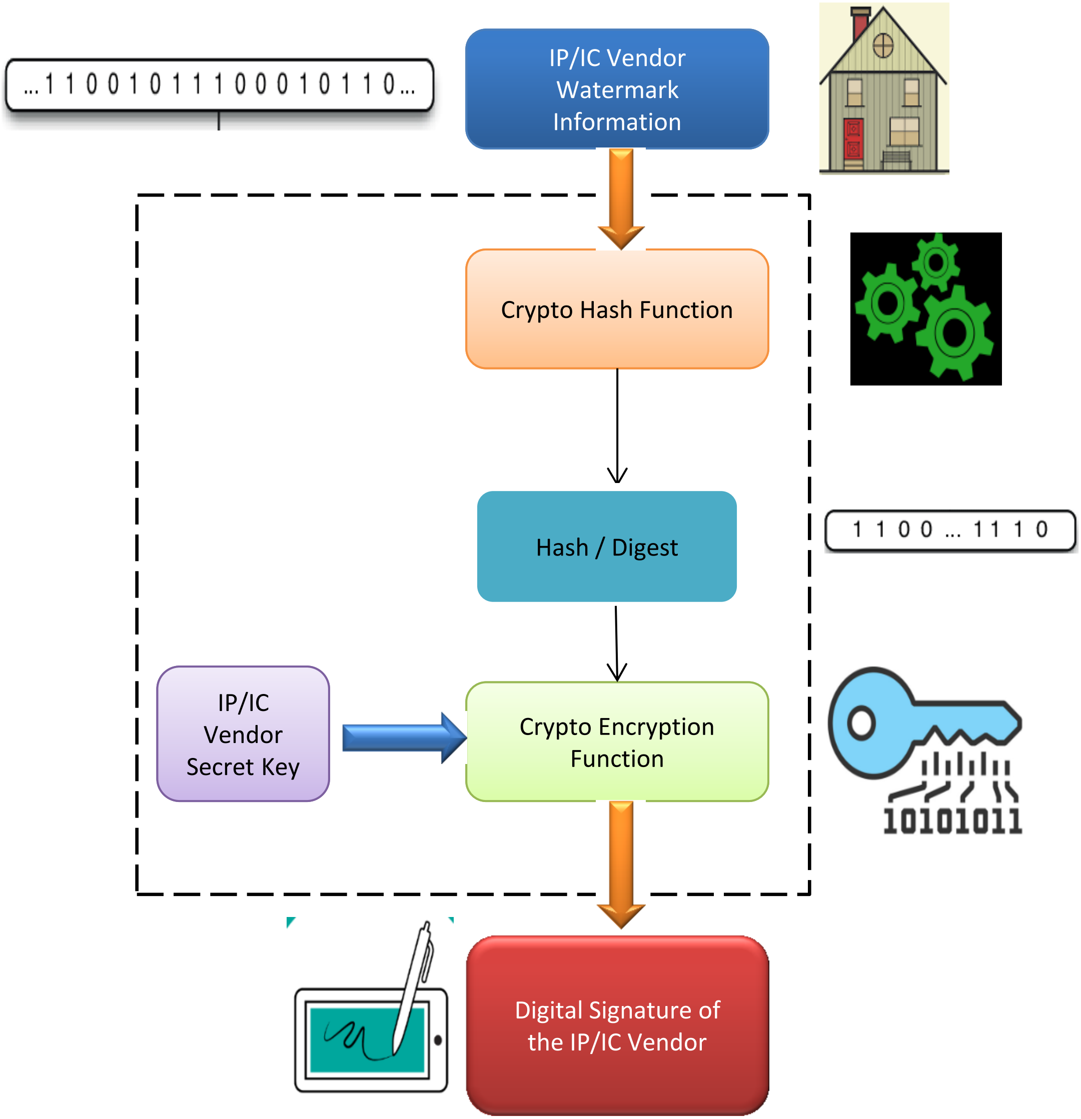


Consumer Electronic devices

SOC with third party IPs

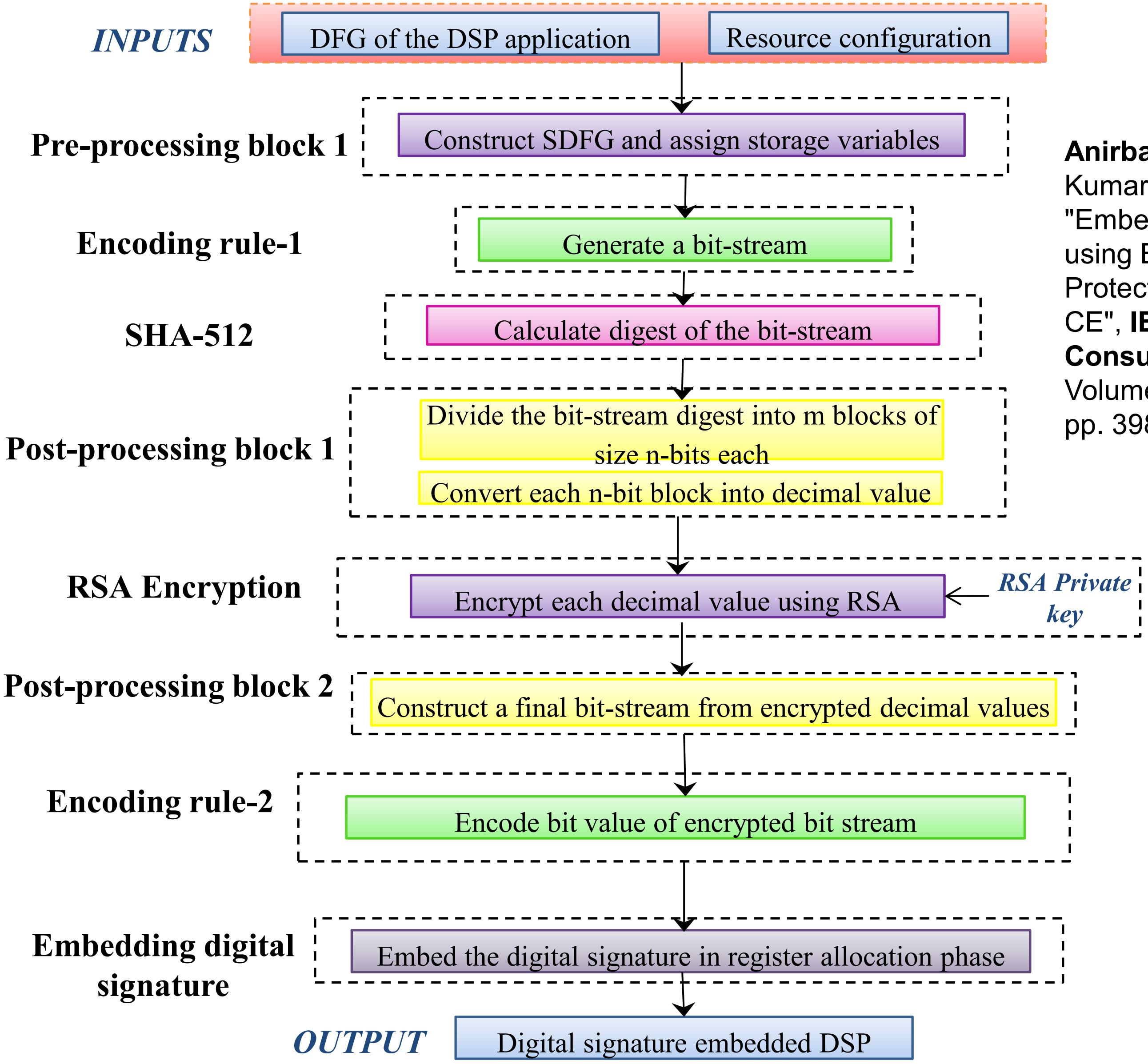
Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", **IEEE Transactions on Consumer Electronics (TCE)**, Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

High-level process of creating digital signature for IP cores



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

Flow of the approach


INPUTS
DFG of the DSP application
Resource configuration
Pre-processing block 1
Construct SDFG and assign storage variables
Encoding rule-1
Generate a bit-stream
SHA-512
Calculate digest of the bit-stream
Post-processing block 1
Divide the bit-stream digest into m blocks of size n-bits each
Convert each n-bit block into decimal value
RSA Encryption
Encrypt each decimal value using RSA
RSA Private key
Post-processing block 2
Construct a final bit-stream from encrypted decimal values
Encoding rule-2
Encode bit value of encrypted bit stream
Embedding digital signature
Embed the digital signature in register allocation phase
OUTPUT
Digital signature embedded DSP

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

Performing SHA-512 and Post Processing-1

➢Performing SHA-512

- Generates decimal digest of DSP core
- The collision resistance and deterministic properties of SHA-512 ensures that the generated hash digest carrying vendor secret mark is unique for an IP core design.

➢ Post-Processing-1

- Divide the bitstream digest into m blocks of size n bits each
- Convert each n-bit block into decimal value

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

RSA Encryption

- RSA is an asymmetric key encryption algorithm in which two distinct keys (private key and public key) are involved in the cryptography.
- It is used to sign the hash digest of vendor secret mark information to ensure authentication of the genuine owner.

Inputs (128 bits) and outputs of RSA module

RSA Decimal Input	Encrypted Decimal Output	Encrypted Binary Equivalent
328629211327023509667307560016780722176	259269232367594955022606516388222677830	110000110000110............011001101000110
338967726051337675217876235804913696768	103304422214721939828321919365106451481	100110110110111............100010000011001
74508071724950413296959519603599240546	24682247863022431965512042630223003075	100101001000110............111110111000011
14047629289186758734138225185020455483	289411796889479622387067677582110256178	110110011011101............110110000110010

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

Post-processing Block 2

- The encrypted decimal values— output of RSA module— are provided as input to the post-processing block 2.
- Each decimal value is converted to binary and these individual binary streams are concatenated to form a single bit-stream.
- This encrypted-hashed bit-stream is referred to as **Digital Signature**. The digital signature size can be selected based on vendor's choice from the continuous bit-stream.
- For instance, if the vendor selects digital signature size as 15, then the first 15 bits of the bit-stream is the digital signature.

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

Bit stream Generation

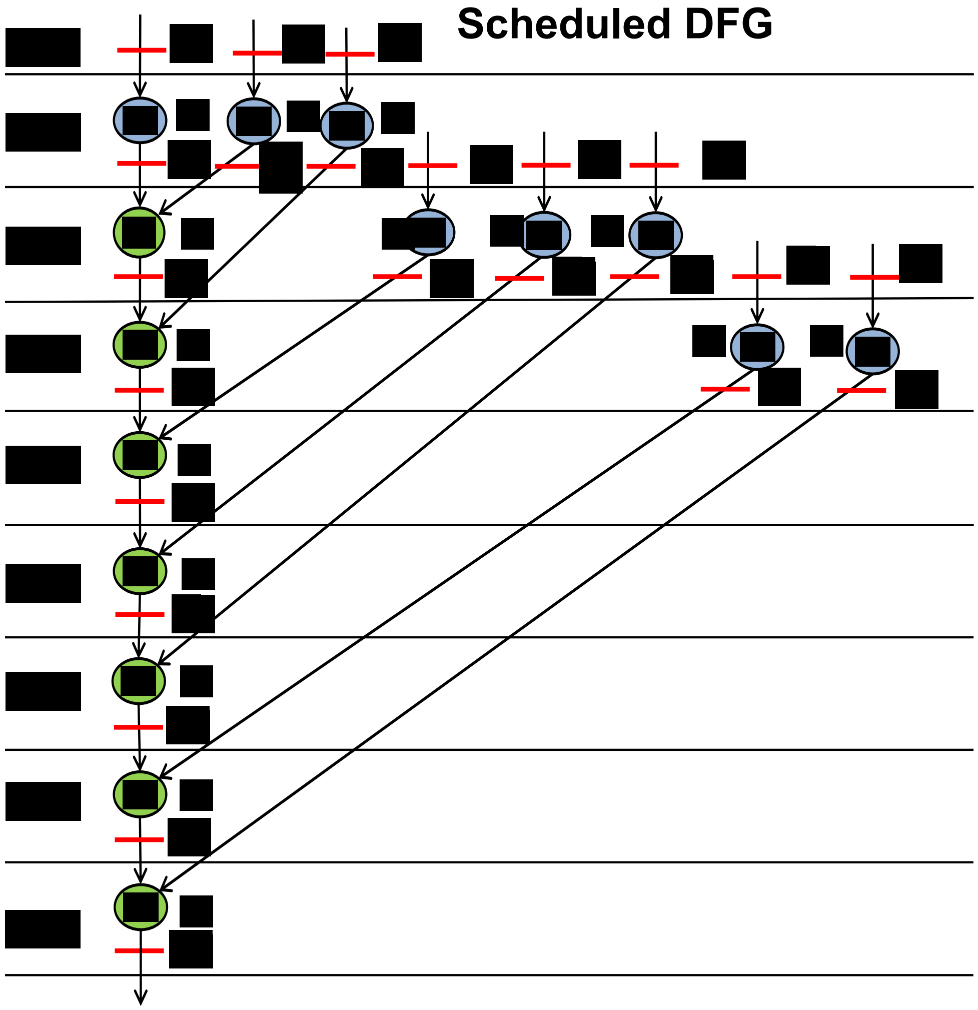
- Based on encoding rule-1

Operation number	Corresponding control step	Encoded
(OPN)	(CS) number	bit
Even	Even	0
Odd	Even	1
Even	Odd	1
Odd	Odd	0

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

Generating the Bit-stream of DCT Core

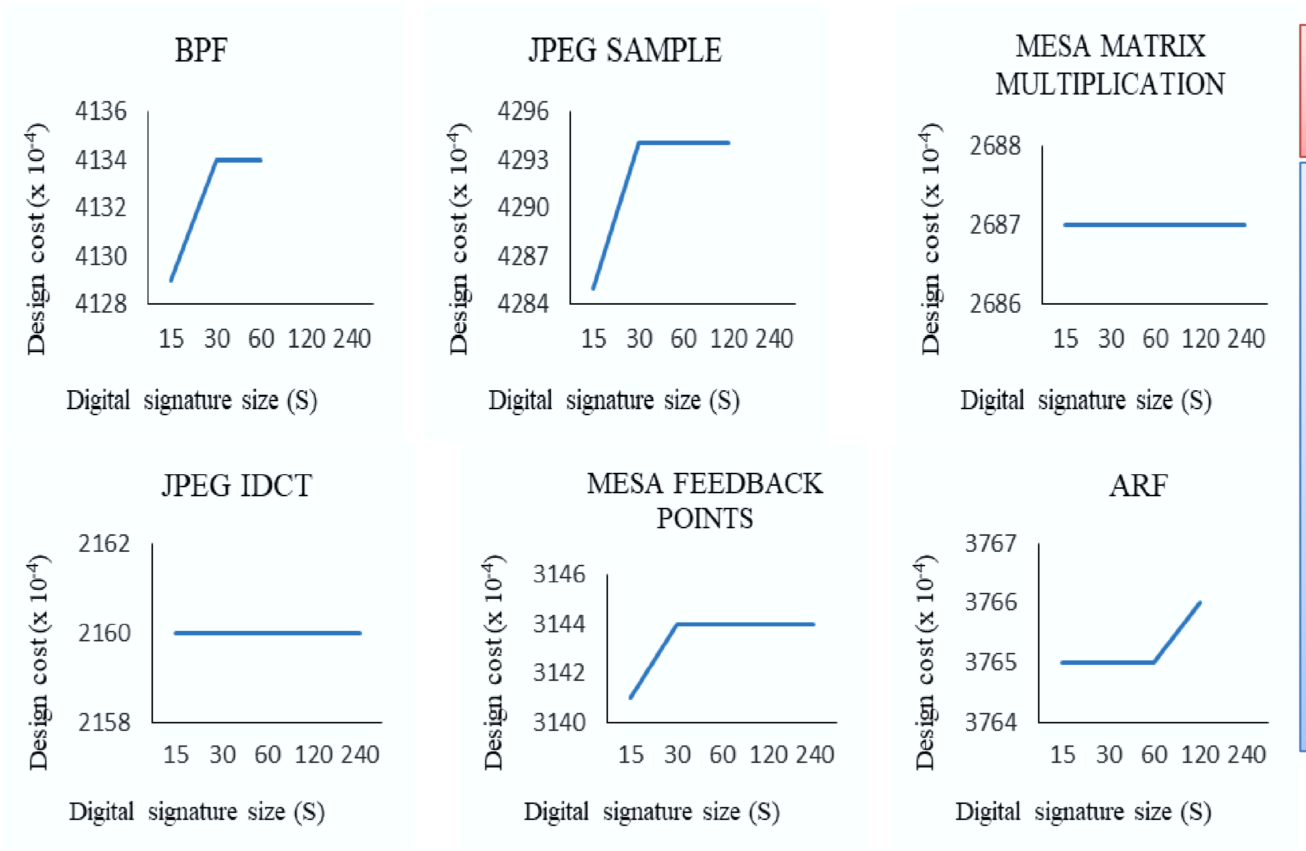
Operation Number	Control Step Number	Bit generated
1	1	0
2	1	1
3	2	1
4	1	1
5	3	0
6	2	0
7	4	1
8	2	0
9	5	0
10	2	0
11	6	1
12	3	1
13	7	0
14	3	1
15	8	1



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

Experimental Results

- **Graphical Representation of Design Cost for different benchmarks**



Design cost

$$C_f(X_i) = \phi_1 \frac{L_T}{L_{max}} + \phi_2 \frac{A_T}{A_{max}}$$

L_T =design latency
A_T =hardware area
L_{max}= maximum execution latency
A_{max} = maximum hardware area.

ϕ_1, ϕ_2 represent the user specified weights both fixed at 0.5 to assign equal preference

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

Experimental Results

- **Evaluation of Robustness Using Probability of Coincidence (Pc)**

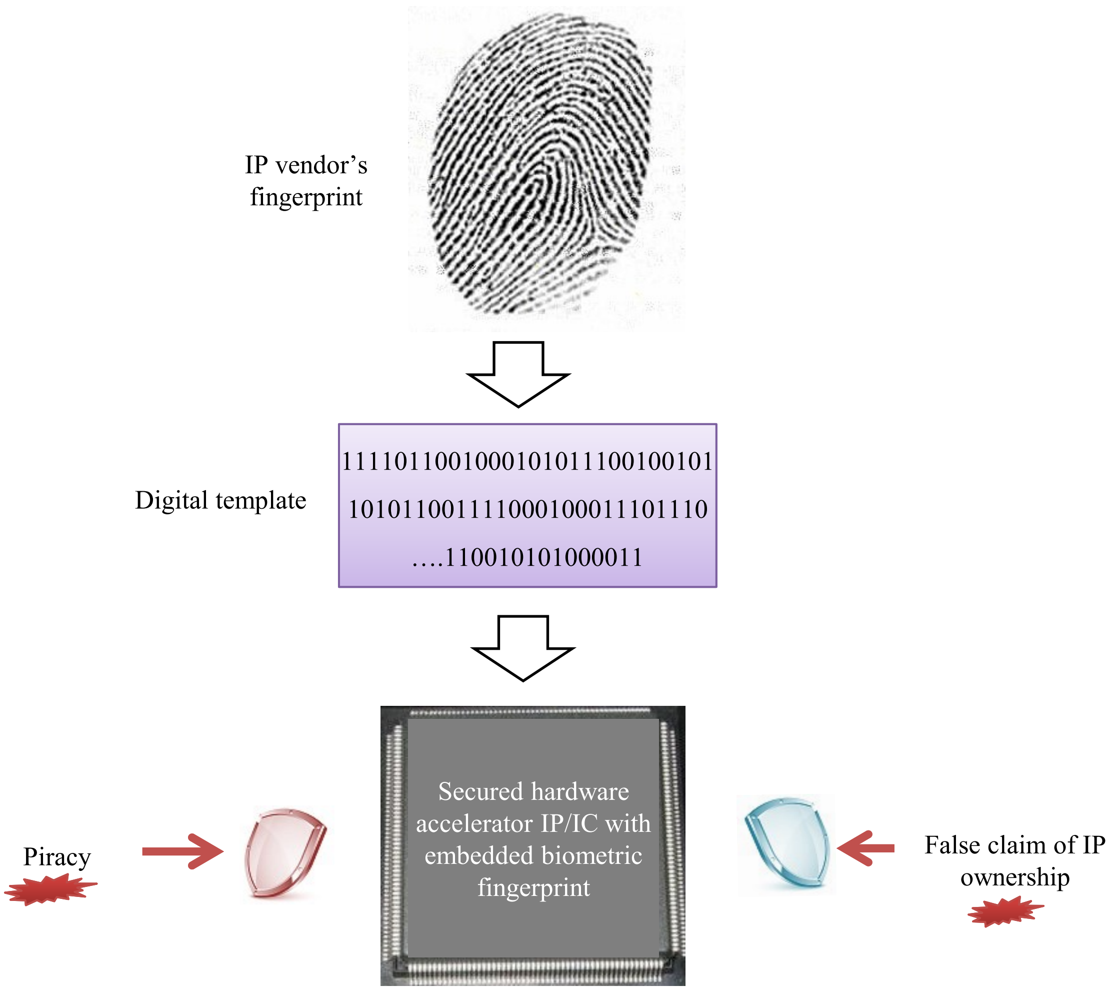
$$P_c = \left(1 - \frac{1}{c}\right)^S$$

‘c’ denotes the number of colours used in the CIG and
‘S’ denotes the digital signature size

Benchmarks	c	Size of Digital signature (S)				
		S = 15	S = 30	S = 60	S = 120	S = 240
		P_c	P_c	P_c	P_c	P_c
BPF	6	0.0649	$4.2127\text{x}10^{-3}$	$1.7747\text{x}10^{-5}$	$3.1496\text{x}10^{-10}$	$9.9198\text{x}10^{-20}$
JPEG SAMPLE	10	0.2059	0.0424	$1.7970\text{x}10^{-3}$	$3.2292\text{x}10^{-6}$	$1.0428\text{x}10^{-11}$
JPEG IDCT	29	0.5907	0.3490	0.1218	0.0148	$2.1999\text{x}10^{-4}$
MESA FEEDBACK POINTS	17	0.4028	0.1622	0.0263	$6.9267\text{x}10^{-4}$	$4.7979\text{x}10^{-7}$
ARF	8	0.1349	0.0182	$3.3150\text{x}10^{-4}$	$1.0989\text{x}10^{-7}$	$1.2076\text{x}10^{-14}$
MESA MATRIX MULTIPLICATION	23	0.5134	0.2635	0.0695	$4.8237\text{x}10^{-3}$	$2.3268\text{x}10^{-5}$

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

Securing hardware accelerators using biometric fingerprinting: Forensics



IP vendor's fingerprint

Digital template

1111011001000101011100100101

101011001111000100011101110

....110010101000011

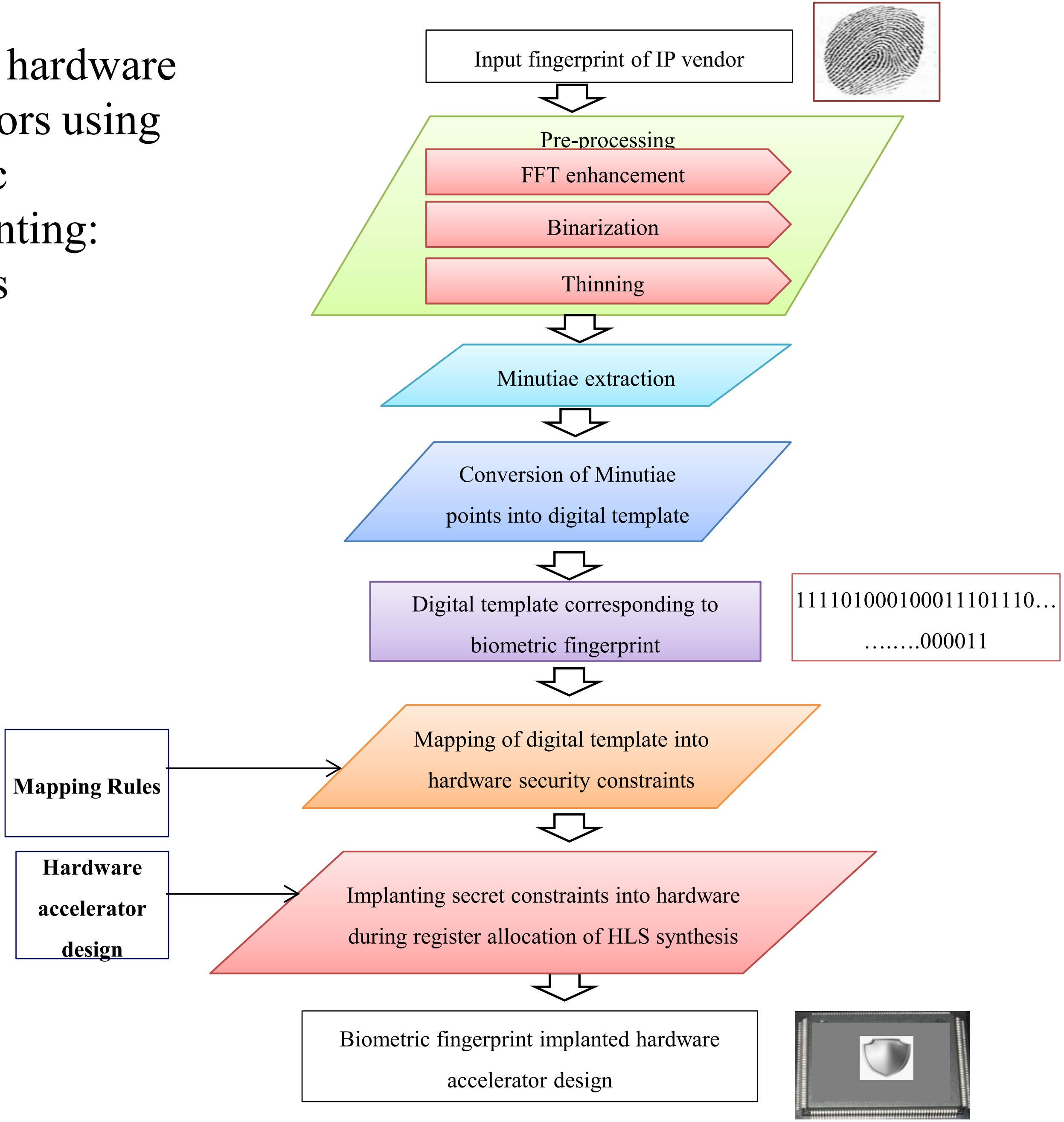
Secured hardware accelerator IP/IC with embedded biometric fingerprint

Piracy

False claim of IP ownership

Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

Securing hardware accelerators using biometric fingerprinting: Forensics



Input fingerprint of IP vendor

Pre-processing

FFT enhancement

Binarization

Thinning

Minutiae extraction

Conversion of Minutiae points into digital template

Digital template corresponding to biometric fingerprint

1111010001000111101110…

……..000011

Mapping Rules

Mapping of digital template into hardware security constraints

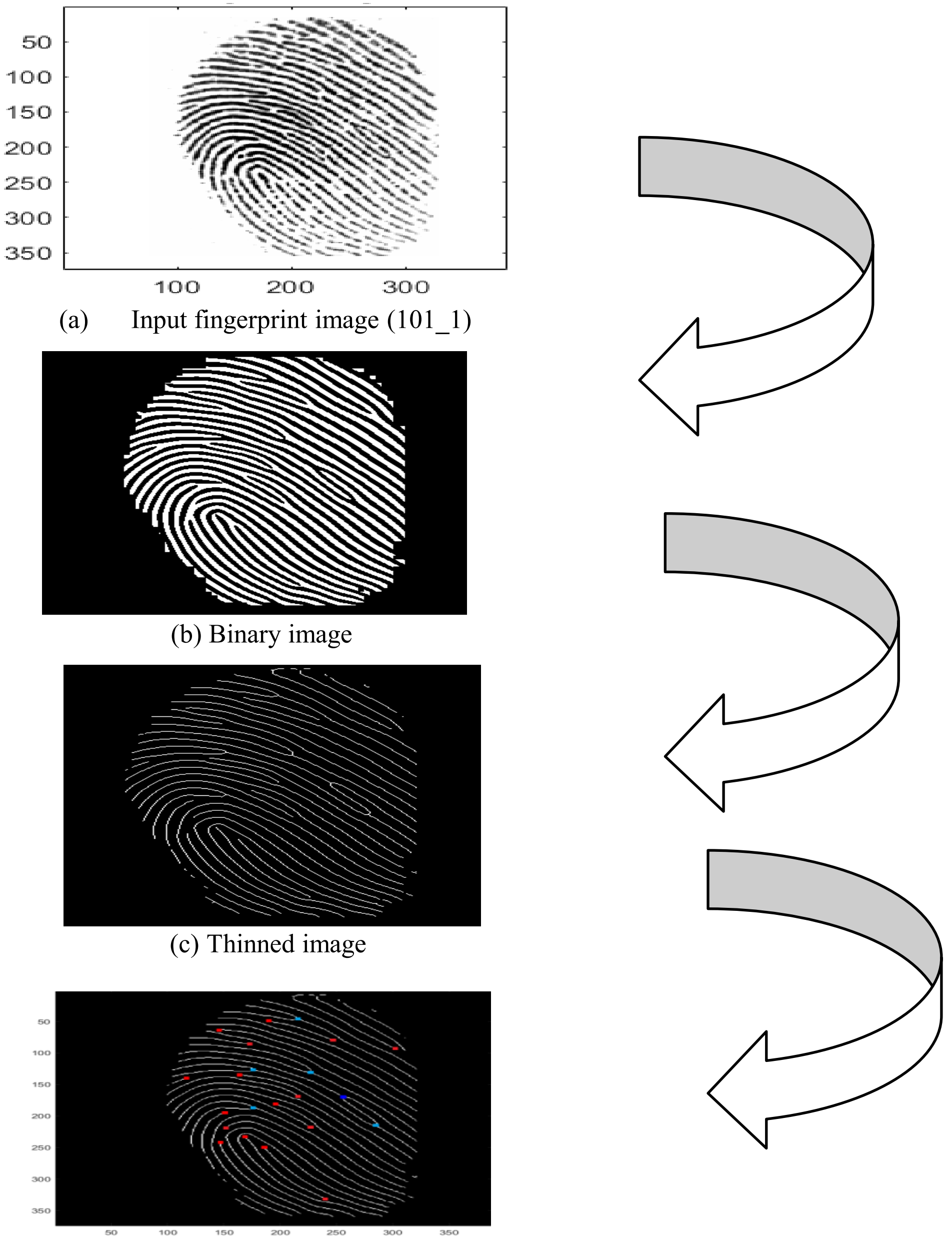
Hardware accelerator design

Implanting secret constraints into hardware during register allocation of HLS synthesis

Biometric fingerprint implanted hardware accelerator design

Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

Securing hardware accelerators using biometric fingerprinting: Forensics: An example



(a) Input fingerprint image (101_1)

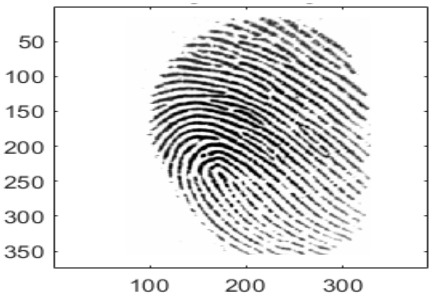
(b) Binary image

(c) Thinned image

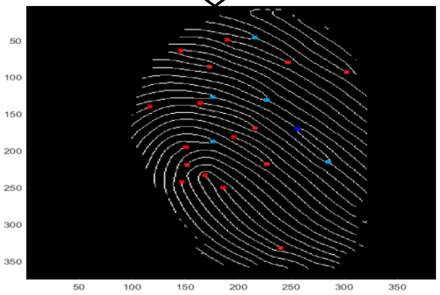
(d) Minutiae points

Minutiae points extraction flow (a) Captured fingerprint image (b) Binary fingerprint image post enhancement (c) Fingerprint image post applying thinning (d) Fingerprint image with minutiae points located

Secret biometric constraints for various fingerprint images



Fingerprint image (101_1)



Minutiae points=22

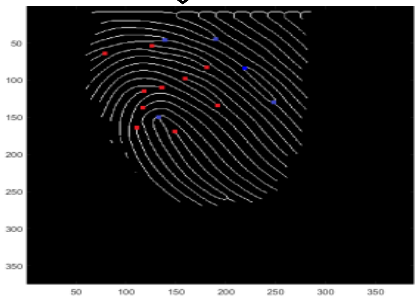
1101100010111011111101101111
10……….101001100111101

Corresponding Digital Template
(Total size =526 bits)

#0s= 224
#1s= 302

Secret biometric constraints
for IC/IP

Fingerprint image:101_2



Minutiae points=15

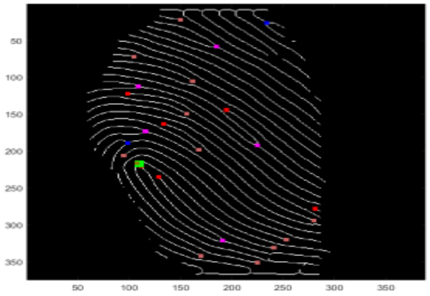
10111110101101111000101000
10111……..01001111101111

Corresponding Digital Template
(Total size =350 bits)

#0s= 148
#1s= 202

Secret biometric constraints
for IC/IP

Fingerprint image:101_8



Minutiae points=24

10010110101101101001110101
011010…..1101011111111110

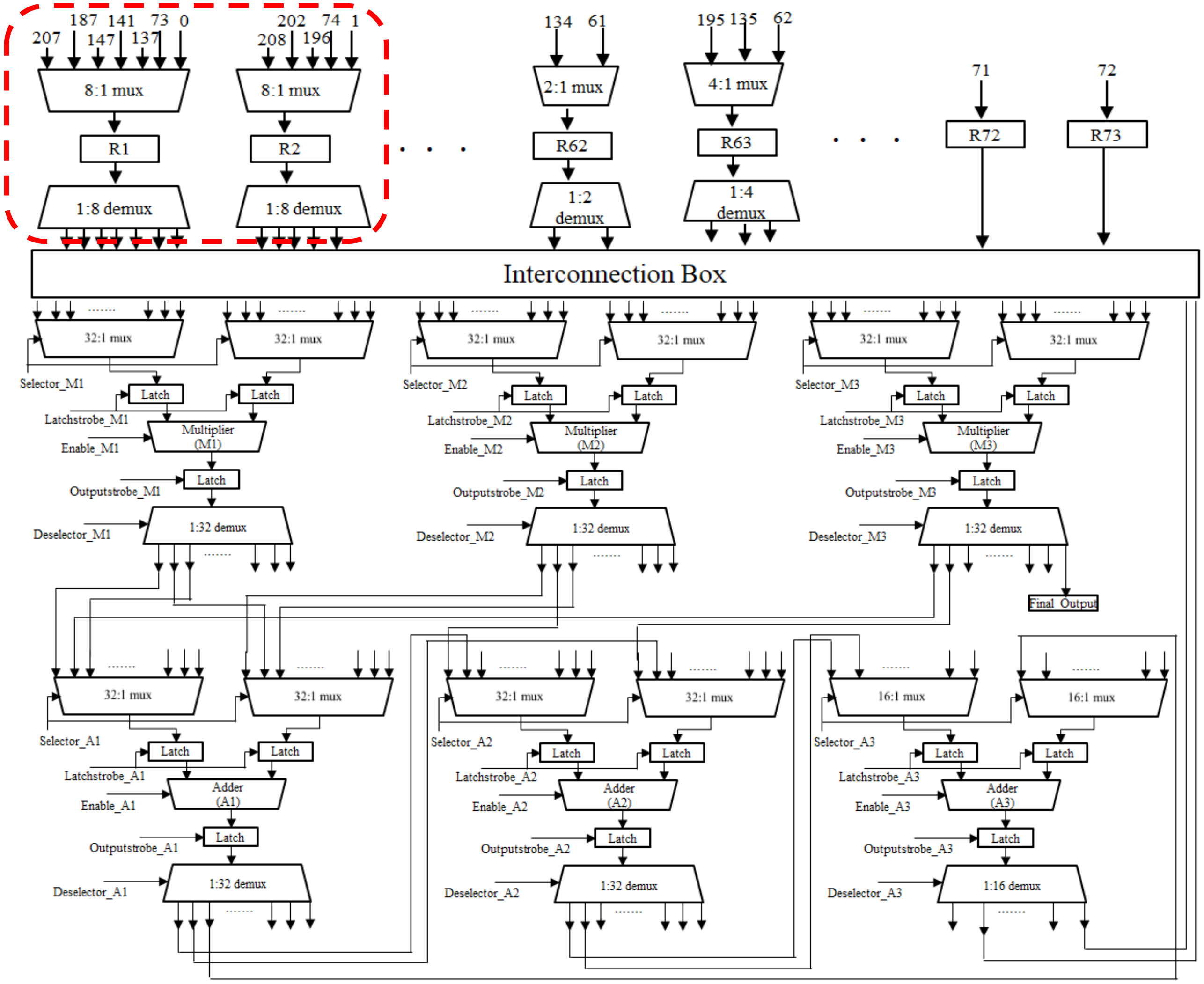
Corresponding Digital Template
(Total size =555 bits)

#0s= 242
#1s= 312

Secret biometric constraints
for IC/IP

Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

Secured datapath of JPEG compression hardware accelerator implanted with biometric fingerprint



Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

Detecting Biometric Fingerprint in a hardware accelerator

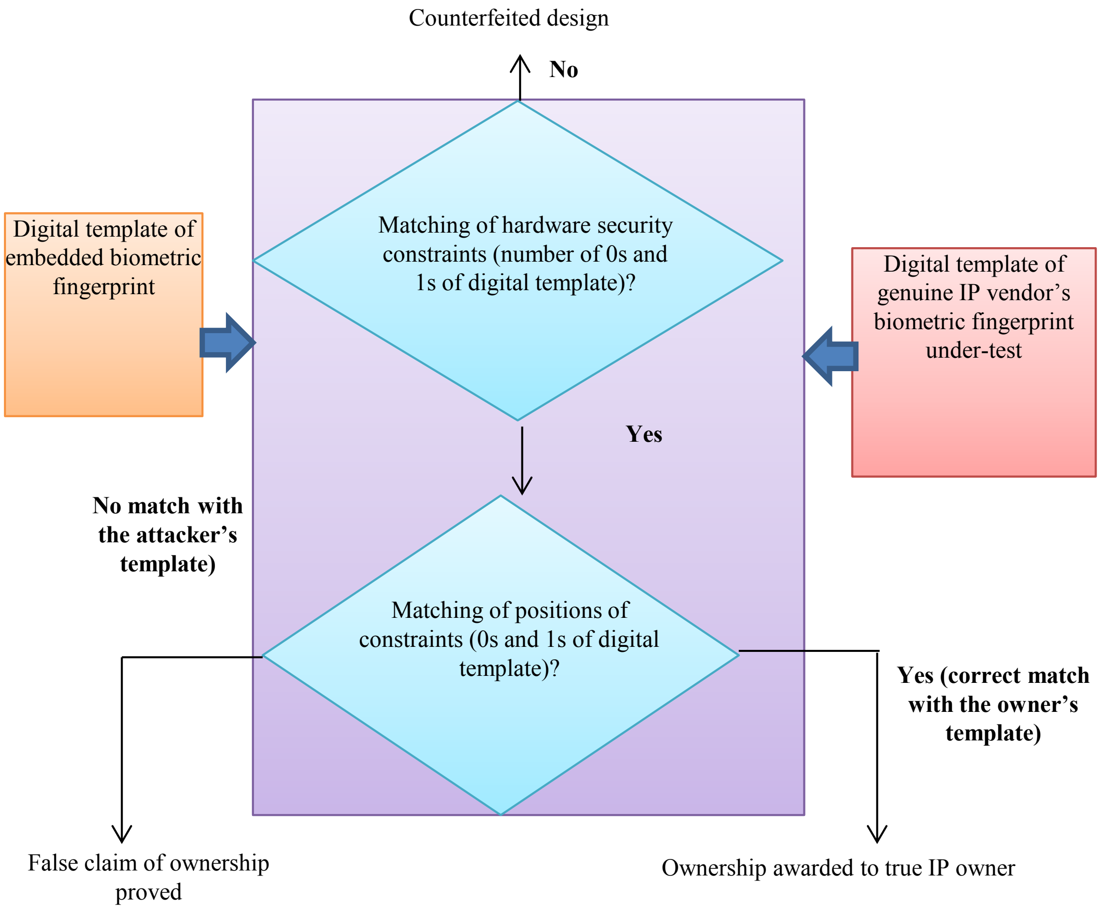
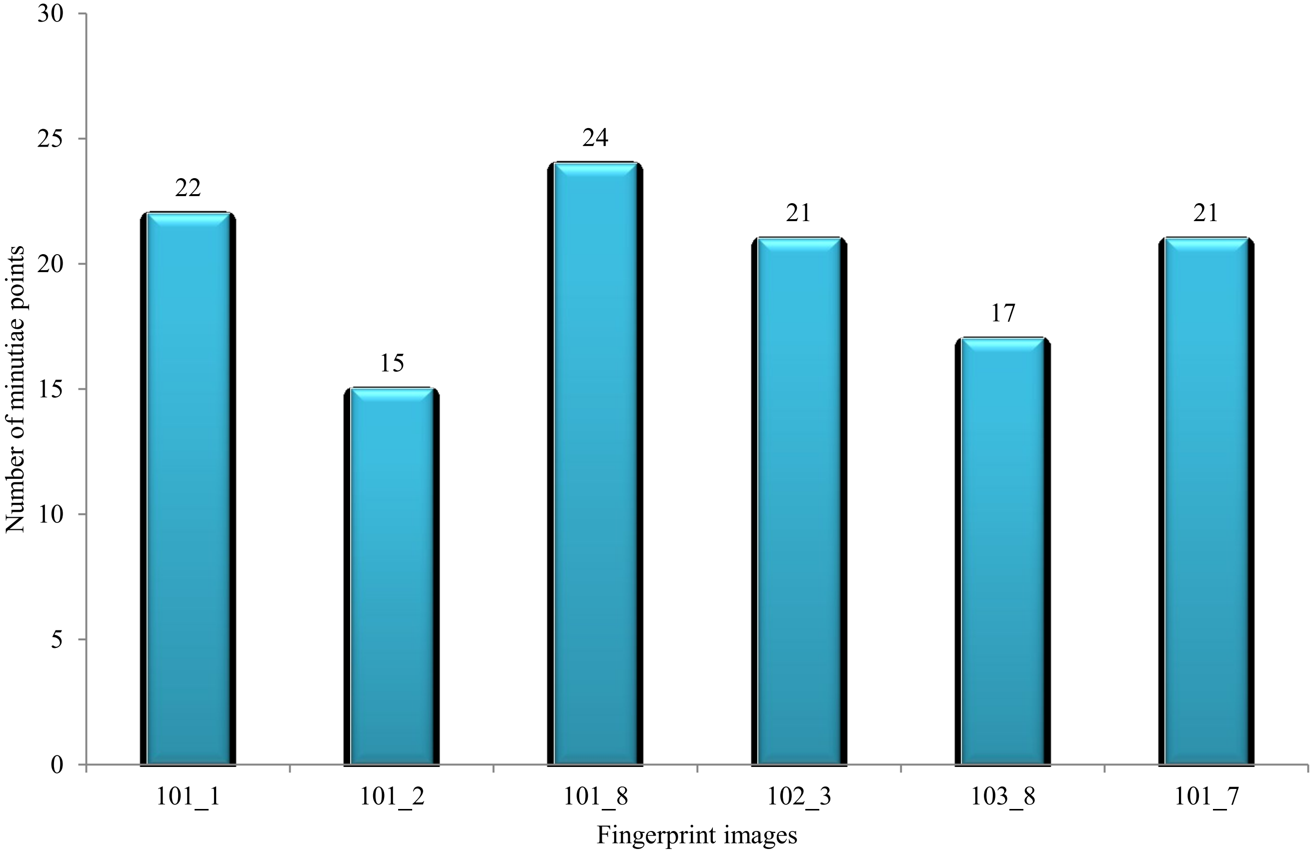

Counterfeited design
No
Digital template of embedded biometric fingerprint
Matching of hardware security constraints (number of 0s and 1s of digital template)?
Digital template of genuine IP vendor's biometric fingerprint under-test
Yes
No match with the attacker's template)
Matching of positions of constraints (0s and 1s of digital template)?
Yes (correct match with the owner's template)
False claim of ownership proved
Ownership awarded to true IP owner

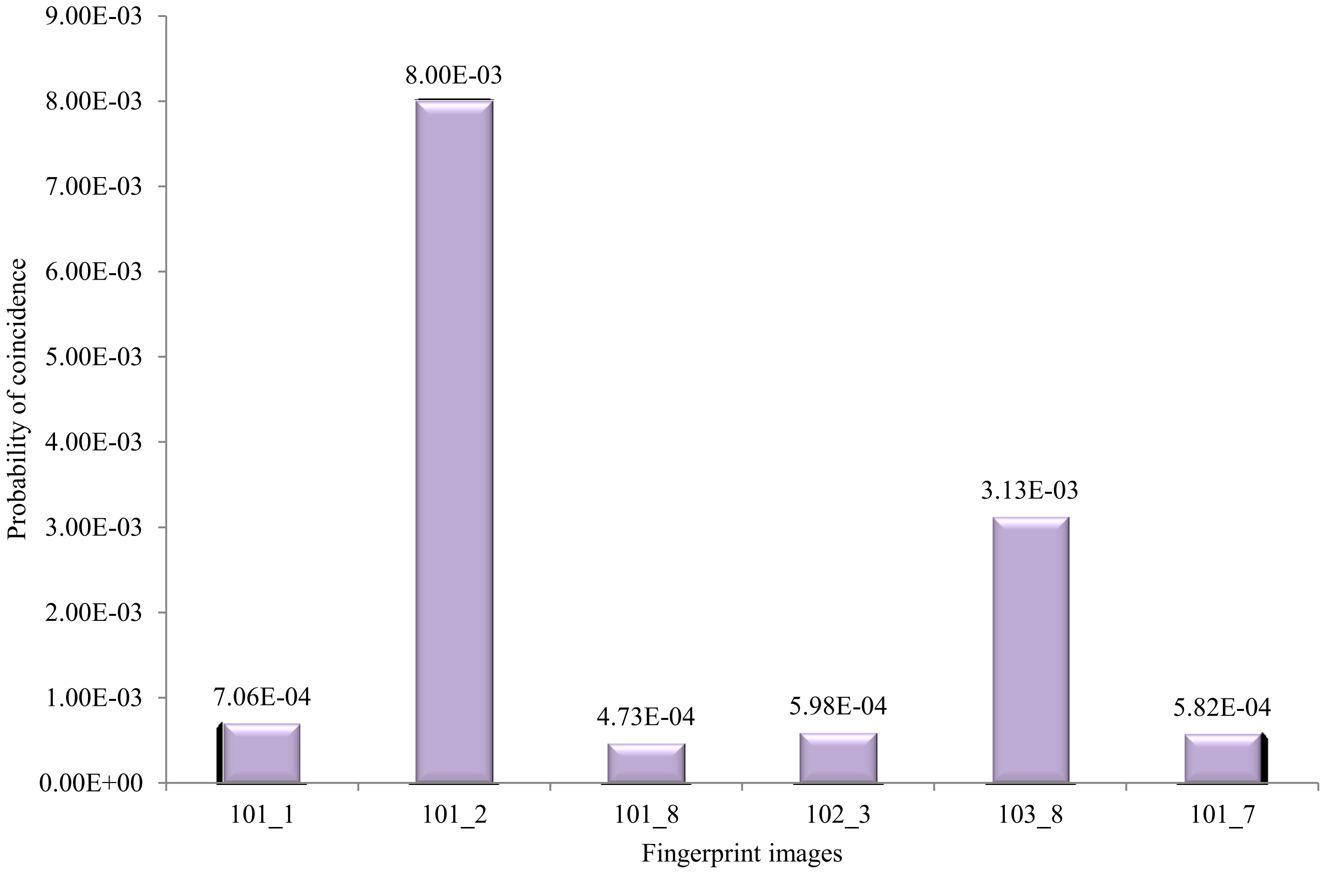
Fig. 9. Proving true IP ownership using proposed detection approach

Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

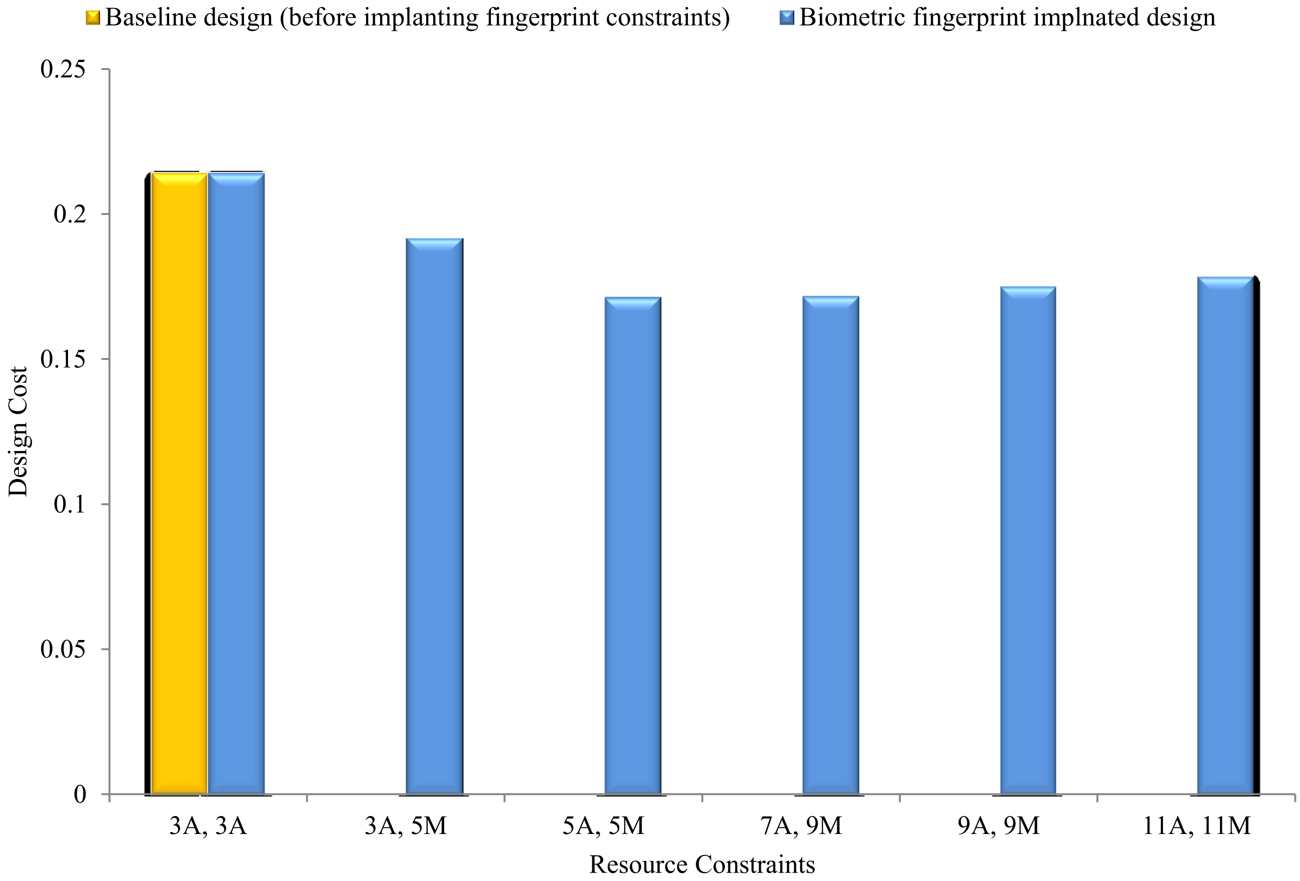
Variation in number of minutiae points for different fingerprint images



Variation in probability of coincidence for different fingerprint images



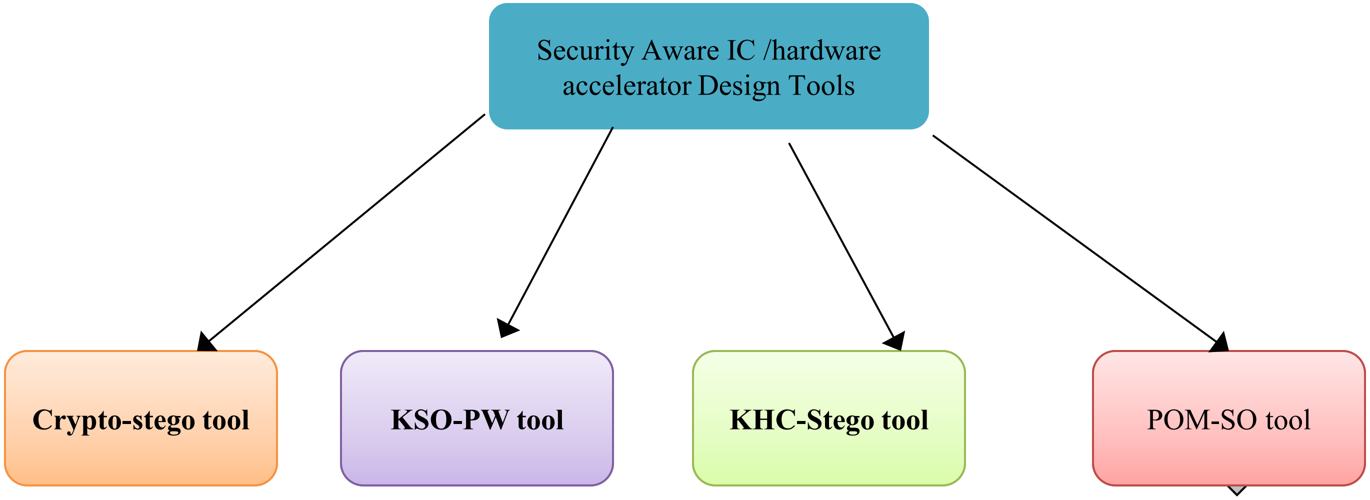
Comparison of design cost of JPEG compression hardware accelerator before and after implanting fingerprint constraints



Our in-house hardware security tools for designing secured accelerators

Released publicly from our group in Sep 2020 !

http://www.anirban-sengupta.com/Hardware_Security_Tools.php



Security Aware IC /hardware accelerator Design Tools

Crypto-stego tool

KSO-PW tool

KHC-Stego tool

POM-SO tool

Crypto-steganography tool for DSP hardware accelerators

Key-driven structural obfuscation and physical level watermarking tool

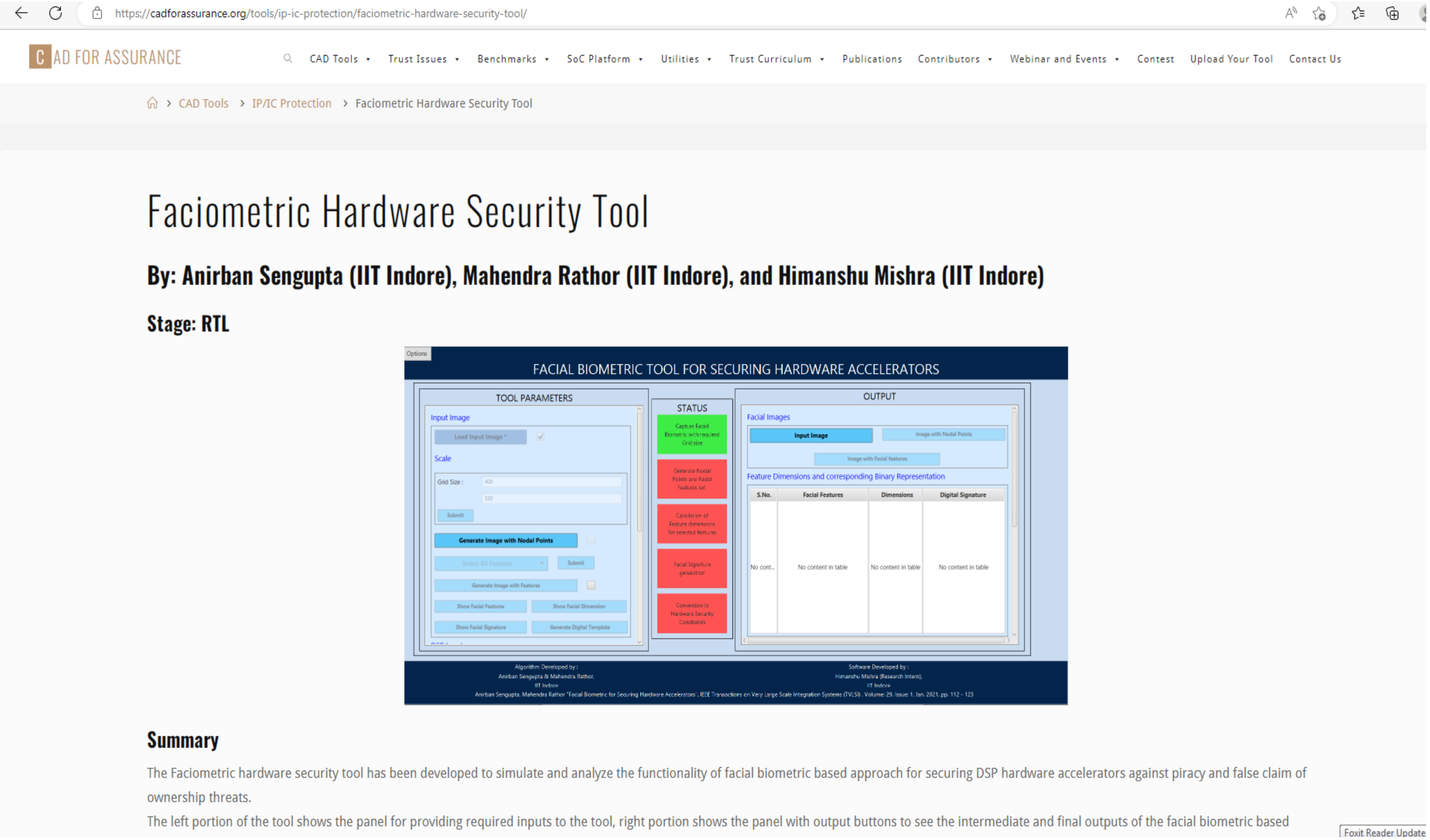
Key-triggered Hash-chaining Driven Steganography tool

Pseudo operation mixing based structural obfuscation tool

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

Faciometric Hardware Security Tool – CAD for Assurance

https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool/



https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool/

CAD Tools > IP/IC Protection > Faciometric Hardware Security Tool

Faciometric Hardware Security Tool

By: Anirban Sengupta (IIT Indore), Mahendra Rathor (IIT Indore), and Himanshu Mishra (IIT Indore)

Stage: RTL

Options
FACIAL BIOMETRIC TOOL FOR SECURING HARDWARE ACCELERATORS
TOOL PARAMETERS
Input Image
Load Input Image *
Scale
Grid Size :
420
520
Submit
Generate Image with Nodal Points
Select All Features
Submit
Generate Image with Features
Show Facial Features
Show Facial Dimension
Show Facial Signature
Generate Digital Template
STATUS
Capture Facial Biometric with required Grid size
Generate Nodal Points and Facial Features set
Calculation of Feature dimensions for selected features
Facial Signature generation
Conversion to Hardware Security Constraints
OUTPUT
Facial Images
Input Image
Image with Nodal Points
Image with Facial features
Feature Dimensions and corresponding Binary Representation
S.No.
Facial Features
Dimensions
Digital Signature
No cont...
No content in table
No content in table
No content in table

Algorithm Developed by :
Anirban Sengupta & Mahendra Rathor,
IIT Indore

Software Developed by :
Himanshu Mishra (Research Intern),
IIT Indore

Anirban Sengupta, Mahendra Rathor "Facial Biometric for Securing Hardware Accelerators", IEEE Transactions on Very Large Scale Integration Systems (TVLSI), Volume: 29, Issue: 1, Jan. 2021, pp. 112 - 123

Summary

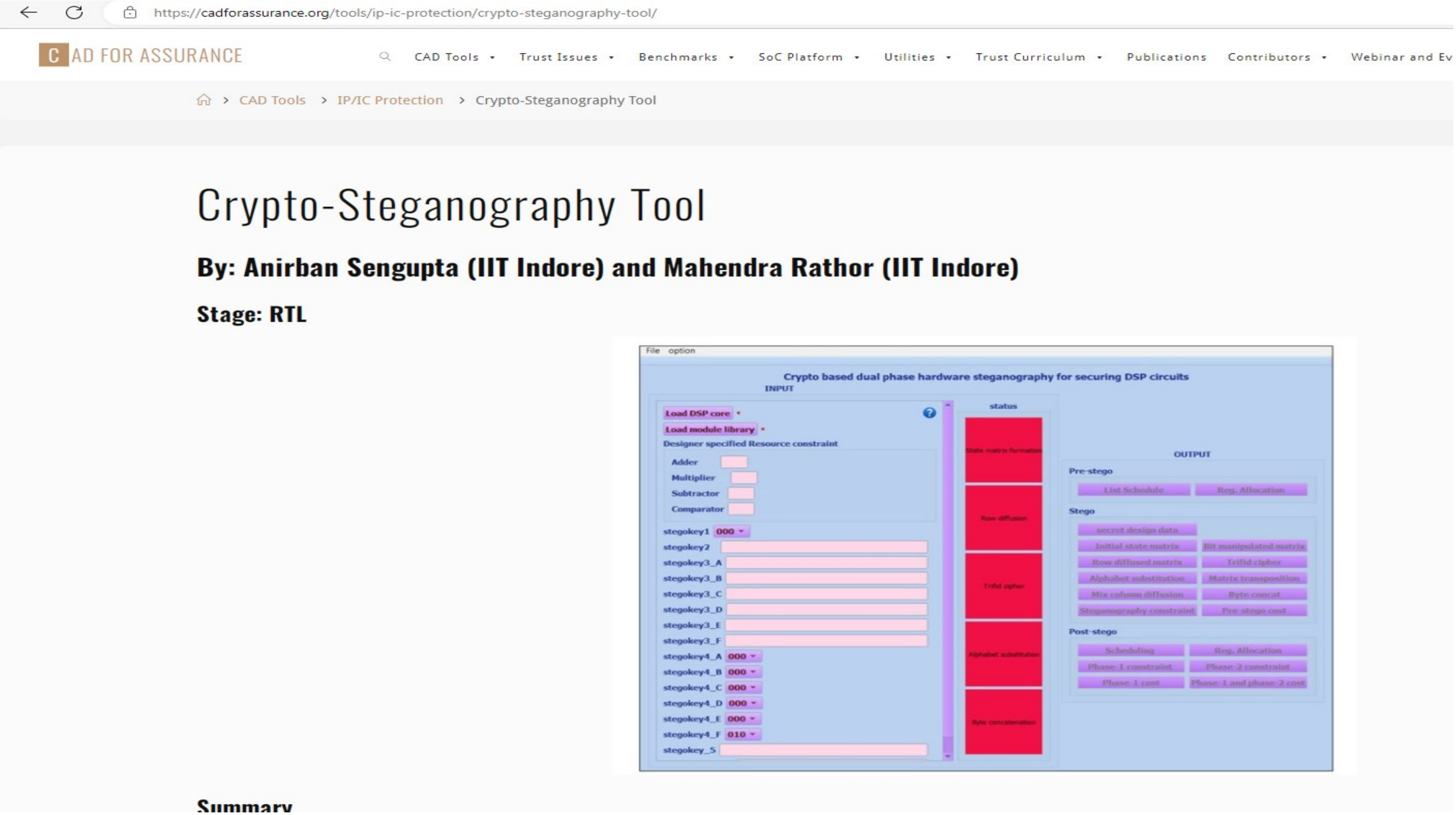
The Faciometric hardware security tool has been developed to simulate and analyze the functionality of facial biometric based approach for securing DSP hardware accelerators against piracy and false claim of ownership threats.

The left portion of the tool shows the panel for providing required inputs to the tool, right portion shows the panel with output buttons to see the intermediate and final outputs of the facial biometric based

(Publicly available under 'CAD for Assurance' tools sponsored by IEEE CEDA, IEEE Hardware Security and Trust Technical Committee, and Warren B. Nelms Institute for the Connected World at University of Florida
(Public access of these tools > 3200 times))

Crypto-Steganography Tool – CAD for Assurance

https://cadforassurance.org/tools/ip-ic-protection/crypto-steganography-tool/



https://cadforassurance.org/tools/ip-ic-protection/crypto-steganography-tool/

Crypto-Steganography Tool

By: Anirban Sengupta (IIT Indore) and Mahendra Rathor (IIT Indore)

Stage: RTL

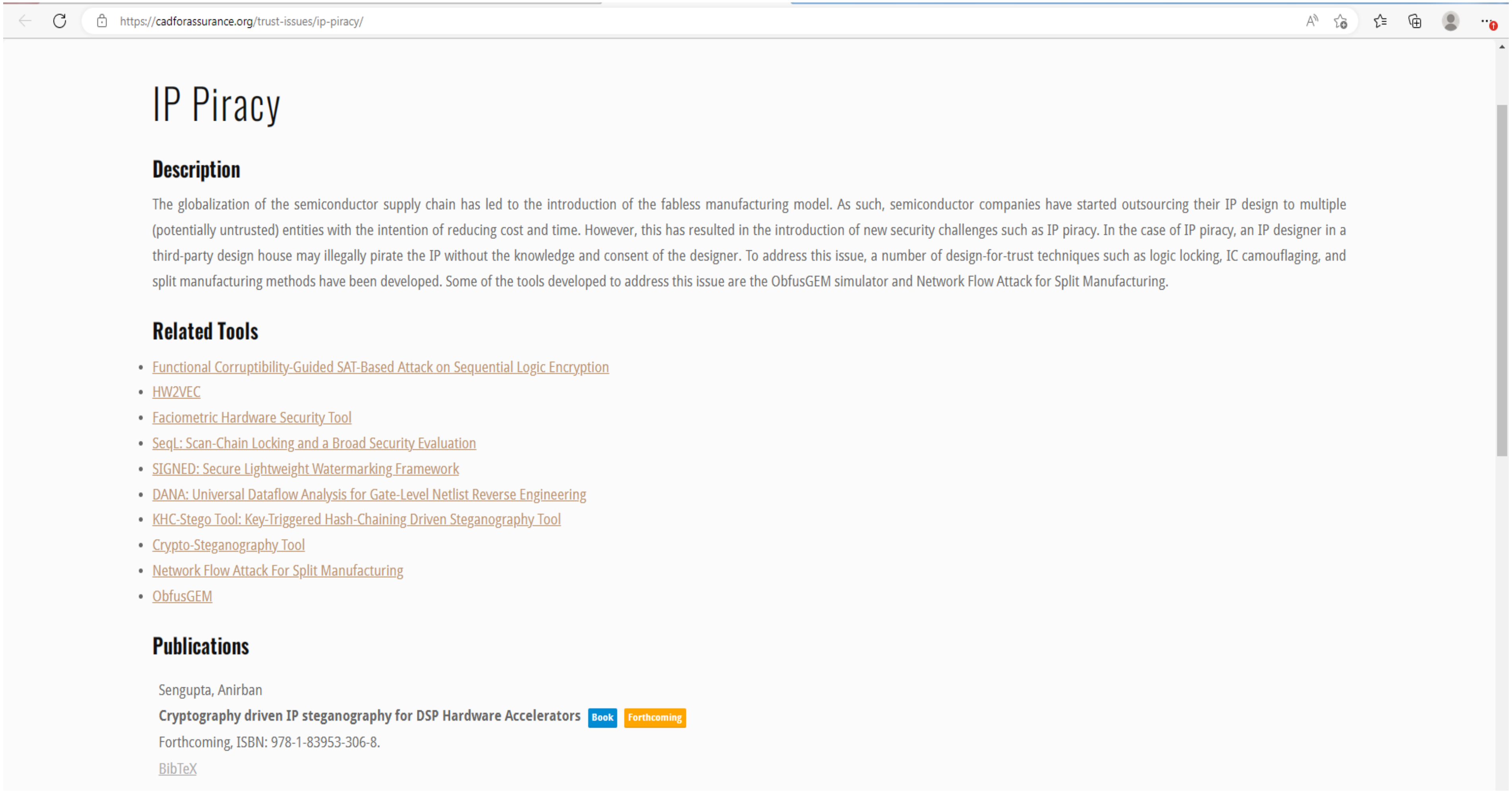
Crypto based dual phase hardware steganography for securing DSP circuits

stegokey1 000
stegokey2
stegokey3_A
stegokey3_B
stegokey3_C
stegokey3_D
stegokey3_E
stegokey3_F
stegokey4_A 000
stegokey4_B 000
stegokey4_C 000
stegokey4_D 000
stegokey4_E 000
stegokey4_F 010
stegokey_5

Summary

(Publicly available under ‘CAD for Assurance’ tools sponsored by IEEE CEDA, IEEE Hardware Security and Trust Technical Committee, and Warren B. Nelms Institute for the Connected World at University of Florida
(Public access of these tools > 3200 times))

IP Piracy – CAD for Assurance



IP Piracy

Description

The globalization of the semiconductor supply chain has led to the introduction of the fabless manufacturing model. As such, semiconductor companies have started outsourcing their IP design to multiple (potentially untrusted) entities with the intention of reducing cost and time. However, this has resulted in the introduction of new security challenges such as IP piracy. In the case of IP piracy, an IP designer in a third-party design house may illegally pirate the IP without the knowledge and consent of the designer. To address this issue, a number of design-for-trust techniques such as logic locking, IC camouflaging, and split manufacturing methods have been developed. Some of the tools developed to address this issue are the ObfusGEM simulator and Network Flow Attack for Split Manufacturing.

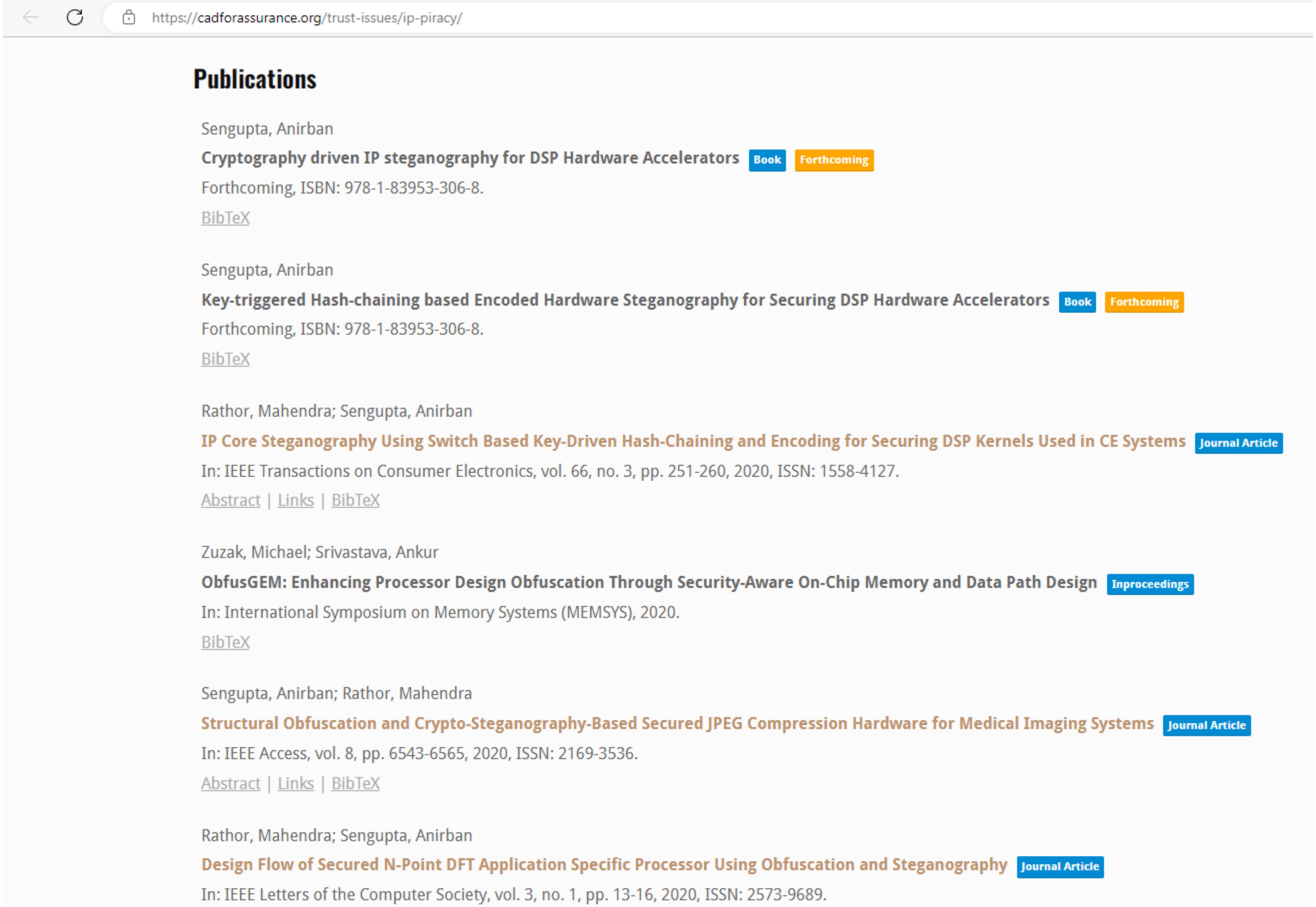
Related Tools

- Functional Corruptibility-Guided SAT-Based Attack on Sequential Logic Encryption
- HW2VEC
- Faciometric Hardware Security Tool
- SeqL: Scan-Chain Locking and a Broad Security Evaluation
- SIGNED: Secure Lightweight Watermarking Framework
- DANA: Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering
- KHC-Stego Tool: Key-Triggered Hash-Chaining Driven Steganography Tool
- Crypto-Steganography Tool
- Network Flow Attack For Split Manufacturing
- ObfusGEM

Publications

Sengupta, Anirban
Cryptography driven IP steganography for DSP Hardware Accelerators Book Forthcoming
Forthcoming, ISBN: 978-1-83953-306-8.
BibTeX

IP Piracy – CAD for Assurance



https://cadforassurance.org/trust-issues/ip-piracy/

Publications

Sengupta, Anirban

Cryptography driven IP steganography for DSP Hardware Accelerators Book Forthcoming

Forthcoming, ISBN: 978-1-83953-306-8.

BibTeX

Sengupta, Anirban

Key-triggered Hash-chaining based Encoded Hardware Steganography for Securing DSP Hardware Accelerators Book Forthcoming

Forthcoming, ISBN: 978-1-83953-306-8.

BibTeX

Rathor, Mahendra; Sengupta, Anirban

IP Core Steganography Using Switch Based Key-Driven Hash-Chaining and Encoding for Securing DSP Kernels Used in CE Systems Journal Article

In: IEEE Transactions on Consumer Electronics, vol. 66, no. 3, pp. 251-260, 2020, ISSN: 1558-4127.

Abstract | Links | BibTeX

Zuzak, Michael; Srivastava, Ankur

ObfusGEM: Enhancing Processor Design Obfuscation Through Security-Aware On-Chip Memory and Data Path Design Inproceedings

In: International Symposium on Memory Systems (MEMSYS), 2020.

BibTeX

Sengupta, Anirban; Rathor, Mahendra

Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging Systems Journal Article

In: IEEE Access, vol. 8, pp. 6543-6565, 2020, ISSN: 2169-3536.

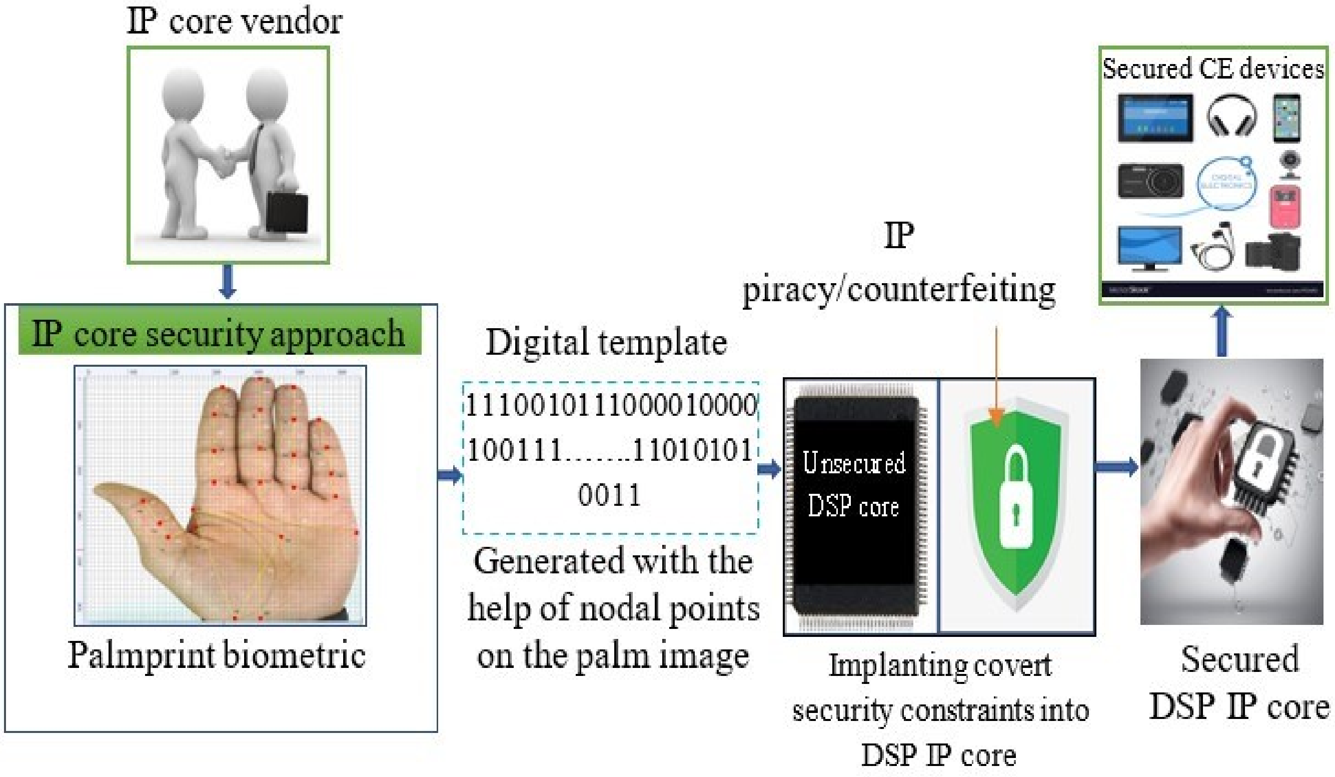
Abstract | Links | BibTeX

Rathor, Mahendra; Sengupta, Anirban

Design Flow of Secured N-Point DFT Application Specific Processor Using Obfuscation and Steganography Journal Article

In: IEEE Letters of the Computer Society, vol. 3, no. 1, pp. 13-16, 2020, ISSN: 2573-9689.

Palmprint based Hardware Security for IPP

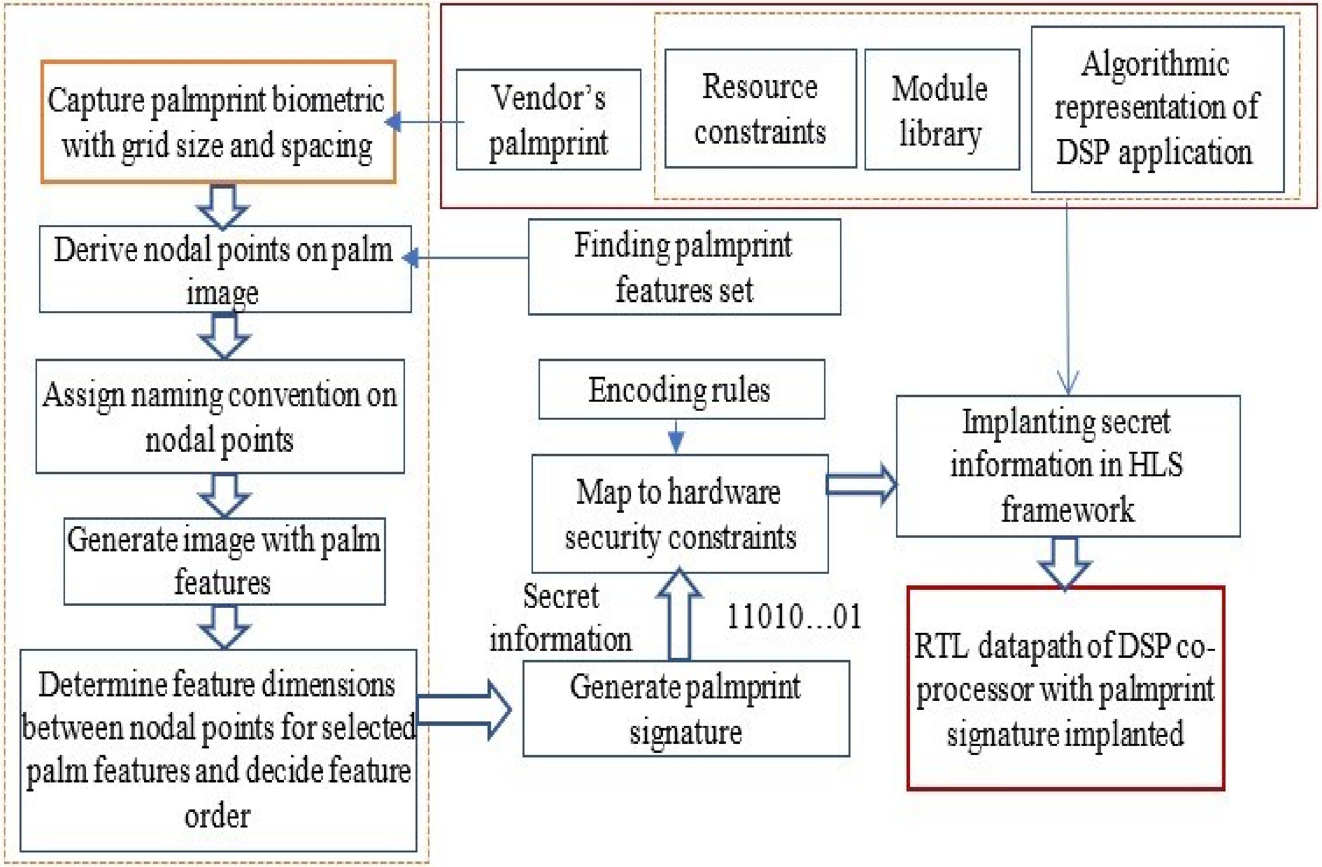


Securing reusable DSP IP core used in CE systems

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

Palmprint based Hardware Security for IPP


Capture palmprint biometric with grid size and spacing
Vendor's palmprint
Resource constraints
Module library
Algorithmic representation of DSP application
Derive nodal points on palm image
Finding palmprint features set
Assign naming convention on nodal points
Encoding rules
Map to hardware security constraints
Implanting secret information in HLS framework
Generate image with palm features
Secret information
11010…01
RTL datapath of DSP co-processor with palmprint signature implanted
Determine feature dimensions between nodal points for selected palm features and decide feature order
Generate palmprint signature

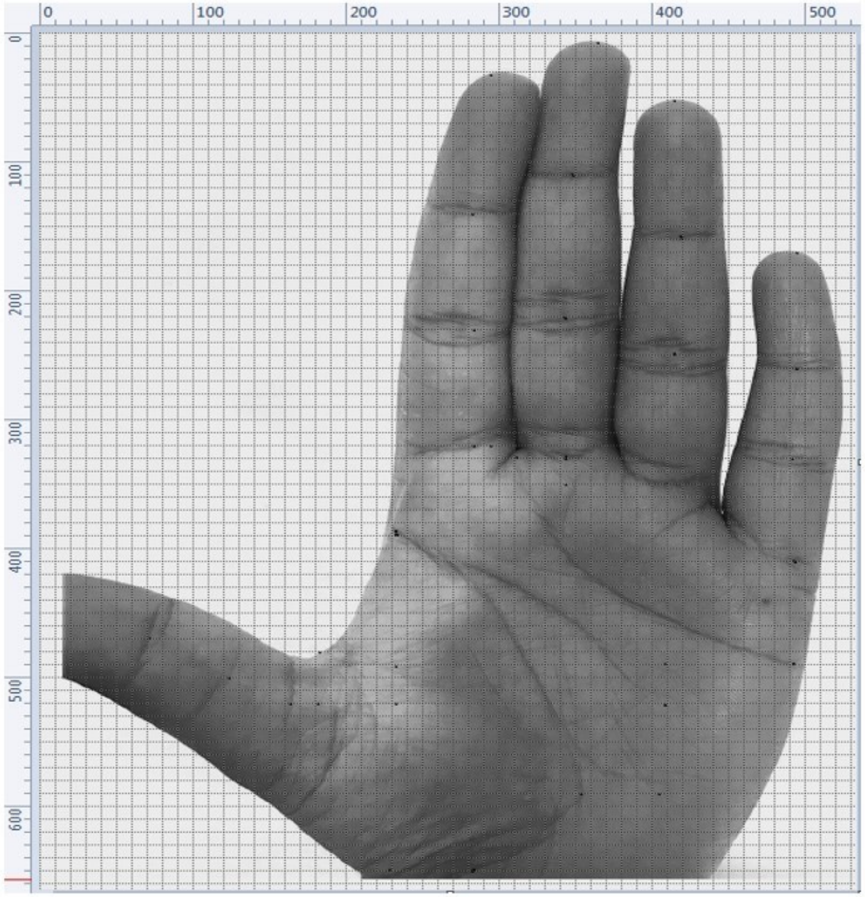
Anirban Sengupta, Rahul Chaurasia, Tarun Reddy "Contact-less Palmprint Biometric for Securing DSP Coprocessors used in CE systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 67, Issue: 3, August 2021, pp. 202-213

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

Palmprint based Hardware Security for IPP

- **Capturing palm image**

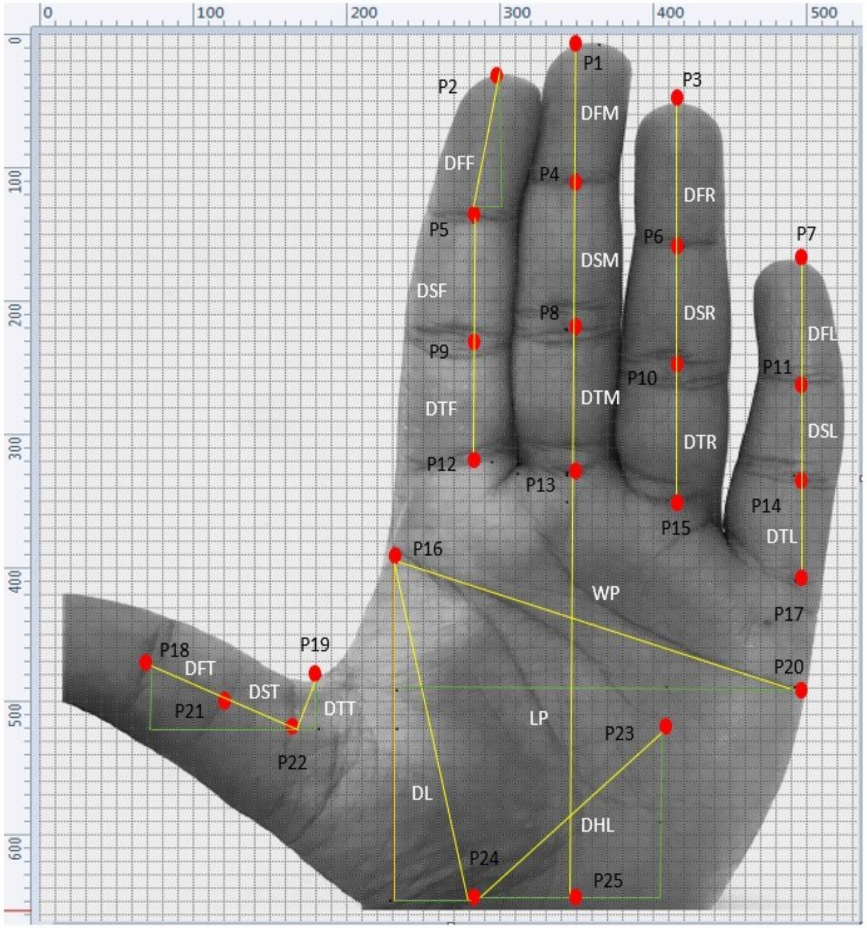
- At first the palmprint biometric of the authentic vendor or designer is captured and subsequently image of the captured palmprint is subjected to a specific grid size/spacing.
- This helps in generating the nodal points precisely.



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

Palmprint based Hardware Security for IPP

- **Generating image with chosen palm features and nodal points**



- Finding Palmprint Feature Set and Deriving Nodal Points for Captured Palmprint Biometric.

- Assigning Naming Convention and Deriving Palmprint Image with Selected Feature set.

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

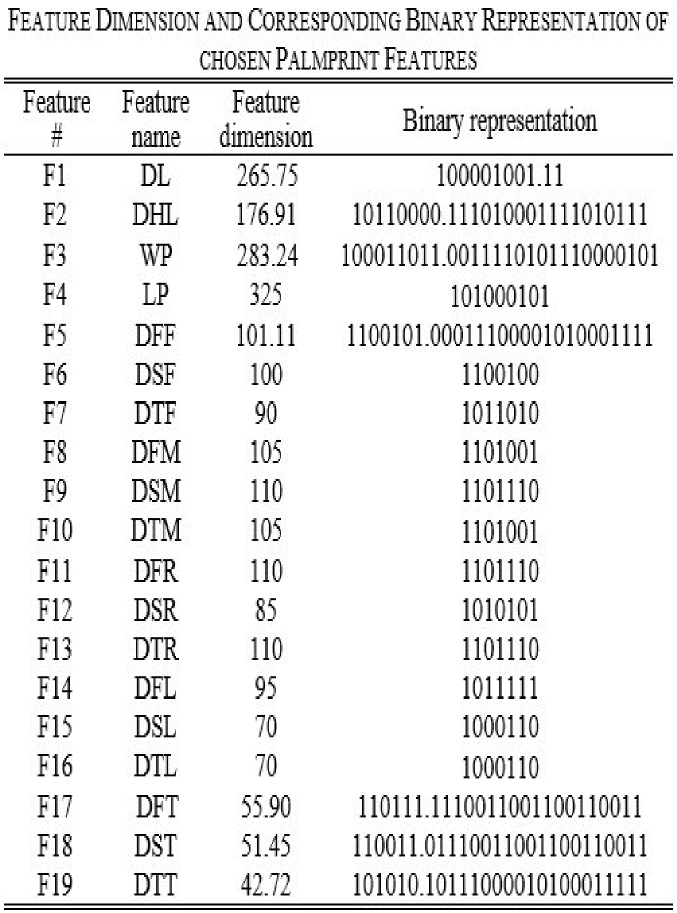
Palmprint based Hardware Security for IPP

Feature #	Palmprint feature name	Naming conventions of nodal points	Co-ordinates (x1,y1)- (x2,y2)
F1	Distance between start of life line and end of life line (DL)	(P16) – (P24)	(230, 390)- (285, 650)
F2	Distance between datum points of head line and life line (DHL)	(P23) – (P24)	(405, 520) -(285, 650)
F3	Width of the palm (WP)	(P16) – (P20)	(230, 390)- (495, 490)
F4	Length of palm (LP)	(P13) – (P25)	(350, 325)- (350, 650)
F5	Distance between first consecutive intersection points of forefinger (DFF)	(P2) – (P5)	(300, 30)- (285, 130)
F6	Distance between second consecutive intersection points of forefinger (DSF)	(P5) – (P9)	(285, 130)- (285, 230)
F7	Distance between third consecutive intersection points of forefinger (DTF)	(P9) – (P12)	(285, 230)- (285, 320)
F8	Distance between first consecutive intersection points of middle finger (DFM)	(P1) – (P4)	(350, 5)- (350, 110)
F9	Distance between second consecutive intersection points of middle finger (DSM)	(P4) – (P8)	(350, 110)- (350, 220)
F10	Distance between third consecutive intersection points of middle finger (DTM)	(P8) – (P13)	(350, 220)- (350, 325)
F11	Distance between first consecutive intersection points of ring finger (DFR)	(P3) – (P6)	(415, 50)- (415, 160)
F12	Distance between second consecutive intersection points of ring finger (DSR)	(P6) – (P10)	(415, 160)- (415, 245)
F13	Distance between third consecutive intersection points of ring finger (DTR)	(P10) – (P15)	(415, 245)- (415, 355)
F14	Distance between first consecutive intersection points of little finger (DFL)	(P7) – (P11)	(495, 170)- (495, 265)
F15	Distance between second consecutive intersection points of little finger (DSL)	(P11) – (P14)	(495, 265)- (495, 335)
F16	Distance between third consecutive intersection points of little finger (DTL)	(P14) – (P17)	(495, 335)- (495, 405)
F17	Distance between first consecutive intersection points of thumb finger (DFT)	(P18) – (P21)	(70, 470)- (120, 495)
F18	Distance between second consecutive intersection points of thumb finger (DST)	(P21) – (P22)	(120, 495)- (165, 520)
F19	Distance between starburst point and third intersection point of thumb (DTT)	(P19) – (P22)	(180, 480) -(165, 520)

SELECTED 19 PALMPRINT FEATURES, CORRESPONDING NODAL POINTS AND CO-ORDINATES

Palmprint based Hardware Security for IPP

- ➢ **Finding Feature Dimensions and Deriving Palmprint Signature Based on the Selected Feature Order**
- For example, a palmprint signature for the selected order of palmprint features ("DL⧺ DHL --- ⧺ DTT". Where, '⧺' represents the concatenation operator) after concatenation is as follows:
- Palmprint Signature: "100001001.1110110000.111010001111010111.---.11111"



FEATURE DIMENSION AND CORRESPONDING BINARY REPRESENTATION OF CHOSEN PALMPRINT FEATURES

Feature #	Feature name	Feature dimension	Binary representation
F1	DL	265.75	100001001.11
F2	DHL	176.91	10110000.111010001111010111
F3	WP	283.24	100011011.001111010111000101
F4	LP	325	101000101
F5	DFF	101.11	1100101.000111000010100011111
F6	DSF	100	1100100
F7	DTF	90	1011010
F8	DFM	105	1101001
F9	DSM	110	1101110
F10	DTM	105	1101001
F11	DFR	110	1101110
F12	DSR	85	1010101
F13	DTR	110	1101110
F14	DFL	95	1011111
F15	DSL	70	1000110
F16	DTL	70	1000110
F17	DFT	55.90	110111.11100110011001100011
F18	DST	51.45	110011.0111001100110011 0011
F19	DTT	42.72	101010.1011100001010001111 1

Note: Size of the palmprint signature varies based on the number of chosen palm features by the vendor for signature generation (depending on the required security strength corresponding to target application).

Palmprint based Hardware Security for IPP

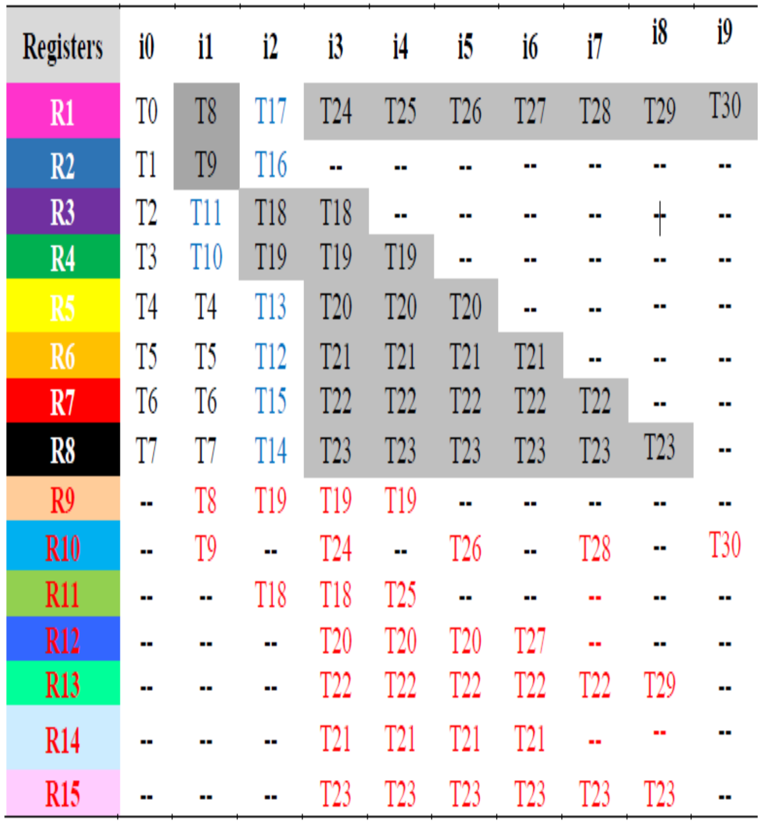
➢ Deriving the Covert Security Constraints and Implanting into Target IP core Design

- Post obtaining the digital template of palmprint signature, corresponding hardware security constraints are generated based on the encoding rules.
- The encoding rules for the signature bits are as follows:

The bit '1' embeds an edge between node pair (odd-odd), bit '0' embeds an edge between node pair (even-even). Moreover, the binary bit '.' embeds an edge between node pair (0, integer) into the CIG of target DSP design.

- For example, for a sample design having 31 storage variables (T0 to T30) executing through 8 registers (R1 to R8), the generated security constraints corresponding to the zeros are: <T0, T2>, <T0, T4>---<T16, T28>, the security constraints corresponding to ones are: <T1, T3>, -----<T27, T29> and corresponding to the binary points are: <T0, T1>, <T0, T3>, -- -, <T0, T11>.

TABLE I
REGISTER ALLOCATION OF A TARGET HARDWARE IP CORE POST IMPLANTATION



Registers	i0	i1	i2	i3	i4	i5	i6	i7	i8	i9
R1	T0	T8	T17	T24	T25	T26	T27	T28	T29	T30
R2	T1	T9	T16	--	--	--	--	--	--	--
R3	T2	T11	T18	T18	--	--	--	--	+	--
R4	T3	T10	T19	T19	T19	--	--	--	--	--
R5	T4	T4	T13	T20	T20	T20	--	--	--	--
R6	T5	T5	T12	T21	T21	T21	T21	--	--	--
R7	T6	T6	T15	T22	T22	T22	T22	T22	--	--
R8	T7	T7	T14	T23	T23	T23	T23	T23	T23	--
R9	--	T8	T19	T19	T19	--	--	--	--	--
R10	--	T9	--	T24	--	T26	--	T28	--	T30
R11	--	--	T18	T18	T25	--	--	--	--	--
R12	--	--	--	T20	T20	T20	T27	--	--	--
R13	--	--	--	T22	T22	T22	T22	T22	T29	--
R14	--	--	--	T21	T21	T21	T21	--	--	--
R15	--	--	--	T23	T23	T23	T23	T23	T23	--

RESULTS AND DISCUSSION

- The proposed palmprint biometric approach is analyzed in terms of security and design overhead.

Security Analysis:

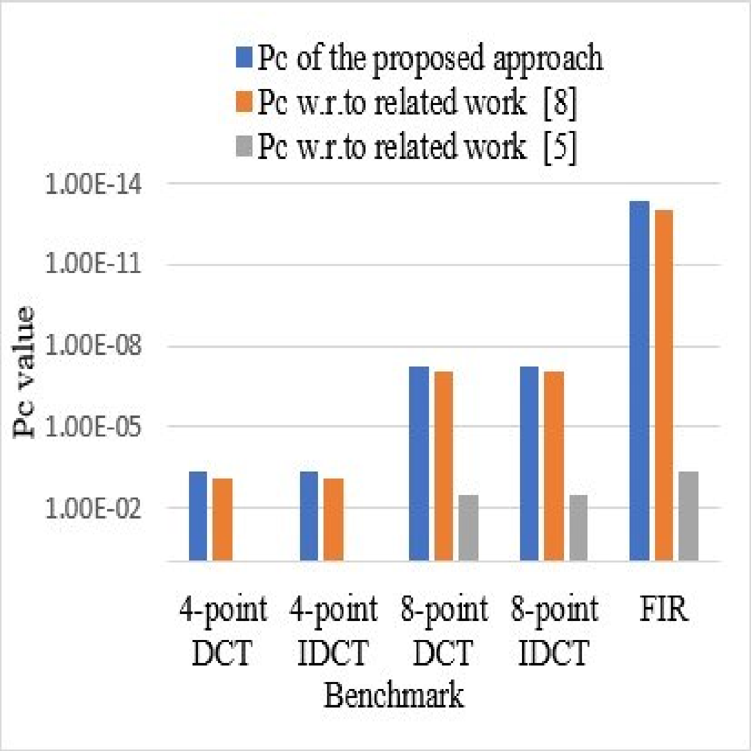
- The security of the proposed approach is analyzed in terms of probability of coincidence (Pc) and temper tolerance (TT) ability.
- The Pc metric is formulated as follows:

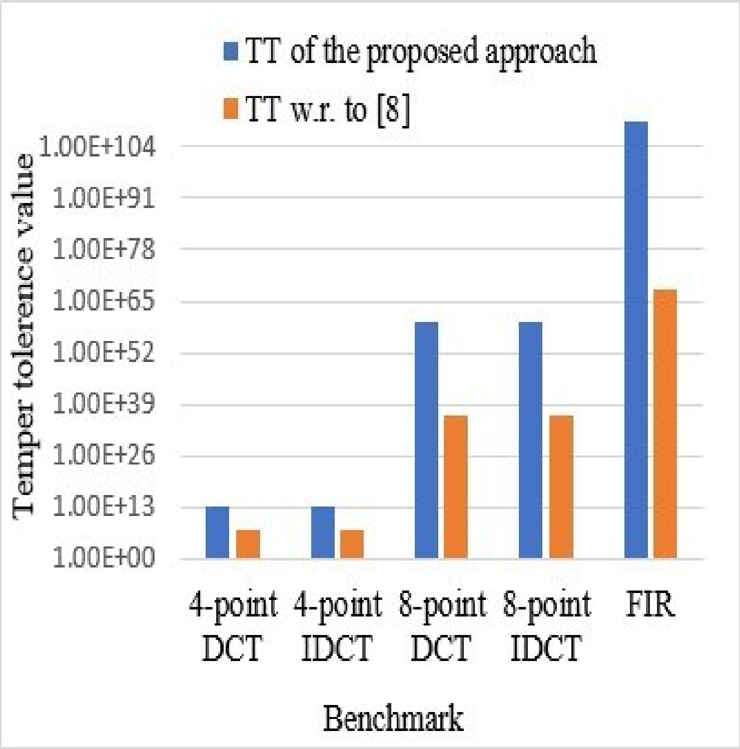
$$\mathrm{Pc} = \left(1 - \frac{1}{\tau}\right)^{S} \qquad (1)$$

- The TT metric is formulated as follows:

$$\mathrm{TT} = P^{Q} \qquad (2)$$

Comparison of Probability of Coincidence and Tamper Tolerance Ability with Previous Works





[5] A. Sengupta and M. Rathor, “IP core steganography for protecting DSP kernels used in CE systems,” IEEE Trans. Consum. Electron., vol. 65, no. 4, pp. 506-515, 2019.

[8] A. Sengupta and M. Rathor, “Securing hardware accelerators for CE systems using biometric fingerprinting,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 28, no. 9, pp. 1979-1992, 2020, doi: 10.1109/TVLSI.2020.2999514.

Design Cost Overhead Post Implanting the Palmprint Signature

Design cost Analysis:

Design cost can be measured using the following metric:

$$Z = h1 \frac{\nabla t}{\nabla \max} + h2 \frac{\Delta t}{\Delta \max} \qquad (3)$$

- Design cost overhead post implanting the palmprint signature into the design is minimal (0.2%-0.8%) as evident from Table II.

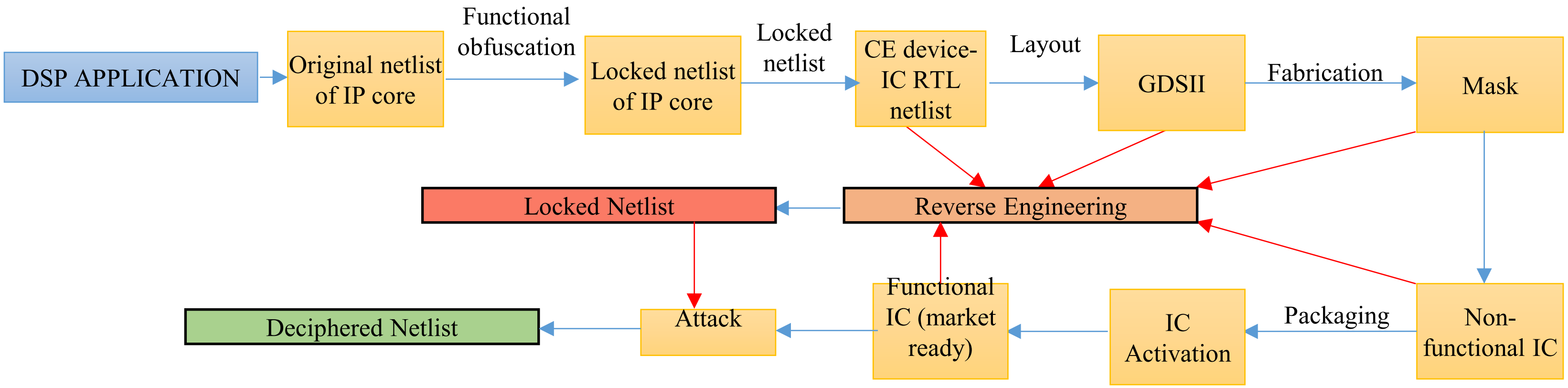
DESIGN COST PRE AND POST EMBEDDING PALMPRINT
BIOMETRIC CONSTRAINTS

Benchmarks	Design cost of baseline	Design cost of palmprint implanted design	% Cost overhead
4-pointDCT	0.5611	0.5623	0.2%
4-point IDCT	0.5611	0.5623	0.2%
8-pointDCT	.4721	.4740	0.4%
8-point IDCT	.4721	.4740	0.4%
FIR	.4443	.4479	0.8%

Key Features

- Presents a novel contact-less palmprint biometric security approach for securing the reusable hardware IP core.
- The proposed approach enables the seamless detection of pirated/counterfeited DSP IPcores used in CE systems, thus ensuring consumers safety and protecting IP/brand value, returning revenue and resolving traffic bleed.
- Any DSP based intellectual property (IP) core can be embedded with proposed palmprint signature to distinguish between authentic and its fake versions.
- The biometric palmprint constraints generated through the proposed approach is non-replicable and non-vulnerable as compared to hardware steganography and hardware watermarking approaches.
- The proposed work presents stronger security and minimal design overhead in parallel, compared to the existing state of the art approaches.

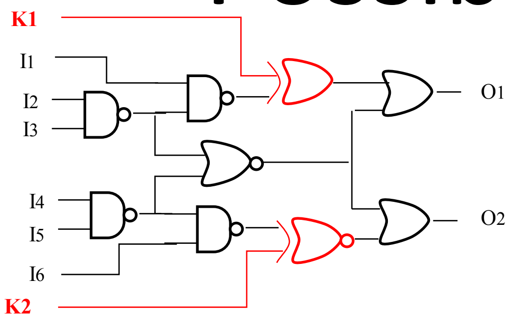
How Hardware of a CE device can be compromised ?



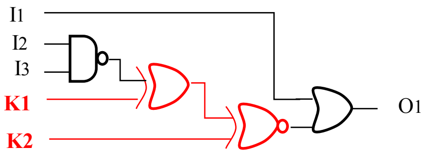
- Reverse engineering (RE) of a DSP core is a process of gaining the complete understanding of its **functionality**, **design** and **structure**.
- However, RE can be used for dishonest intention such as **overbuilding**, **piracy**, or **counterfeiting** a DSP core or inserting a **hardware Trojan**.

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

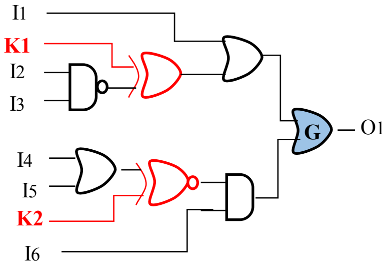
Possible Threat Scenarios



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.

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

The Vulnerability of Functional Obfuscation towards Different Attacks

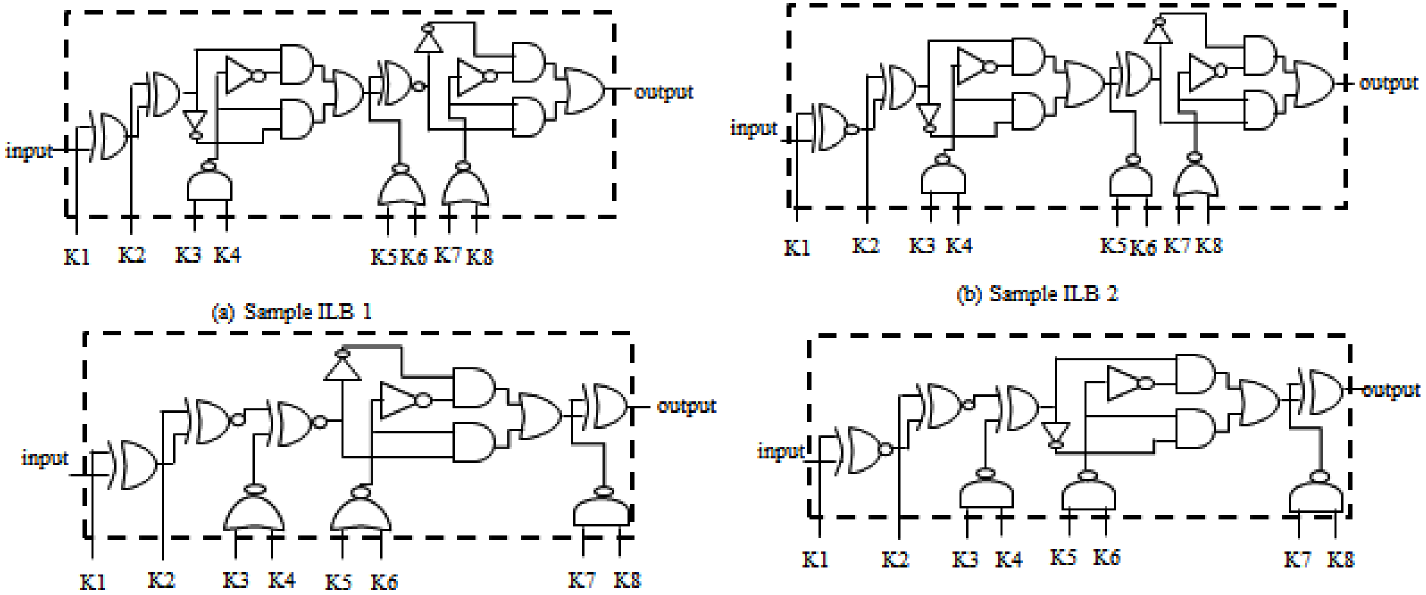
❑ ***Key sensitization attack:***

- An attacker can extract keys of a locked (functionally obfuscated) netlist through key sensitization attack.
- To mount this attack, the attacker also requires a functional IC (can be obtained from open market) along with the obfuscated netlist (may be obtained through RE).

➢ **Can sensitize the key through following possibilities :**

- The attacker can sensitize a key-bit at primary output by controlling the primary inputs of the design. To do so, the attacker needs to identify the input pattern that can sensitize the correct key-bits to the primary output.
- The Attacker tries to find isolated key-gates in the obfuscated netlist. This is because the key-bits are easy to sensitize through isolated key-gates. (If a key-gate is not connected to other key gates (through any path) in the obfuscated design, then it is termed as an isolated key-gate).
- If the attacker finds a sequence of key gates in the obfuscated design, then he/she can substitute it by a single gate. This leads to reduction in key-bits. Thus, run of key-gates makes obtaining key-bits easier for an attacker.
- In the path of sensitization of a key-bit, the effect of other key-bits can be nullified by muting the relevant key-gates.

Proposed IP core locking blocks (ILBs)



(a) Sample ILB 1

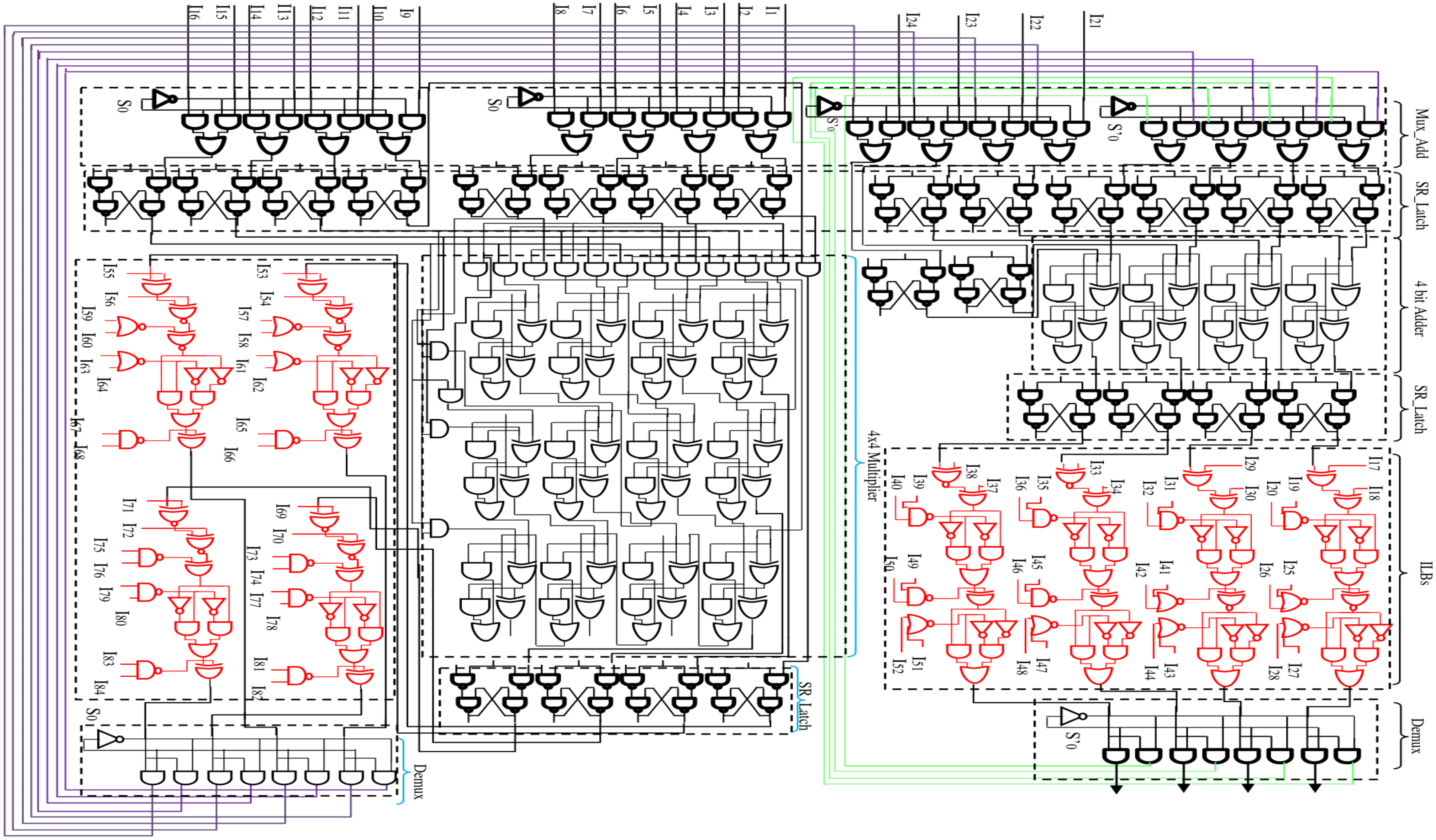
(b) Sample ILB 2

(c) Sample ILB 3

(d) Sample ILB 4

- 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.

Obfuscated gate structure of 4-bit FIR designed using



Security of Functionally Obfuscated DSP core against Removal Attack

- The security against removal attack can be provided by making the ILBs structurally reconfigurable
- That is the gate structures of the ILB architecture can be configured according to the values at the key bits.
- In other words, the ILB gate structure used (in the obfuscated netlist) is never fixed to make it undetectable to an attacker.
- Different ILB gate structures are used based on the reconfiguration to confuse the attacker and thwart removal attack.
- This is possible because various structures of ILBs can be generated using different combinations of same basic gates (XOR, XNOR, AND, NAND, OR, NOT gates).
- Yet, each ILB structure is capable to provide similar security strength.

Anirban Sengupta, Mahendra Rathor "Security of Functionally Obfuscated DSP cores"**, IET Book "Frontiers in Securing Hardware IP Cores: Forensic detective control and obfuscation techniques"**, 2020, ISBN: 978-1-83953-031-9/978-1-83953-032-6

Security using custom SHA-512 based ILBs-Key generation Hardware

- The ILBs structures are reconfigured based on output of custom SHA- 512 based ILBs-key generation logic. Thus, detection of ILBs in the complex DSP netlist becomes difficult because its architecture is not known to the attacker in advance.
- Post synthesis, the ILBs gate structure change and get camouflaged (unrecognizable) the form of basic gates in the entire design netlist. Thus, the removal attack on ILBs becomes extremely difficult.
- Additionally, since authors have designed a custom SHA-512 based ILBs-key generation hardware (not publicly available), therefore post synthesis, its detection in the design netlist (comprising of DSP core and ILBs) is highly challenging.
- The crypto hash function (SHA-512) provides some strong security features such as collision resistance, uniformity , deterministic .

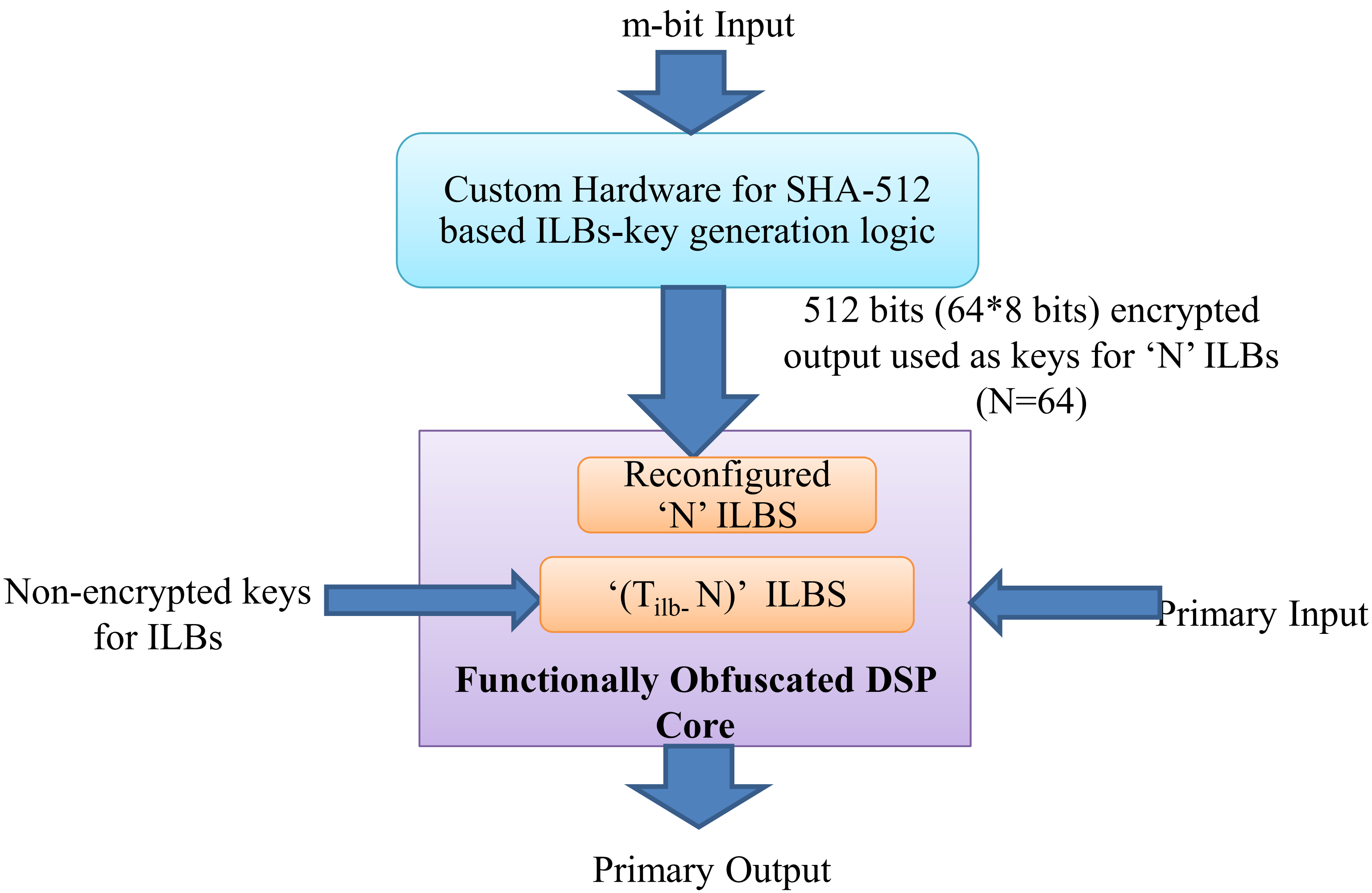
Anirban Sengupta, Mahendra Rathor "Security of Functionally Obfuscated DSP cores"**, IET Book "Frontiers in Securing Hardware IP Cores: Forensic detective control and obfuscation techniques"**, 2020, ISBN: 978-1-83953-031-9/978-1-83953-032-6

❖ Features of this approach

- To know the 512-bit hash-digest, an attacker needs to find 1024 bits of plaintext input of SHA-512 algorithm.
- Therefore, for an attacker to know the architecture of 64 reconfigured ILBs, 512 bits of ILBs keys are required to be decoded from 1024 bits of plaintext input of SHA-512
- To reconfigure up to 64 ILBs, one SHA-512 based key generation block needs to be integrated with a functionally obfuscated DSP design.
- It incurs considerably low area overhead than four instances of AES-128 required to structurally reconfigure the same number of ILBs

Anirban Sengupta, Mahendra Rathor "Security of Functionally Obfuscated DSP cores"**, IET Book "Frontiers in Securing Hardware IP Cores: Forensic detective control and obfuscation techniques"**, 2020, ISBN: 978-1-83953-031-9/978-1-83953-032-6

Overview Protection scenario using SHA-512 based ILBs-key generation hardware


m-bit Input
Custom Hardware for SHA-512 based ILBs-key generation logic
512 bits (64*8 bits) encrypted output used as keys for 'N' ILBs (N=64)
Reconfigured 'N' ILBS
Non-encrypted keys for ILBs
'(T_{ilb-}N)' ILBS
Primary Input
Functionally Obfuscated DSP Core
Primary Output

Anirban Sengupta, Mahendra Rathor "Security of Functionally Obfuscated DSP cores"**, IET Book "Frontiers in Securing Hardware IP Cores: Forensic detective control and obfuscation techniques"**, 2020, ISBN: 978-1-83953-031-9/978-1-83953-032-6

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
- Anirban Sengupta, Saumya Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis", IEEE Access, Invited paper, Volume:4, Issue: 99, pp. 2198 - 2215, May 2016 .

Conclusion

The future is:

Hardware/Chip Design with Energy-Security Tradeoff..

Thank you