

IEEE Computer Society Chapter, IEEE Hyderabad Section

Oct 4, 2024

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

PROF. ANIRBAN SENGUPTA, PROFESSOR

FIET, FBCS, FIETE

IEEE Distinguished Visitor of IEEE Computer Society

IEEE Distinguished Lecturer of IEEE Consumer Technology Society

IEEE Senior Member

Editor-in-Chief, IET Computers and Digital Techniques (CDT)

Associate Editor, IEEE Transactions on VLSI Systems (of IEEE CS/IEEE CAS Society)

Associate Editor, IEEE Embedded Systems Letters (of IEEE CEDA)

Former Chair, IEEE Computer Society Technical Committee on VLSI

Former Chair and Board Member, IEEE Consumer Technology Society Technical Committee on Security & Privacy

Former Editor-in-Chief, IEEE VLSI Circuits & Systems Letter (of IEEE Computer Society TCVLSI)

Former Associate Editor, IEEE Transactions on Consumer Electronics (TCE)

Former Associate Editor, IEEE Transactions on Aerospace & Electronic Systems (TAES)

Former Guest Editor, IEEE Transactions on CAD of Integrated Circuits and Systems (TCAD)

Former Visiting Scientist, Indian Statistical Institute (ISI)

Department of Computer Science and Engineering

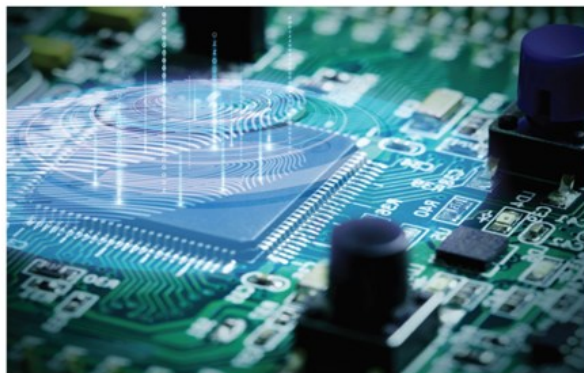
Indian Institute of Technology Indore

Email: asengupt@iiti.ac.in

Web: <http://www.anirban-sengupta.com>

Secured Hardware Accelerators for DSP and Image Processing Applications

Anirban Sengupta



Sengupta

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Anirban Sengupta and Saraju P. Mohanty



Sengupta and Mohanty

Frontiers in Securing IP Cores

Forensic detective control
and obfuscation techniques

Anirban Sengupta



Sengupta

Sengupta et al. (Eds.)

CCIS
1066

VLSI Design and Test

VDAT
2019

Anirban Sengupta · Sudeb Dasgupta ·
Virendra Singh · Rohit Sharma ·
Santosh Kumar Vishvakarma (Eds.)

Communications in Computer and Information Science 1066

VLSI Design and Test

23rd International Symposium, VDAT 2019
Indore, India, July 4–6, 2019
Revised Selected Papers

 Springer

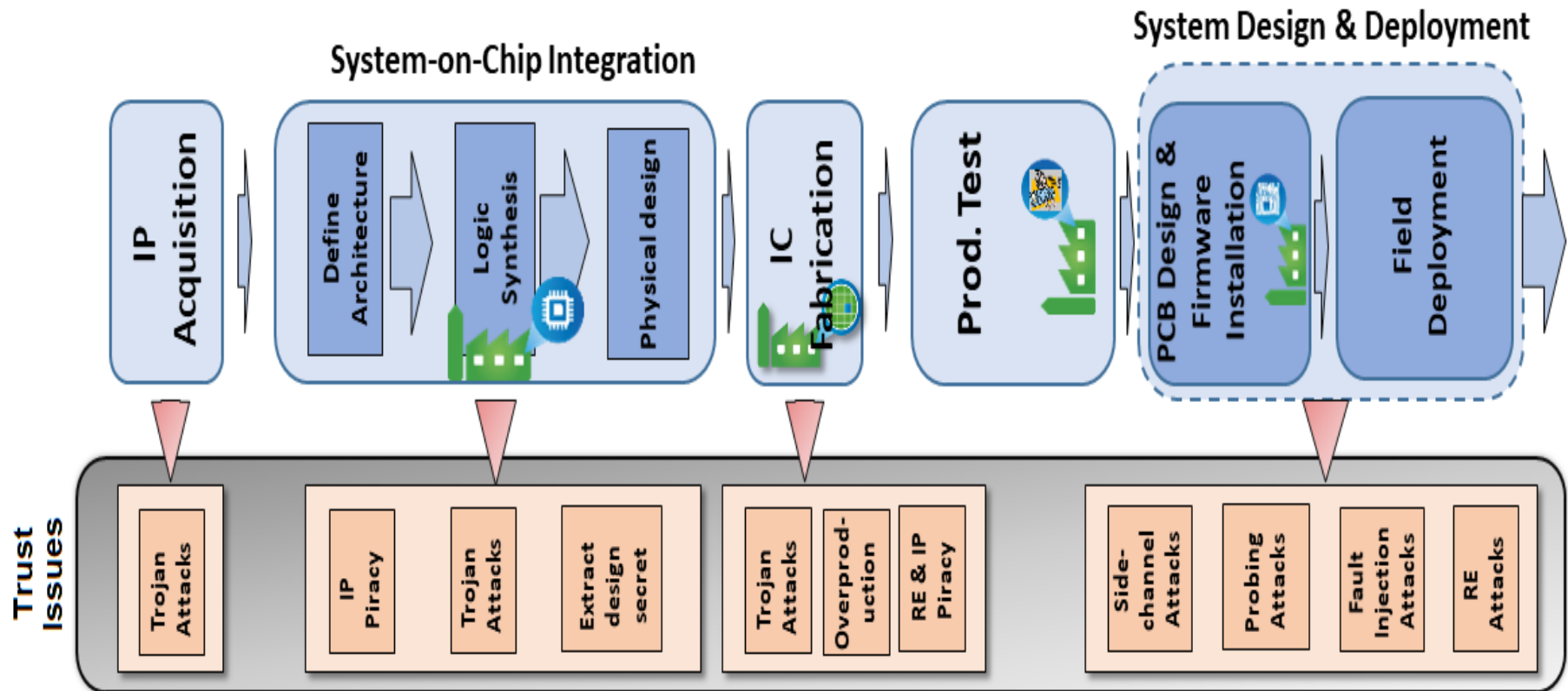
Introduction

- 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

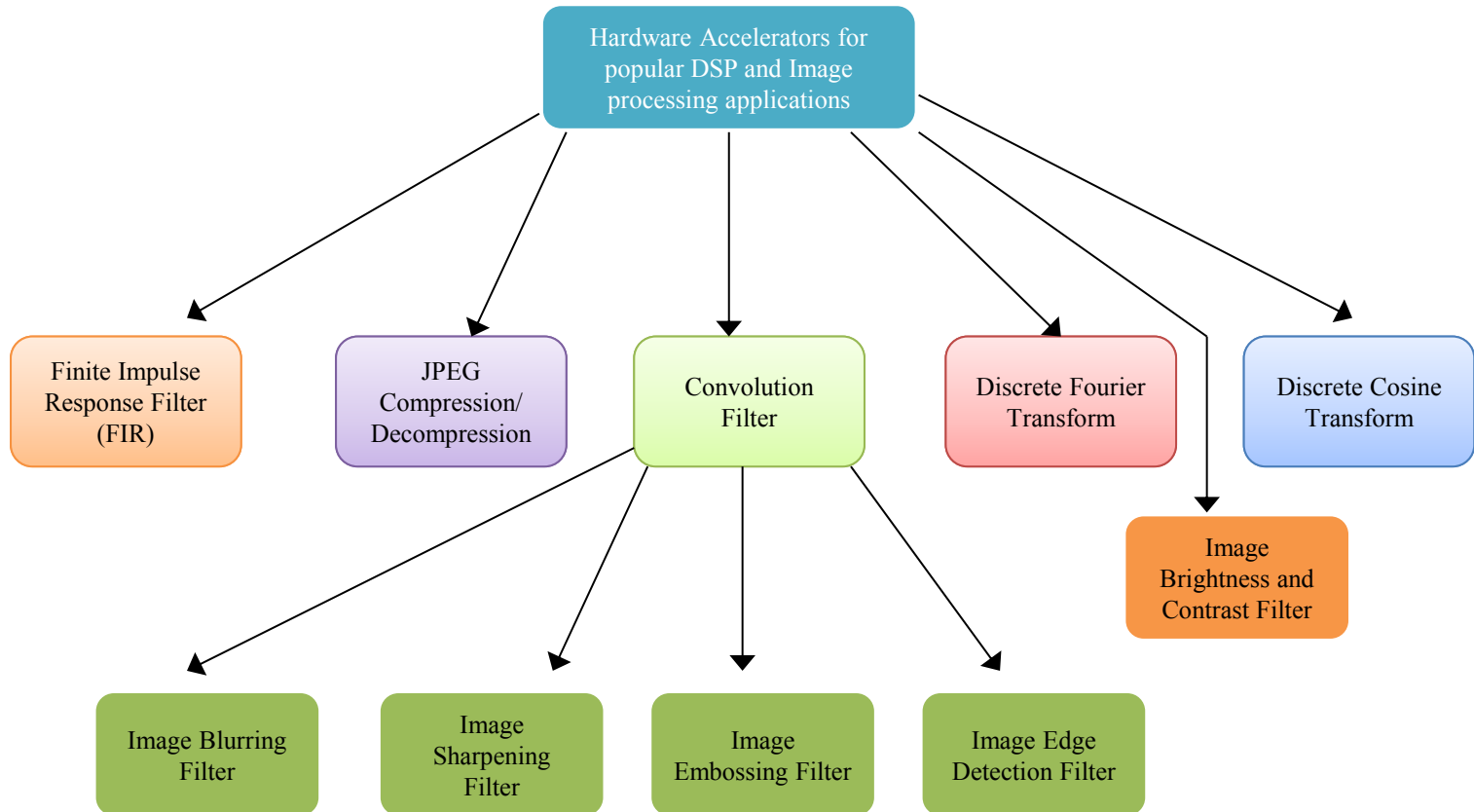
Anirban Sengupta, Mahendra Rathor "Protecting DSP Kernels using Robust Hologram based Obfuscation", **IEEE Transactions on Consumer Electronics**, 2019

IP Core Protection and Hardware Security

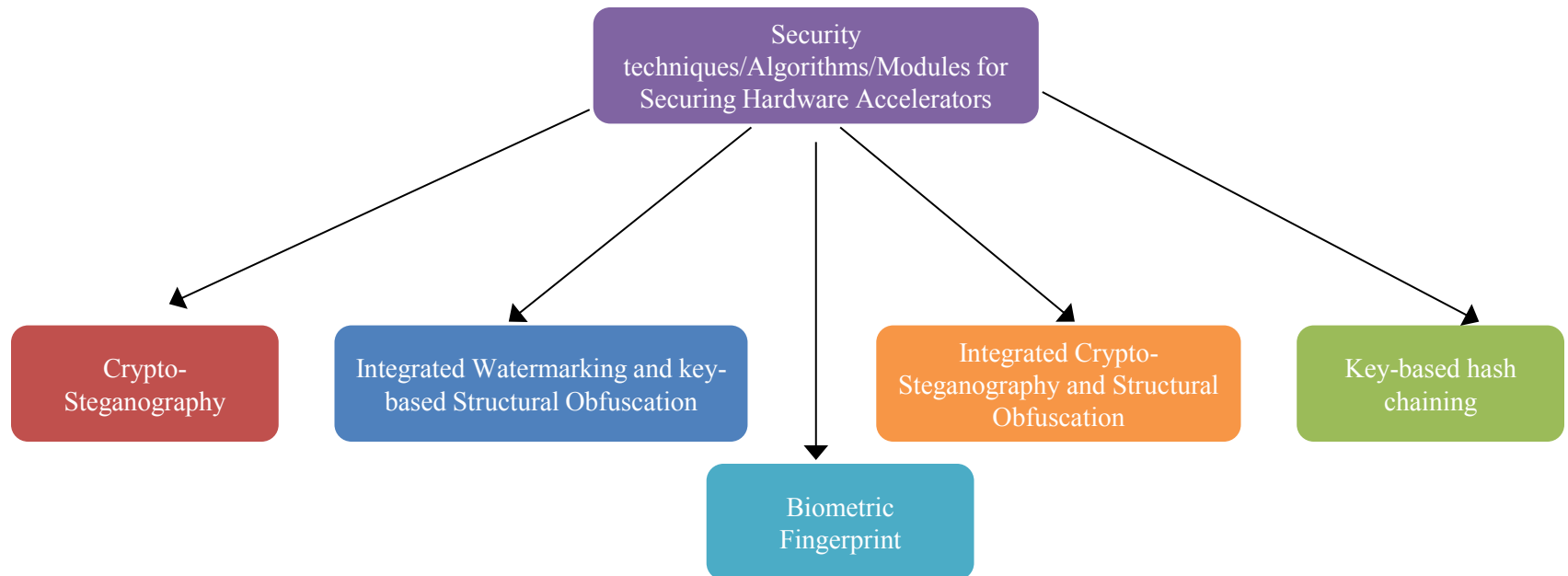


CAD for Assurance – CAD for Assurance of Electronic Systems

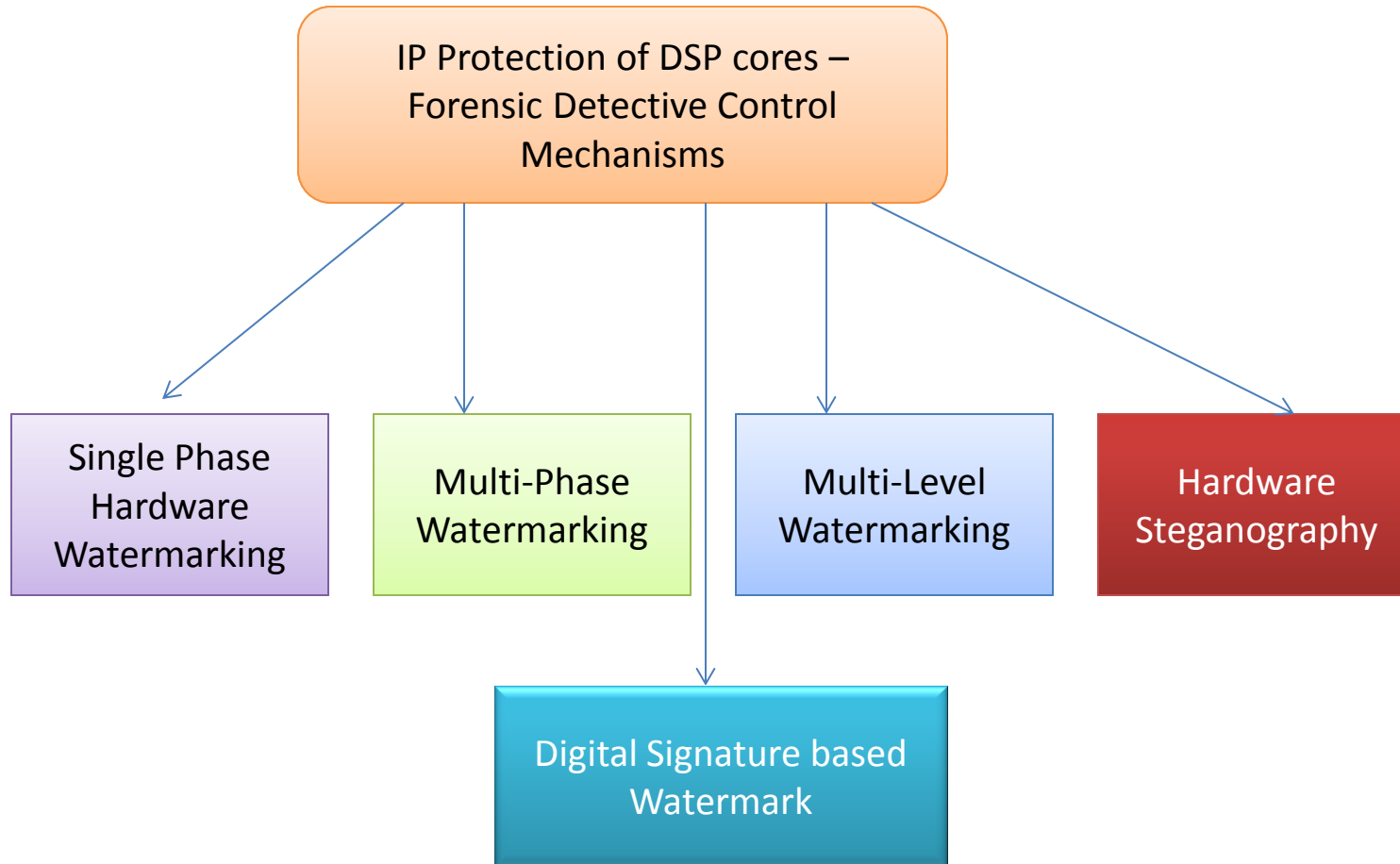
Hardware accelerators: Example



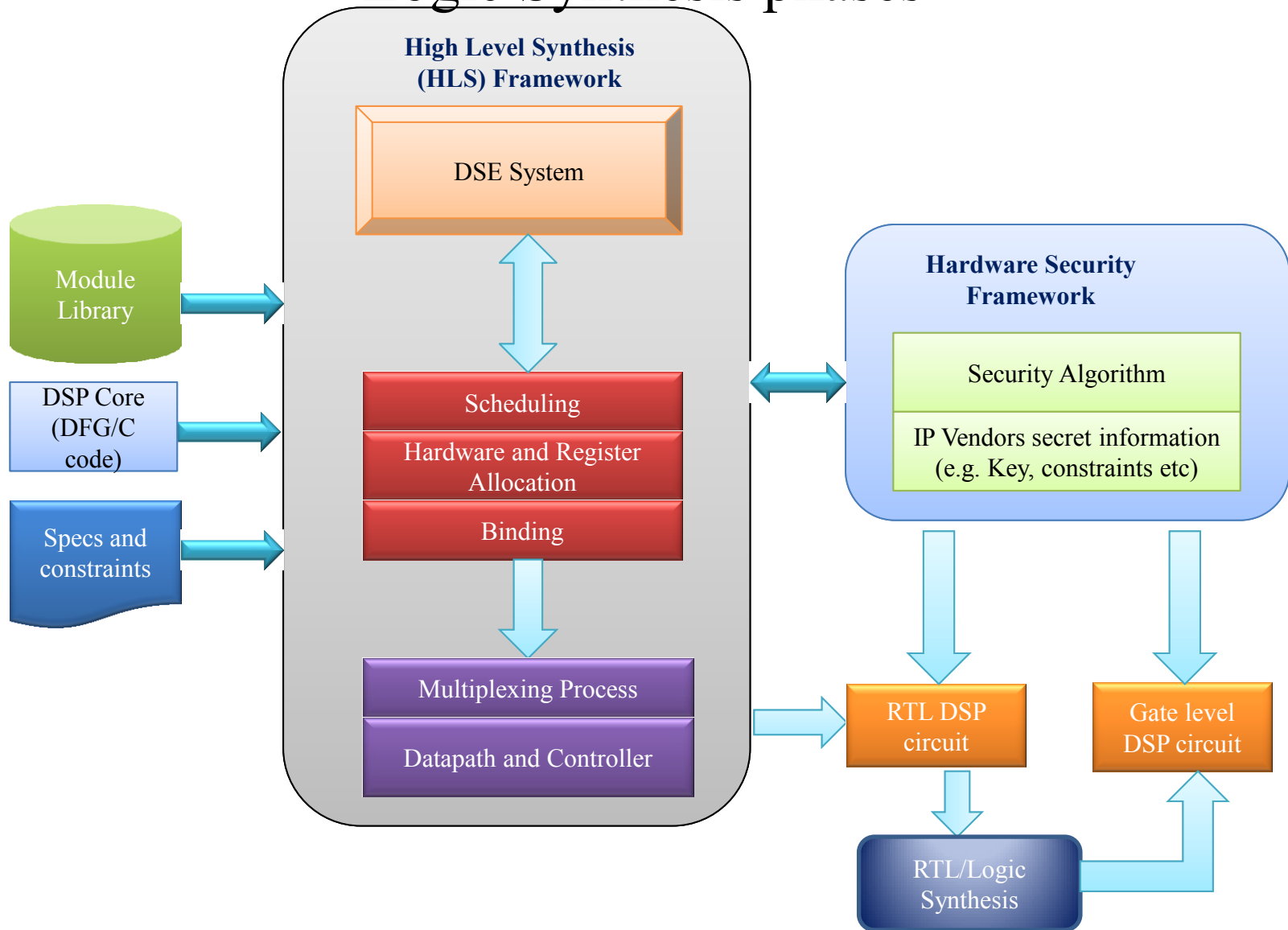
Hardware security techniques for securing hardware accelerators



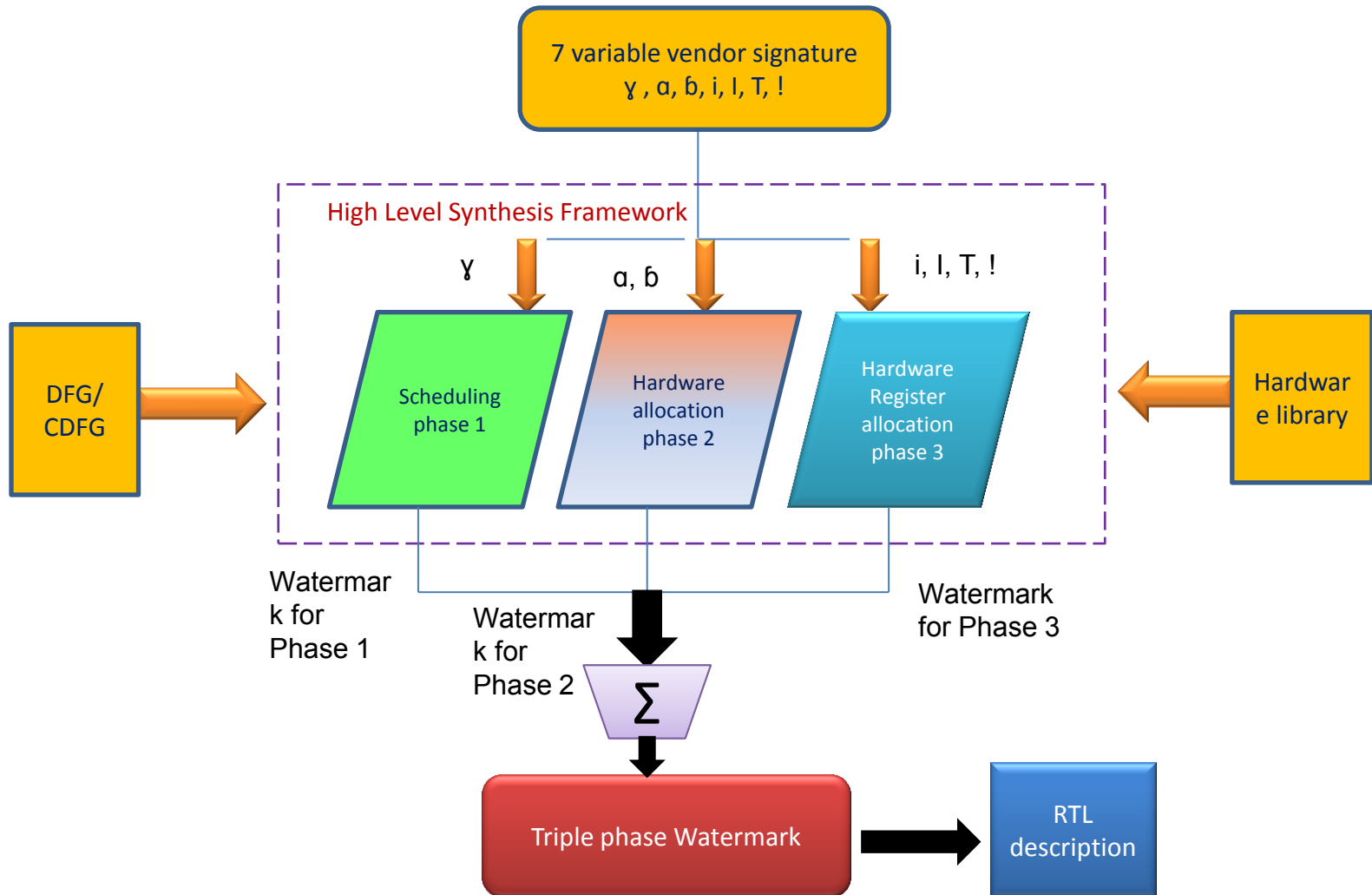
IP Protection of DSP cores – Forensic Detective Control Mechanisms



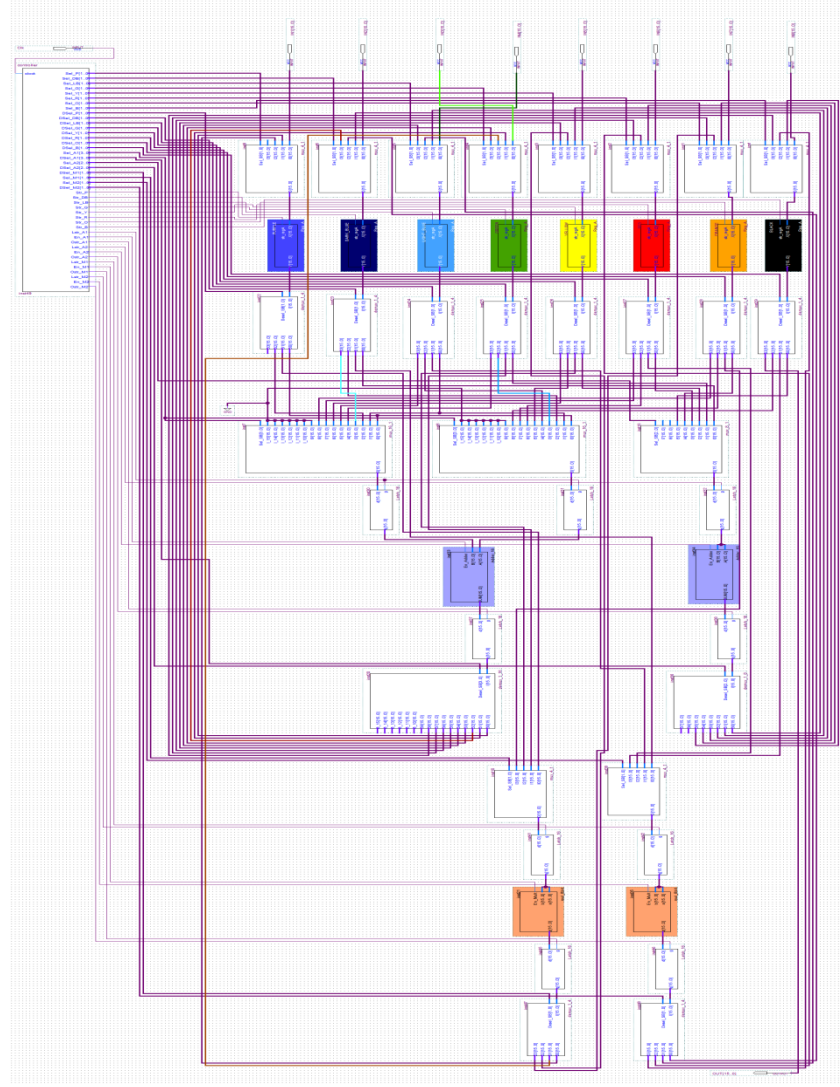
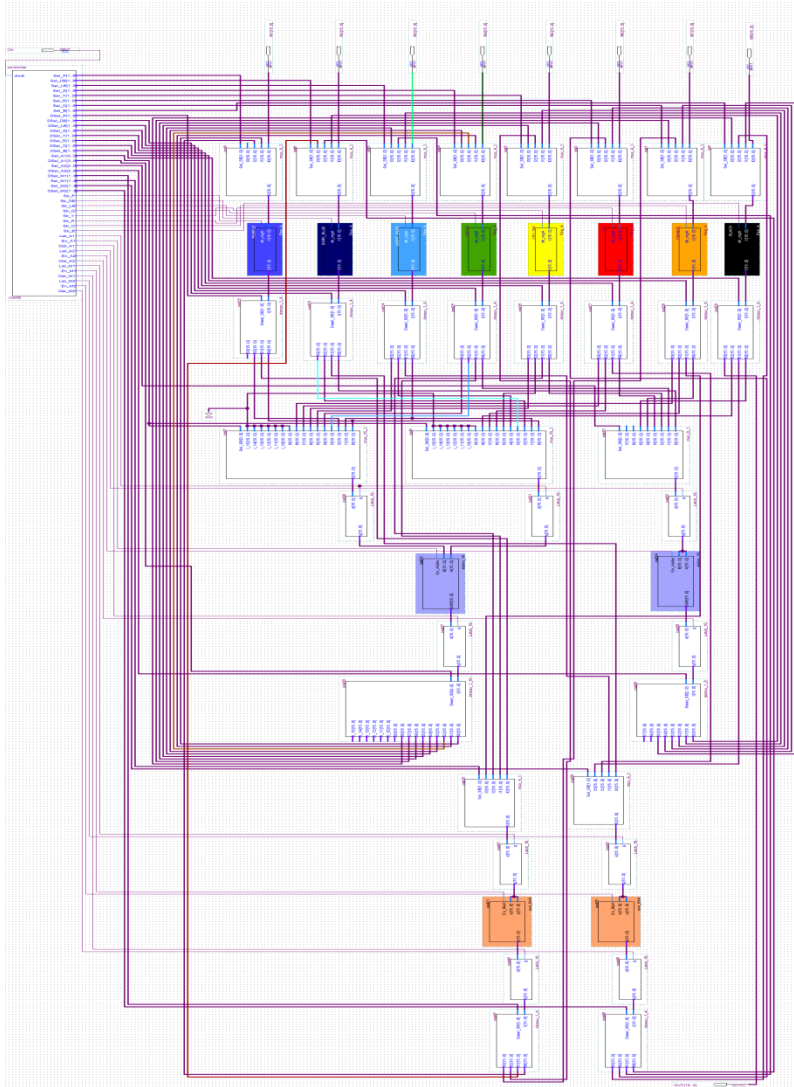
Hardware Security Algorithms integrated with HLS and Logic Synthesis phases



HLS based Triple phase watermarking



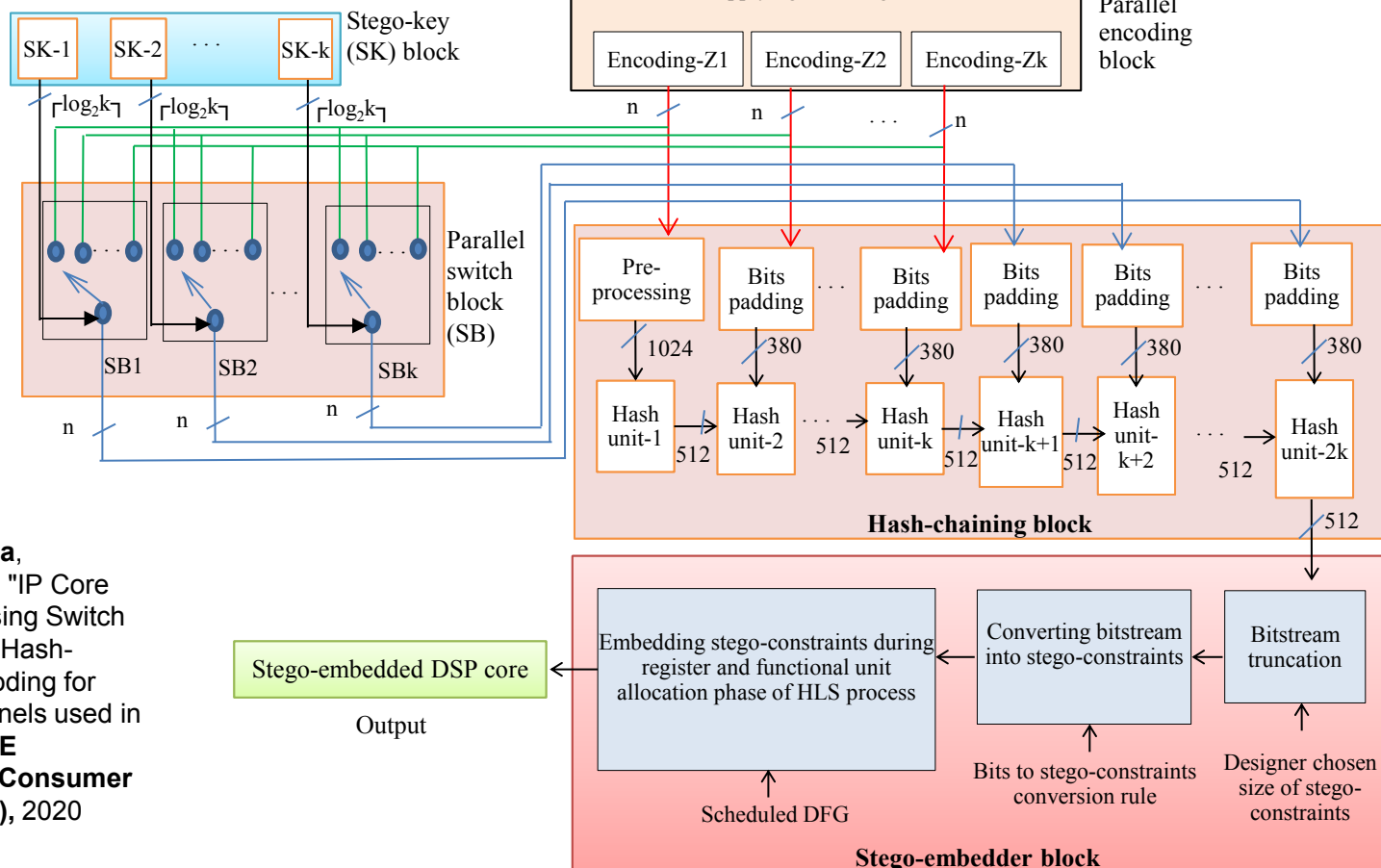
Watermarked FIR Vs Non-Watermarked FIR at RTL



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

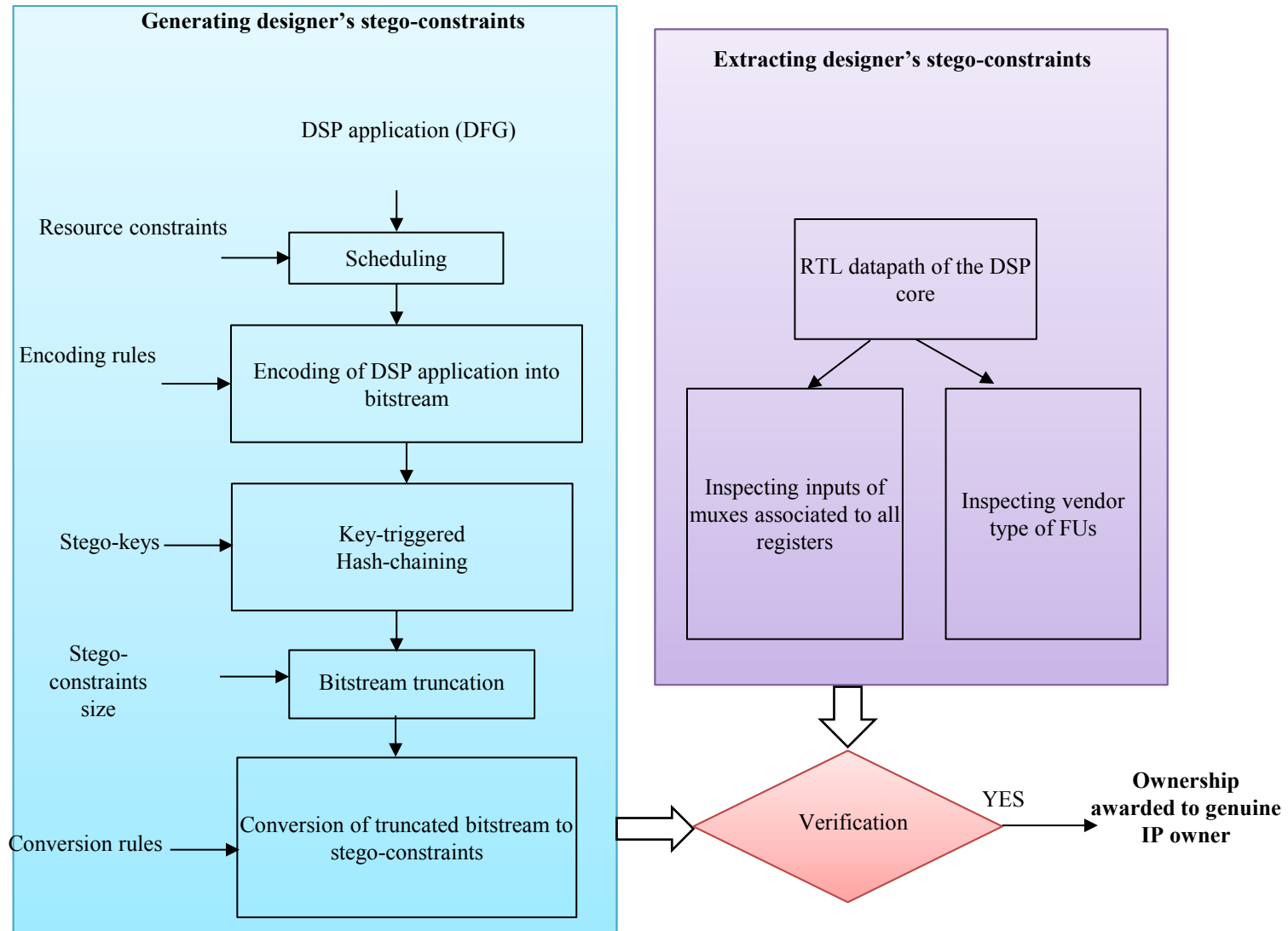
Securing DSP cores using key-triggered hash-chaining based steganography

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.

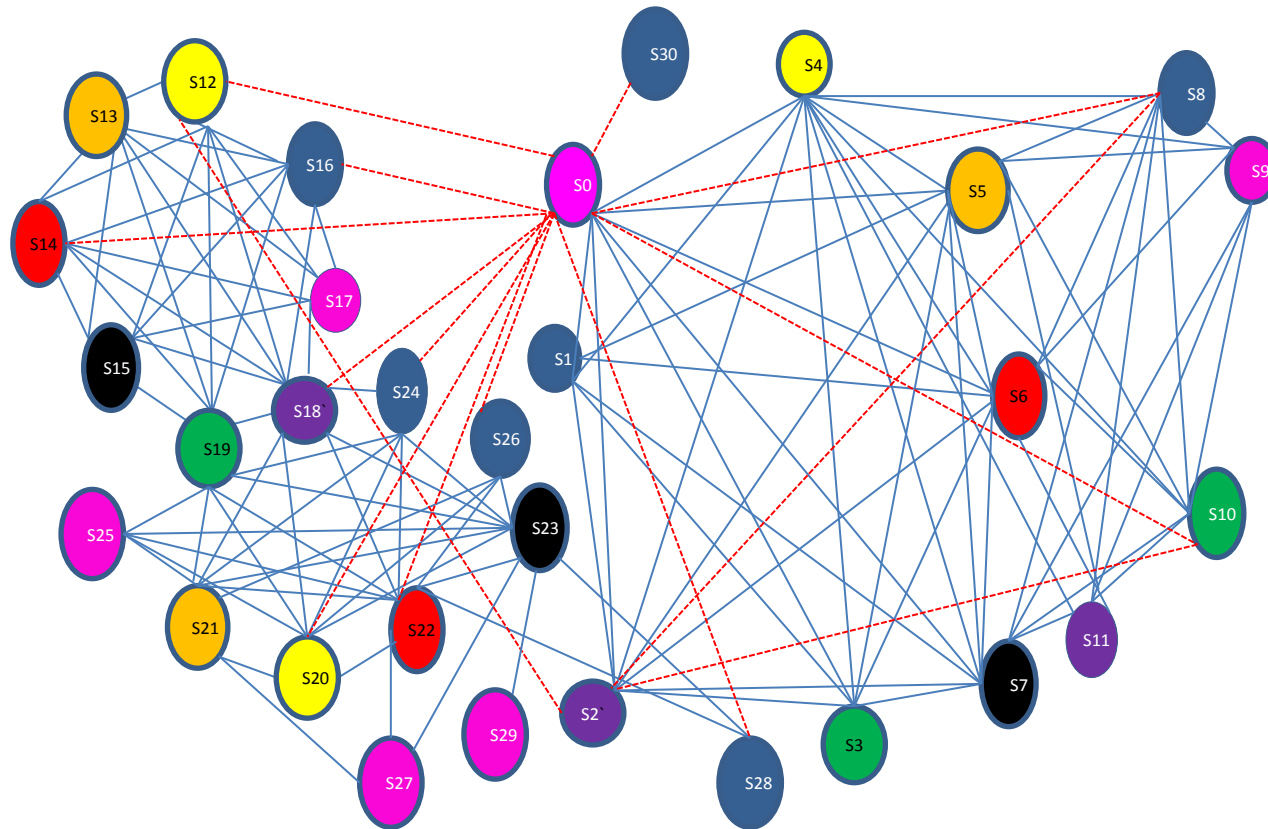


For remaining hash-blocks, 1024-bit input is constructed using following proposed rule:
1024 bit = (512-bit output of previous hash-block) & "1000" & (380-bit output of bits-padding block) & (128-bit representation of the length '512 bits' of previous hash)

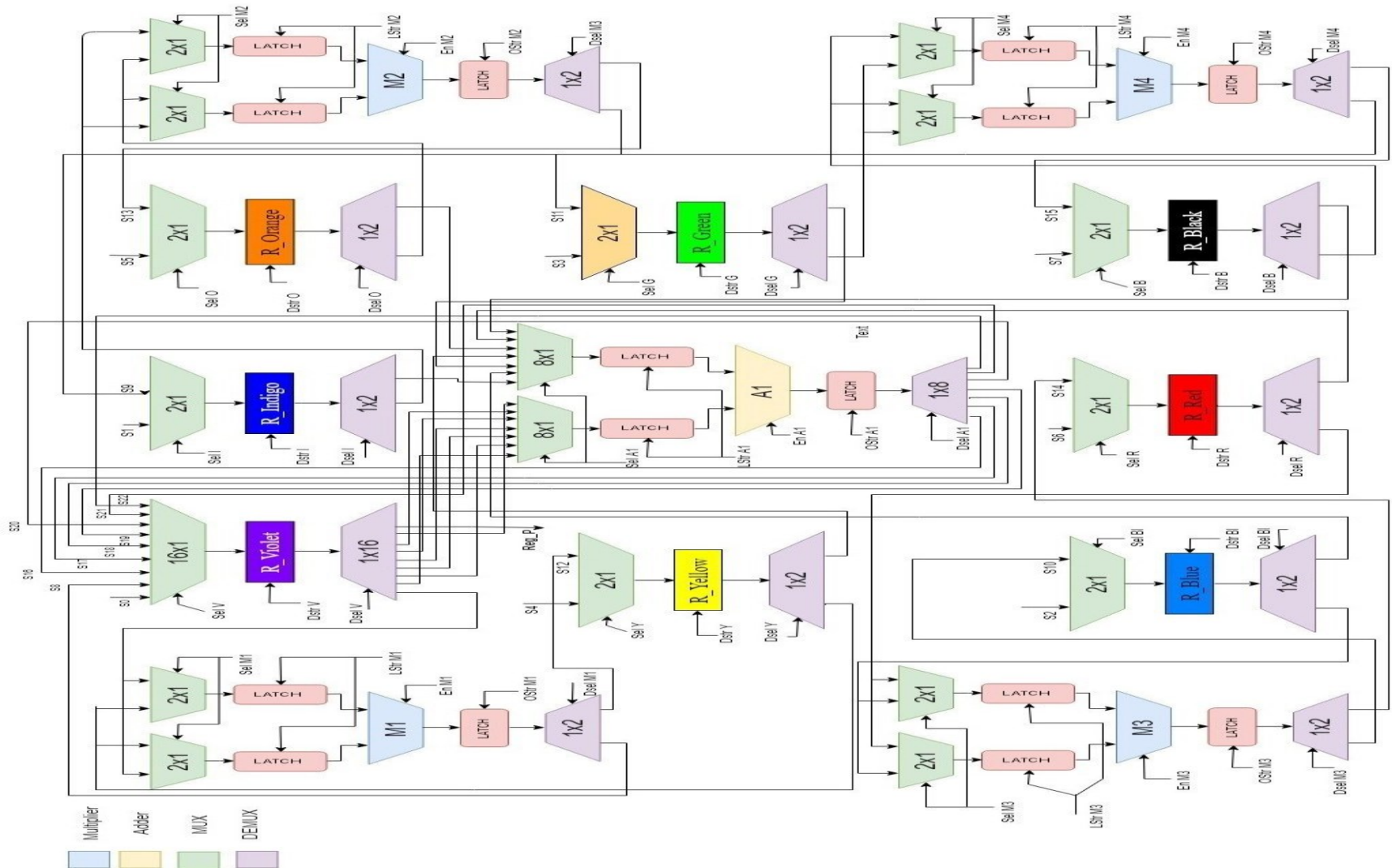
Detection process of steganography



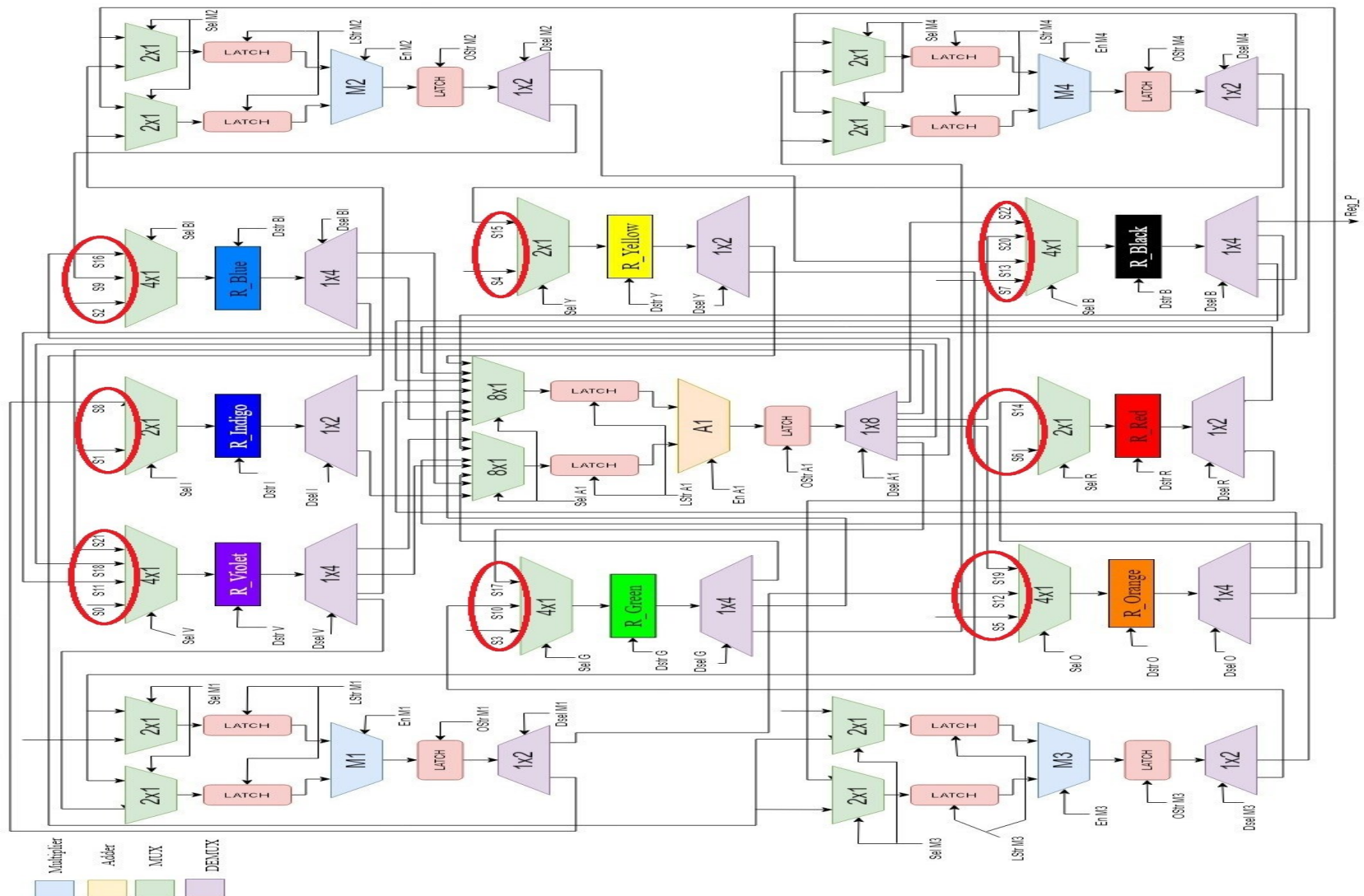
CIG of FIR filter hardware accelerator (IP core) after steganography/Watermarking



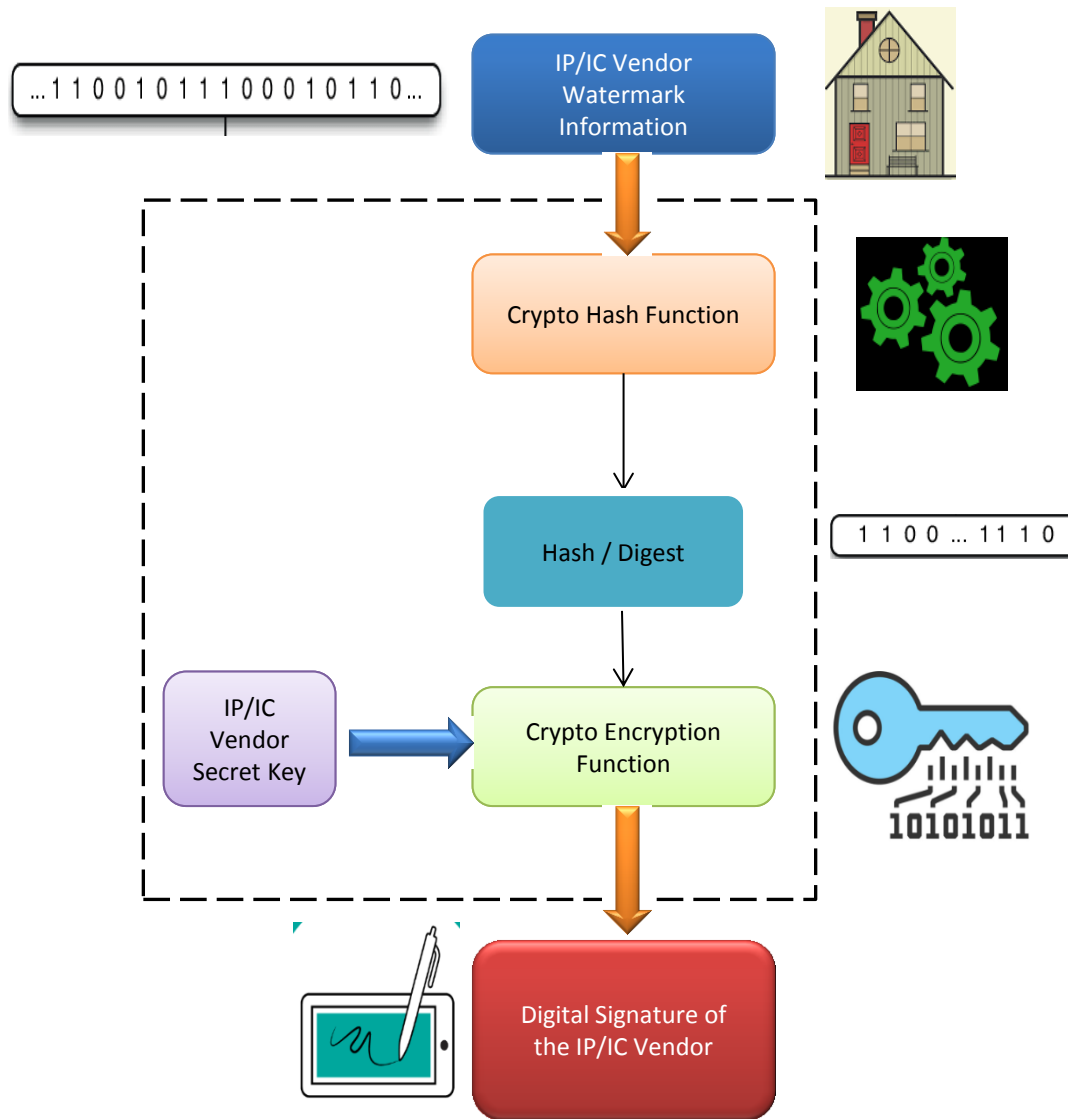
RTL datapath of 8-point DCT before steganography



RTL datapath of 8-point DCT after Steganography



High-level process of creating digital signature for IP cores



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

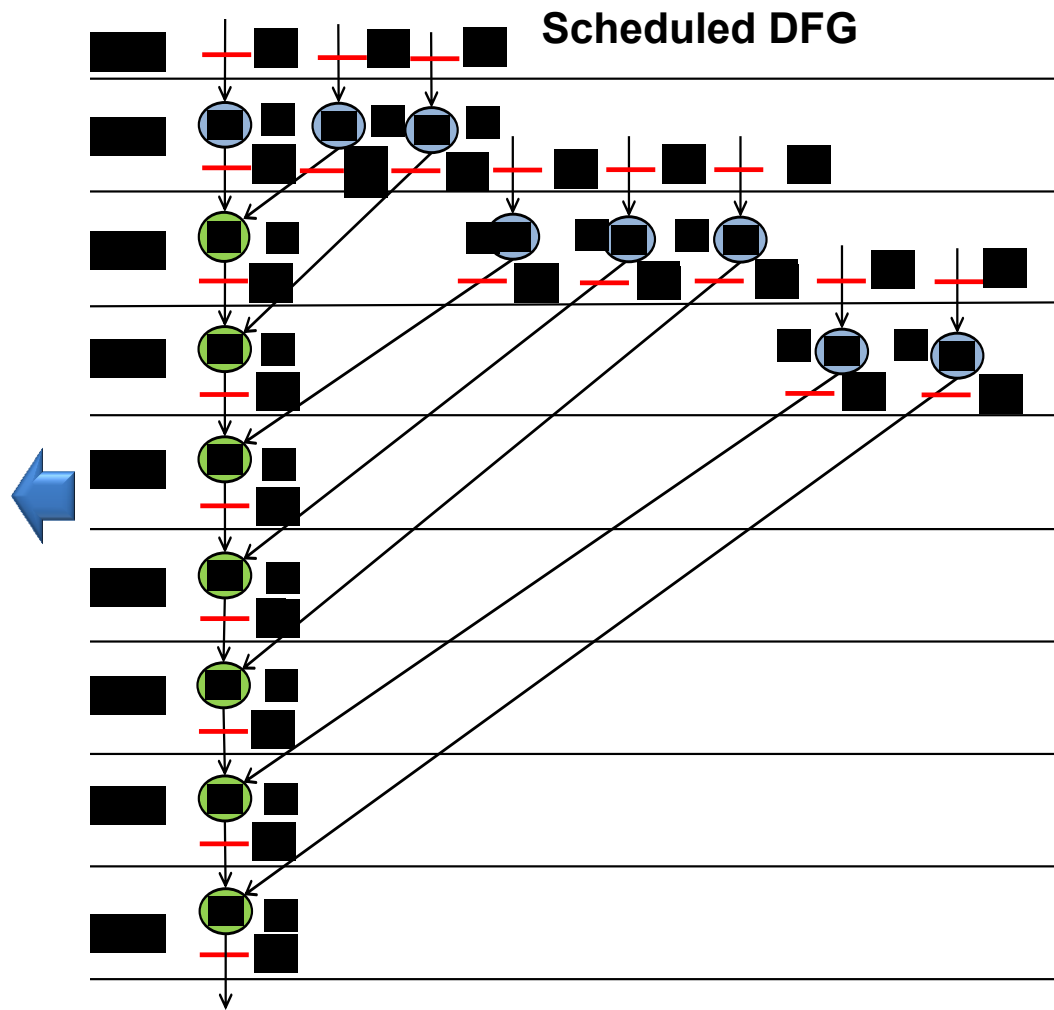
RSA Decimal Input	Encrypted Decimal Output	Encrypted Binary Equivalent
328629211327023509667307560 016780722176	259269232367594955022606516 388222677830	110000110000110.....011001 101000110
338967726051337675217876235 804913696768	103304422214721939828321919 365106451481	100110110110111.....100010 000011001
745080717249504132969595196 03599240546	246822478630224319655120426 30223003075	100101001000110.....111110 111000011
140476292891867587341382251 85020455483	289411796889479622387067677 582110256178	110110011011101.....110110 000110010

Post-processing Block

- 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.

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



Experimental Results

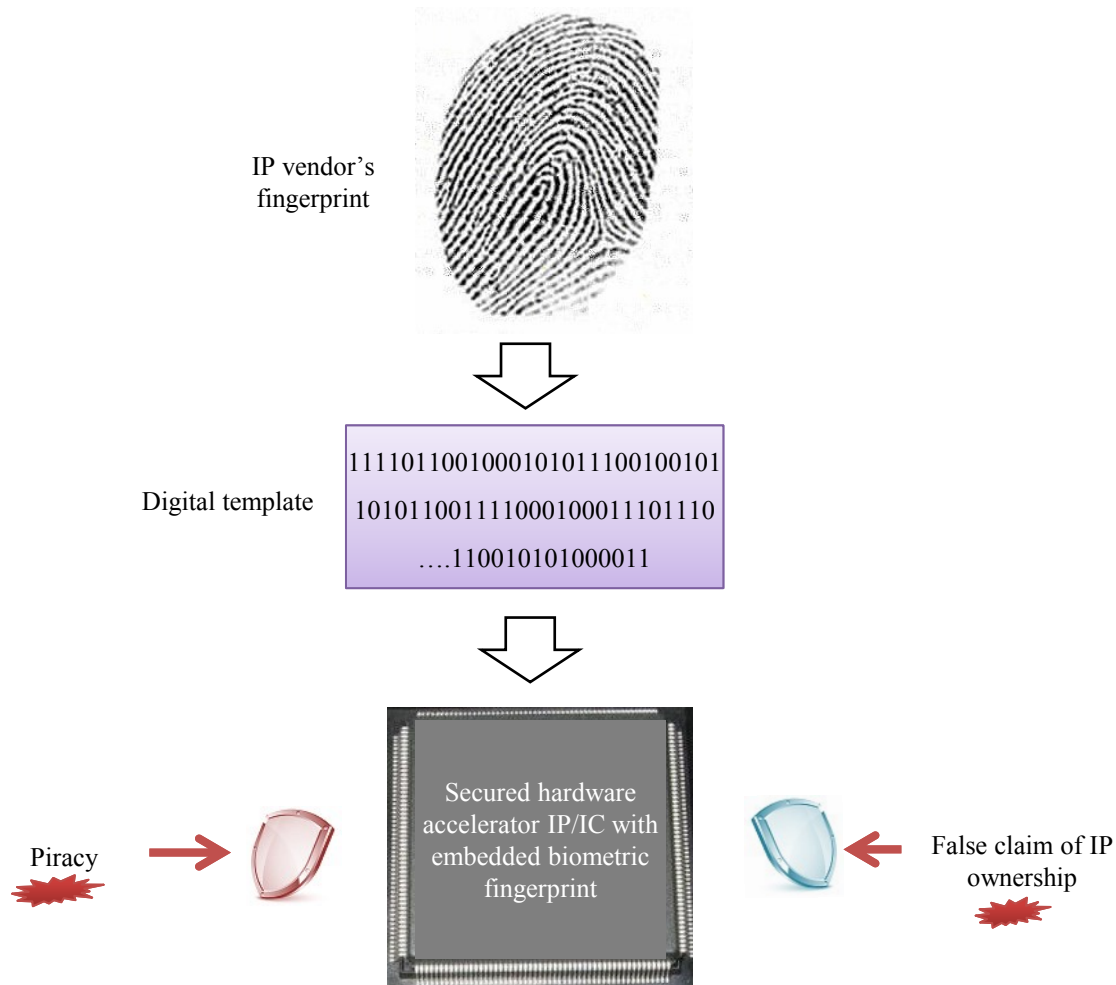
➤ Evaluation of Robustness Using Probability of Coincidence (P_c)

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

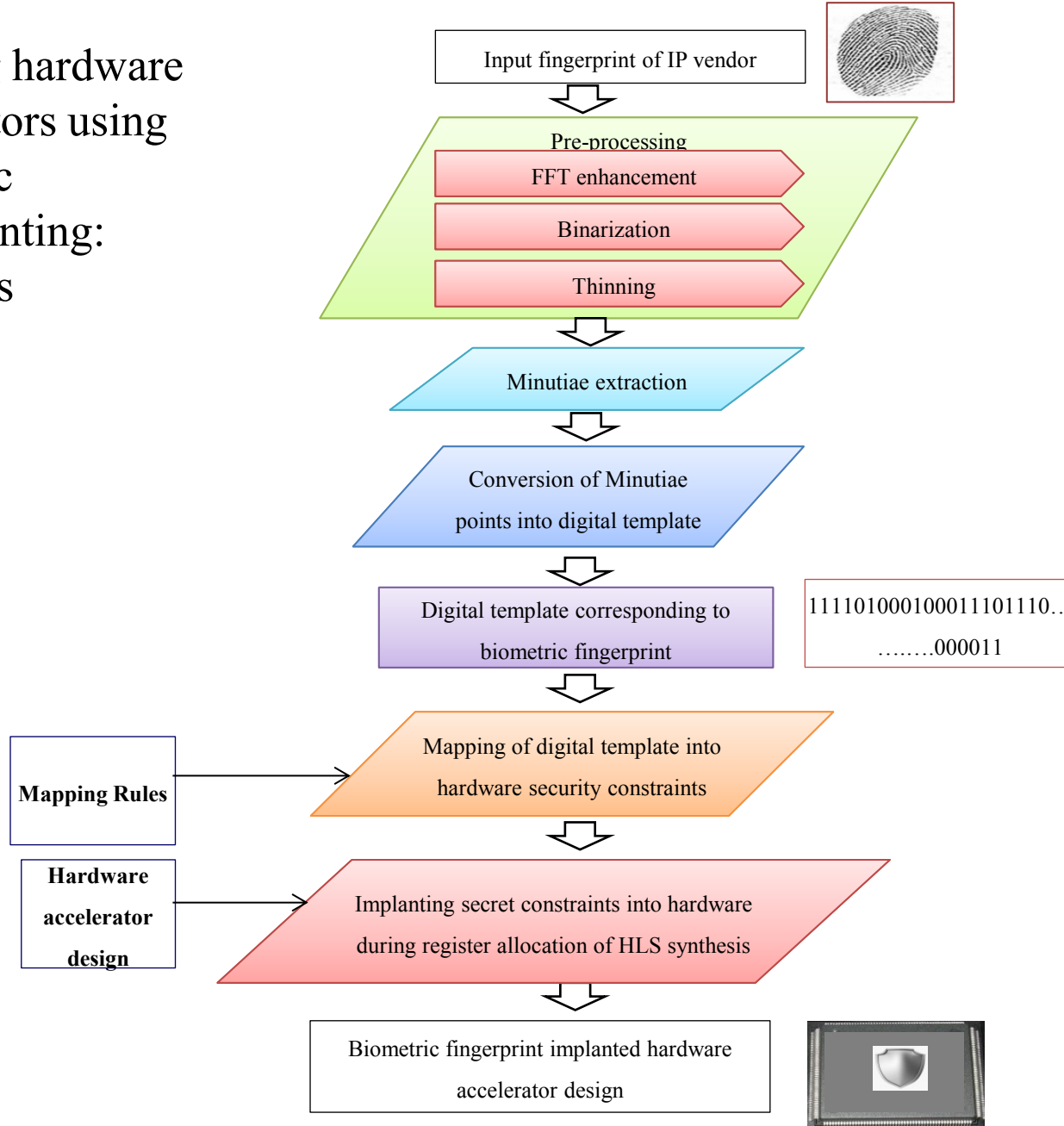
‘c’ denotes the number of colours used in the CIG and
‘S’ denotes the digital signature size

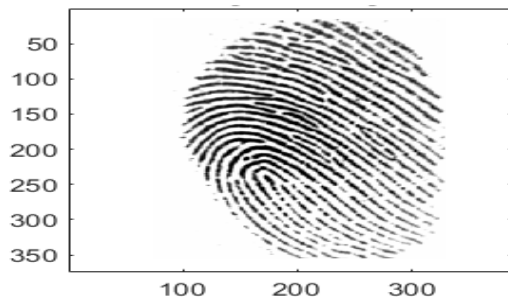
Benchmarks	c	Size of Digital signature (S)				
		S = 15	S = 30	S = 60	S = 120	S = 240
		P _c	P _c	P _c	P _c	P _c
BPF	6	0.0649	4.2127x10 ⁻³	1.7747x10 ⁻⁵	3.1496x10 ⁻¹⁰	9.9198x10 ⁻²⁰
JPEG SAMPLE	10	0.2059	0.0424	1.7970x10 ⁻³	3.2292x10 ⁻⁶	1.0428x10 ⁻¹¹
JPEG IDCT	29	0.5907	0.3490	0.1218	0.0148	2.1999x10 ⁻⁴
MESA FEEDBACK POINTS	17	0.4028	0.1622	0.0263	6.9267x10 ⁻⁴	4.7979x10 ⁻⁷
ARF	8	0.1349	0.0182	3.3150x10 ⁻⁴	1.0989x10 ⁻⁷	1.2076x10 ⁻¹⁴
MESA MATRIX MULTIPLICATION	23	0.5134	0.2635	0.0695	4.8237x10 ⁻³	2.3268x10 ⁻⁵

Securing hardware accelerators using biometric fingerprinting: Forensics

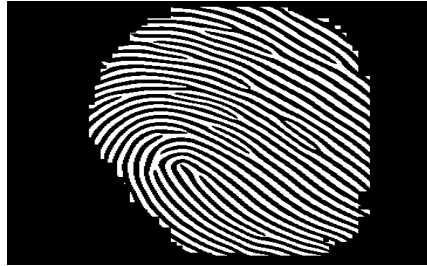


Securing hardware accelerators using biometric fingerprinting: Forensics





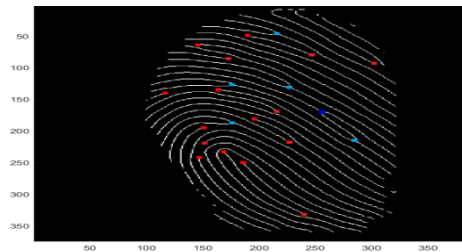
(a) Input fingerprint image (101_1)



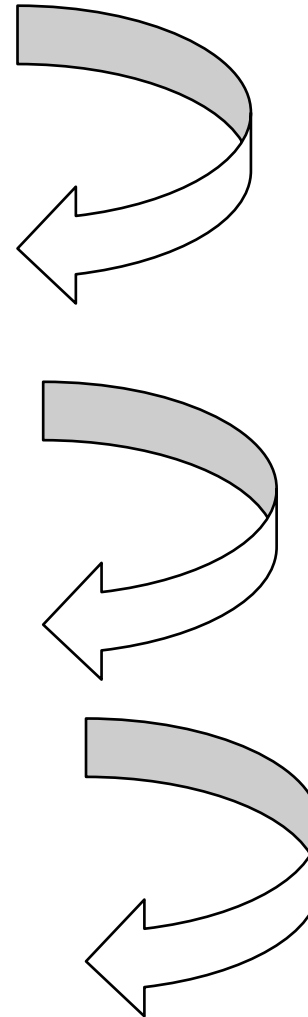
(b) Binary image



(c) Thinned image



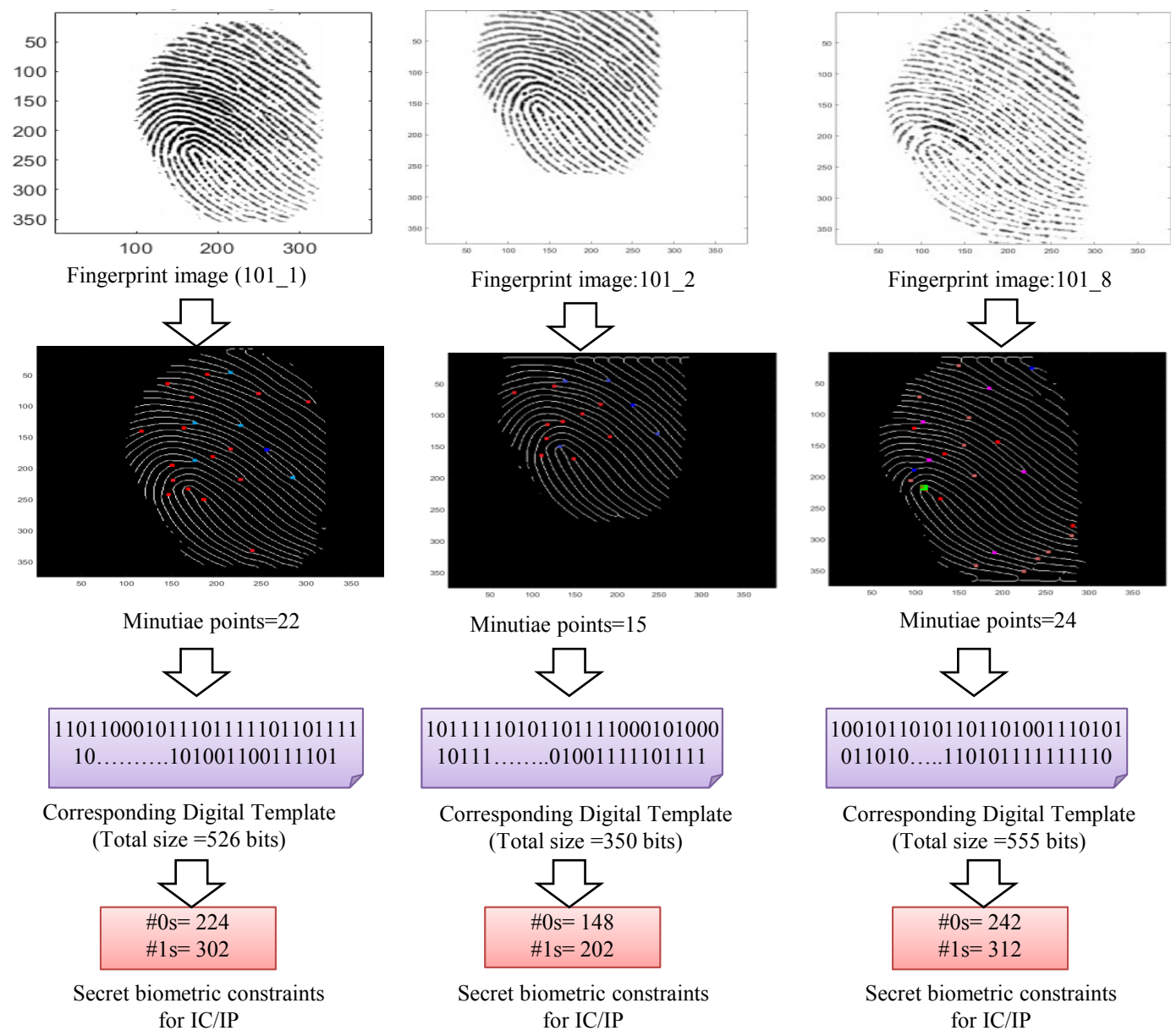
(d) Minutiae points



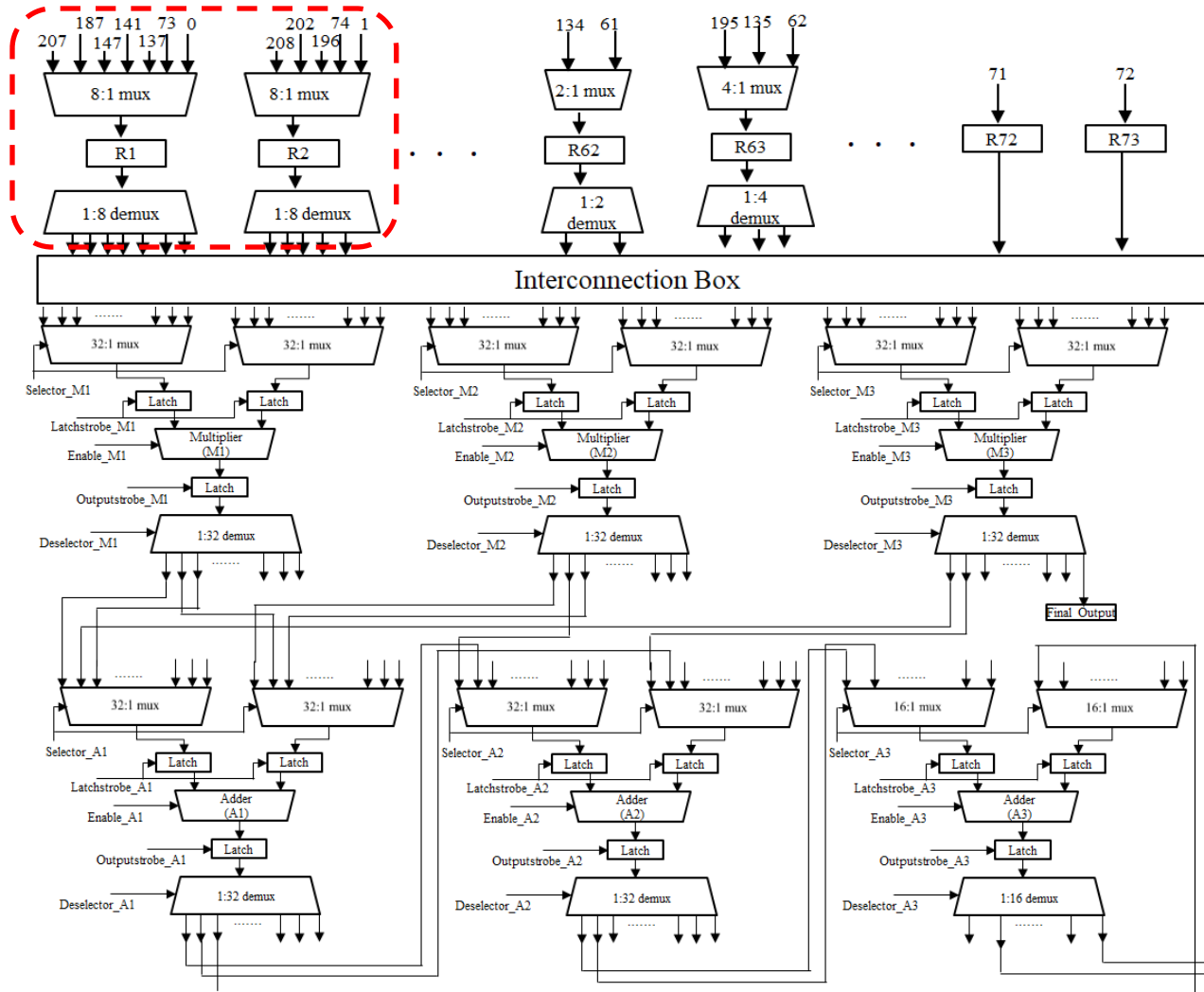
Securing hardware
accelerators using
biometric
fingerprinting:
Forensics: An
example

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



Secured datapath of JPEG compression hardware accelerator implanted with biometric fingerprint



Detecting Biometric Fingerprint in a hardware accelerator

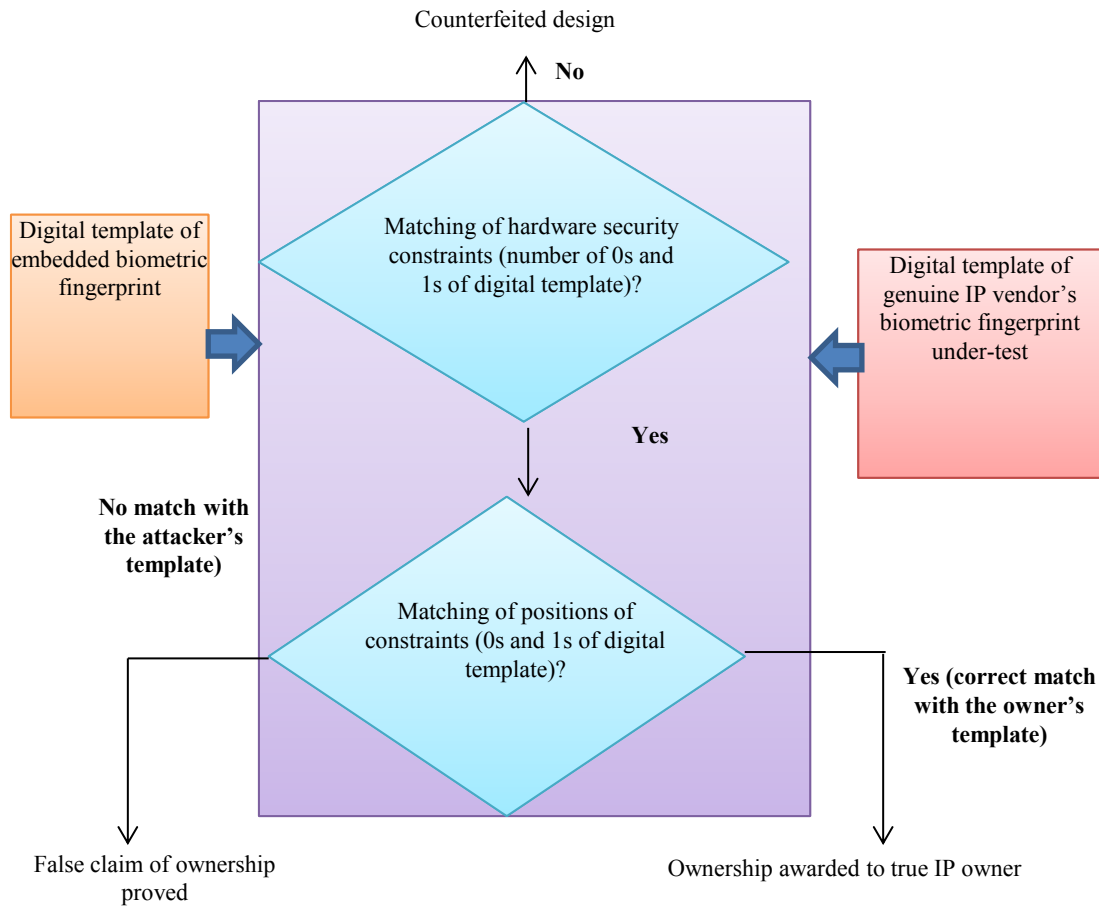
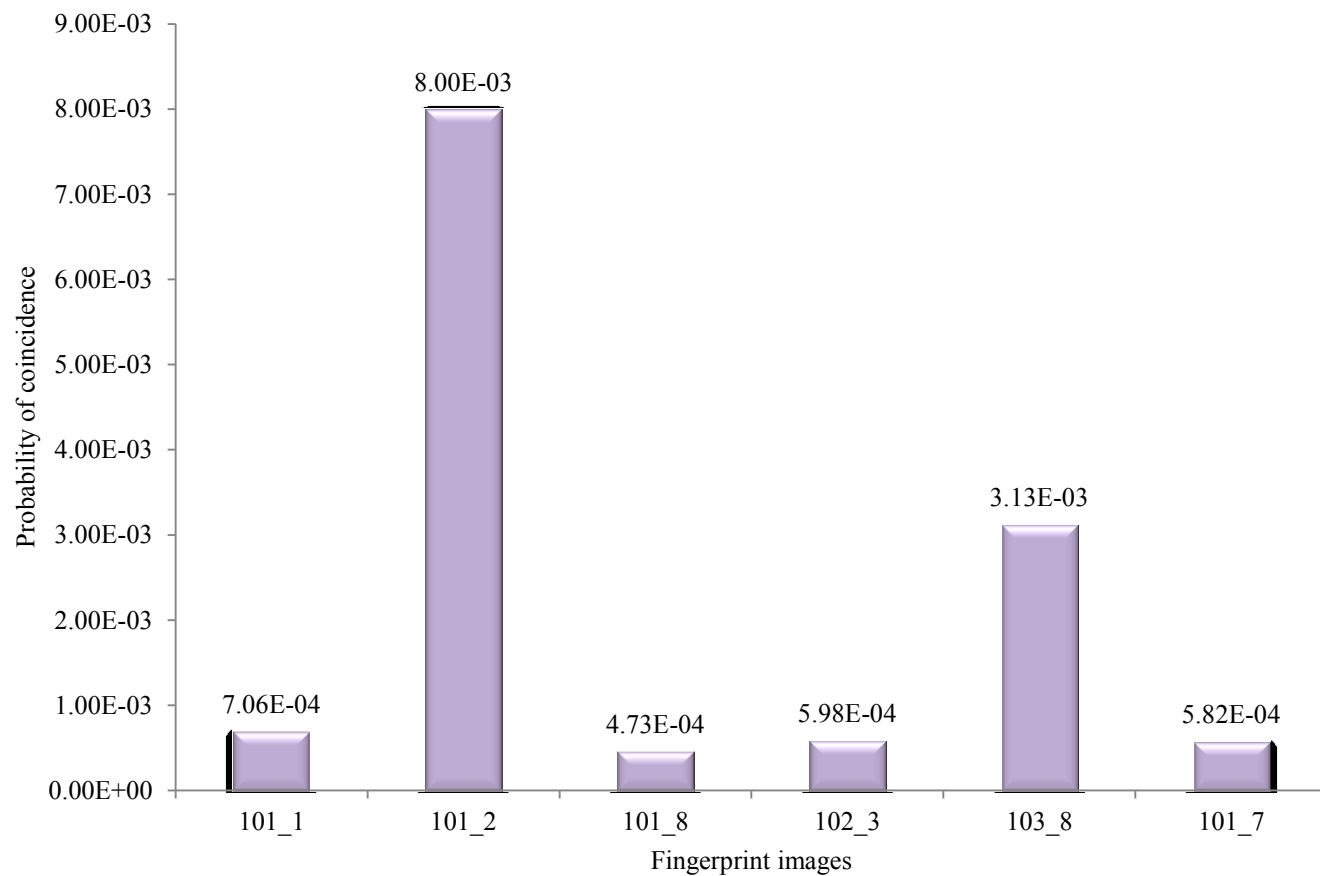


Fig. 9. Proving true IP ownership using proposed detection approach

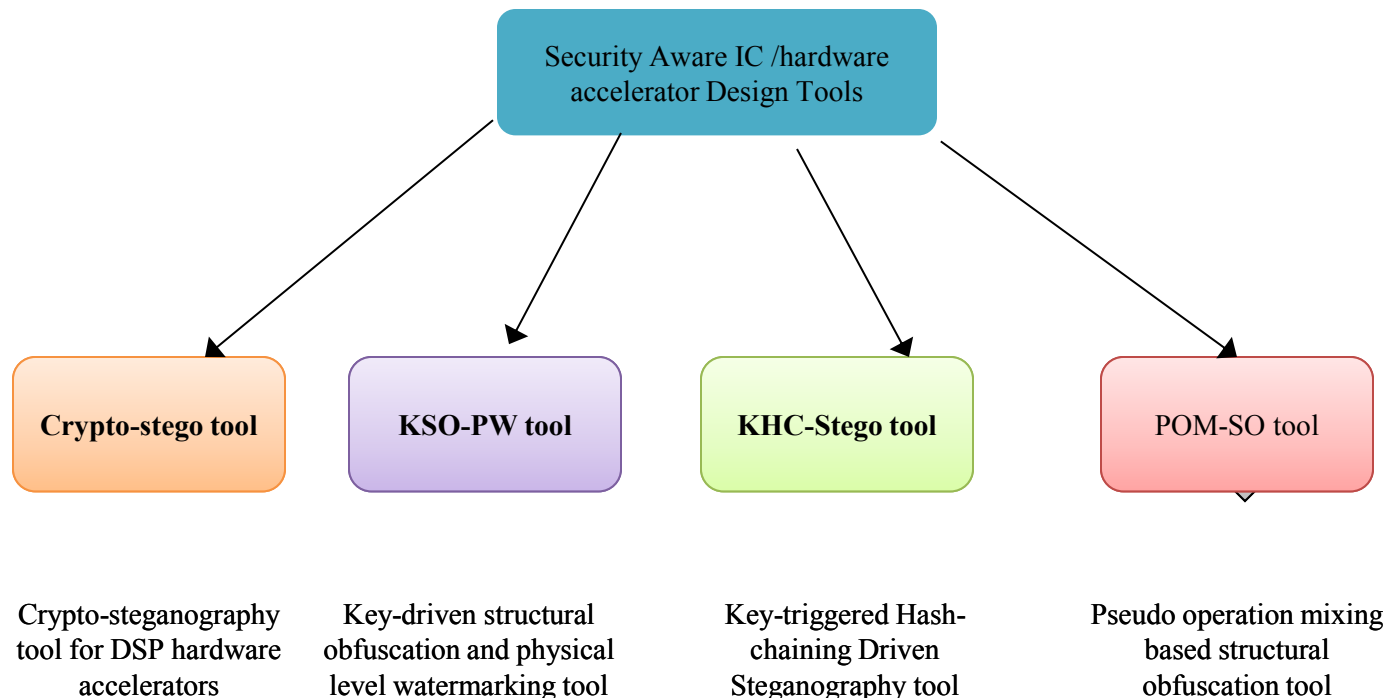
Variation in probability of coincidence for different fingerprint images



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



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/> 🗲 🌐 📄 📁

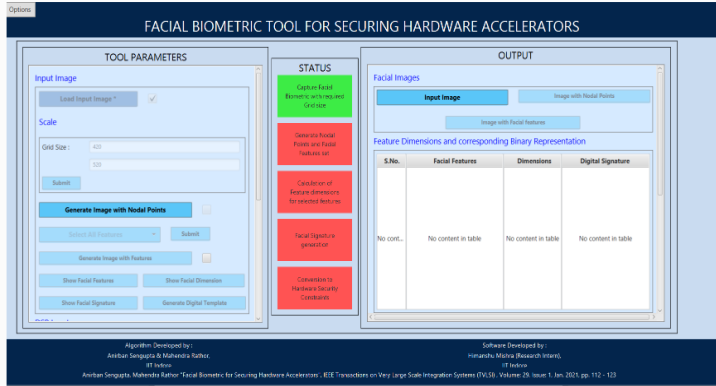
CAD FOR ASSURANCE 🔍 CAD Tools • Trust Issues • Benchmarks • SoC Platform • Utilities • Trust Curriculum • Publications • Contributors • Webinar and Events • Contest • Upload Your Tool • Contact Us

🏠 > 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



TOOL PARAMETERS

Input Image: ☐ Load Input Image * ☒

Scale: Grid Size:

STATUS

Custom Face ☒

OUTPUT

Facial Images:

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
Anirban Sengupta, Mahendra Rathor "Facial Biometric for Securing Hardware Accelerators", IEEE Transactions on Very Large Scale Integration Systems (TVLSI), Volume 28, Issue 1, Jan. 2021, pp.112 – 123

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

🔍 Foxit Reader Update

Summary

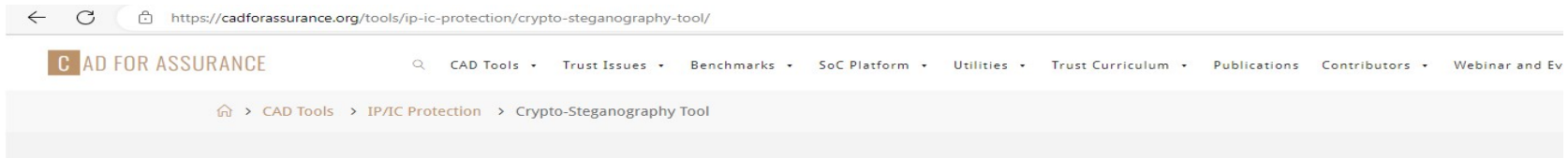
The Faciometric hardware security tool has been developed to simulate and analyze the functionality of facial biometric based approach for securing DSP hardware accelerators against piracy and false claim of ownership threats.

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/>



Crypto-Steganography Tool

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

Stage: RTL



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.

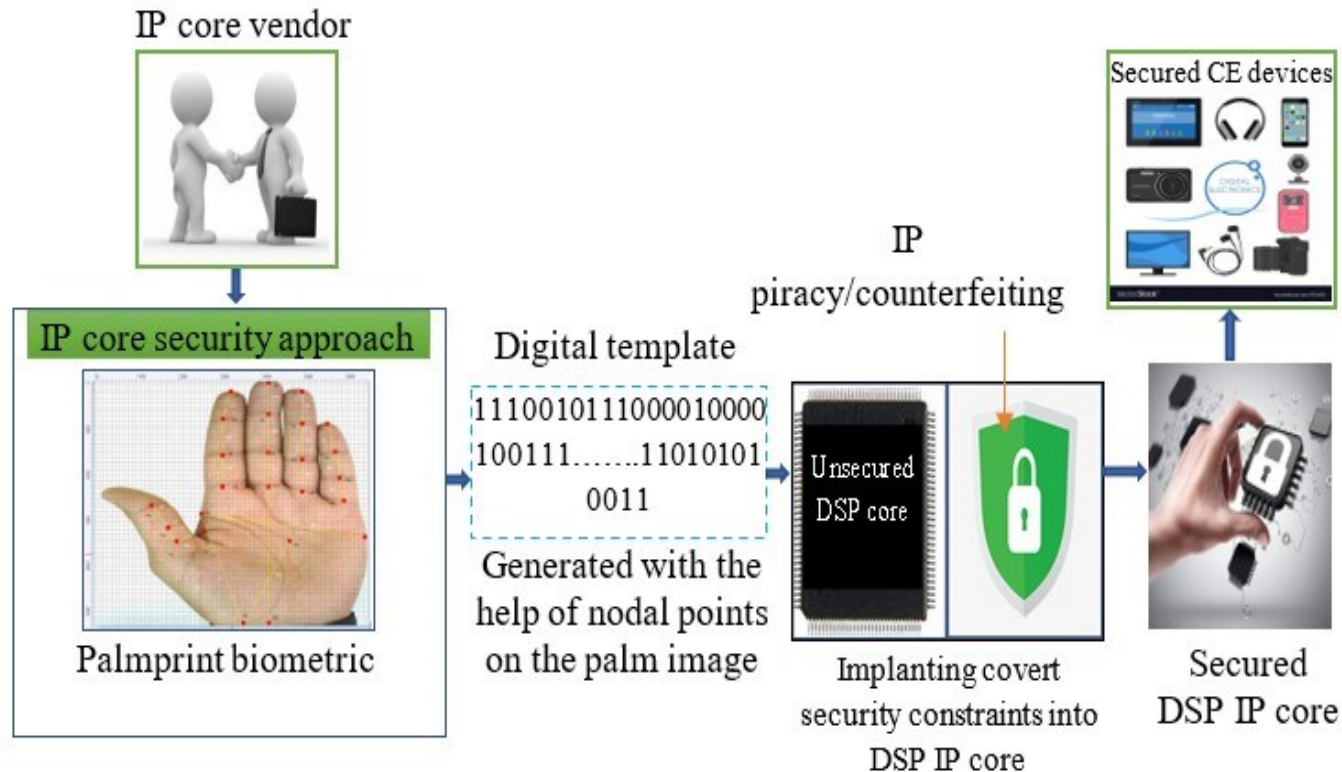
[Abstract](#) | [Links](#) | [BibTeX](#)

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.

Palmpoint based Hardware Security for IPP

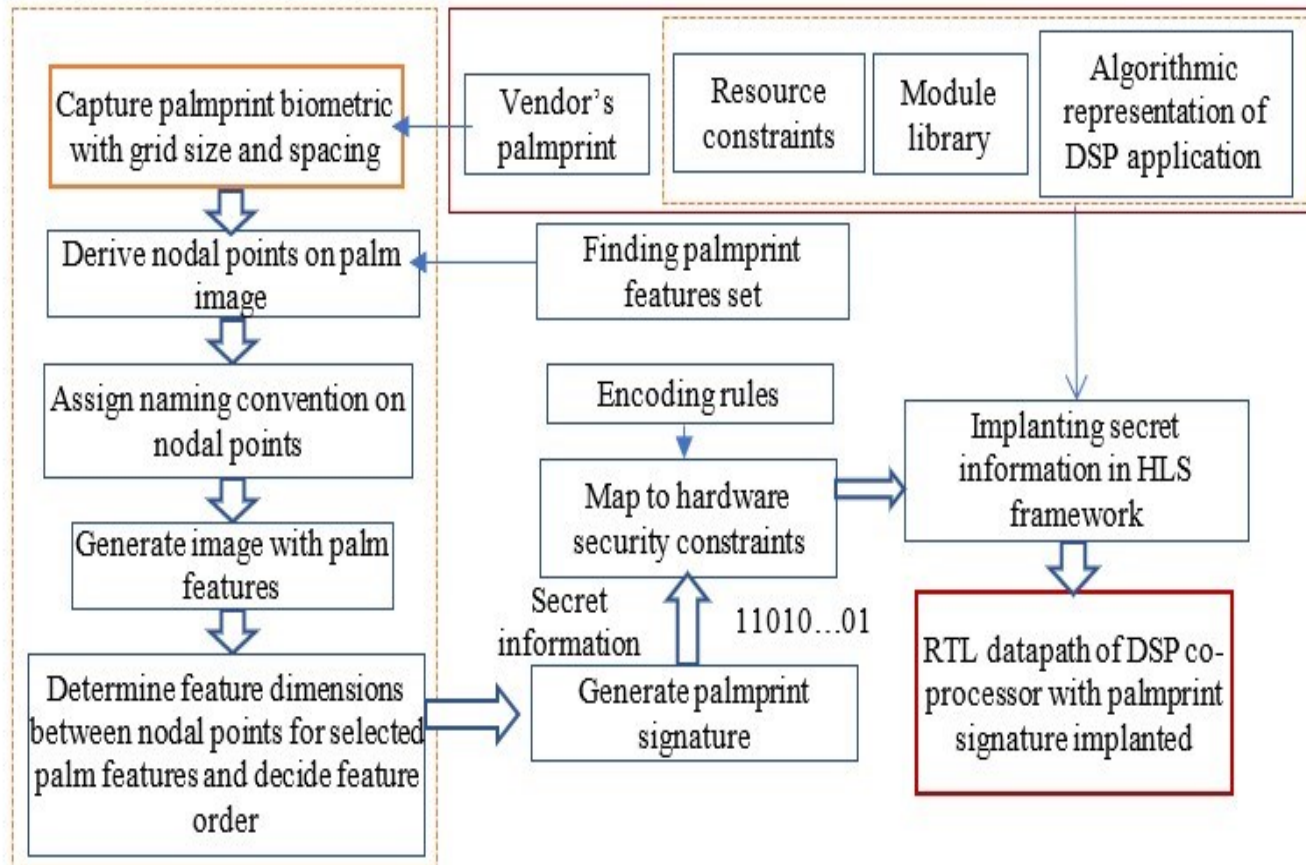


Securing reusable DSP IP core used in CE systems

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



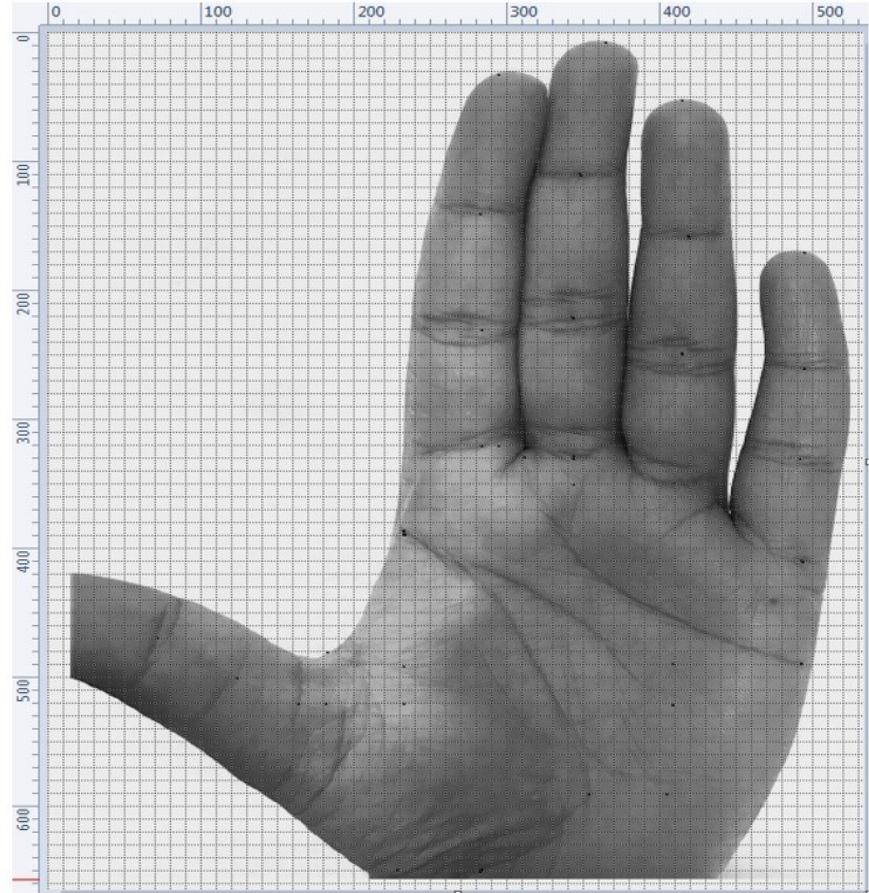
Anirban Sengupta, Rahul Chaurasia, Tarun Reddy "Contact-less Palmprint Biometric for Securing DSP Coprocessors used in CE systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 67, Issue: 3, August 2021, pp. 202-213

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 34

Palmprint based Hardware Security for IPP

➤ Capturing palm image

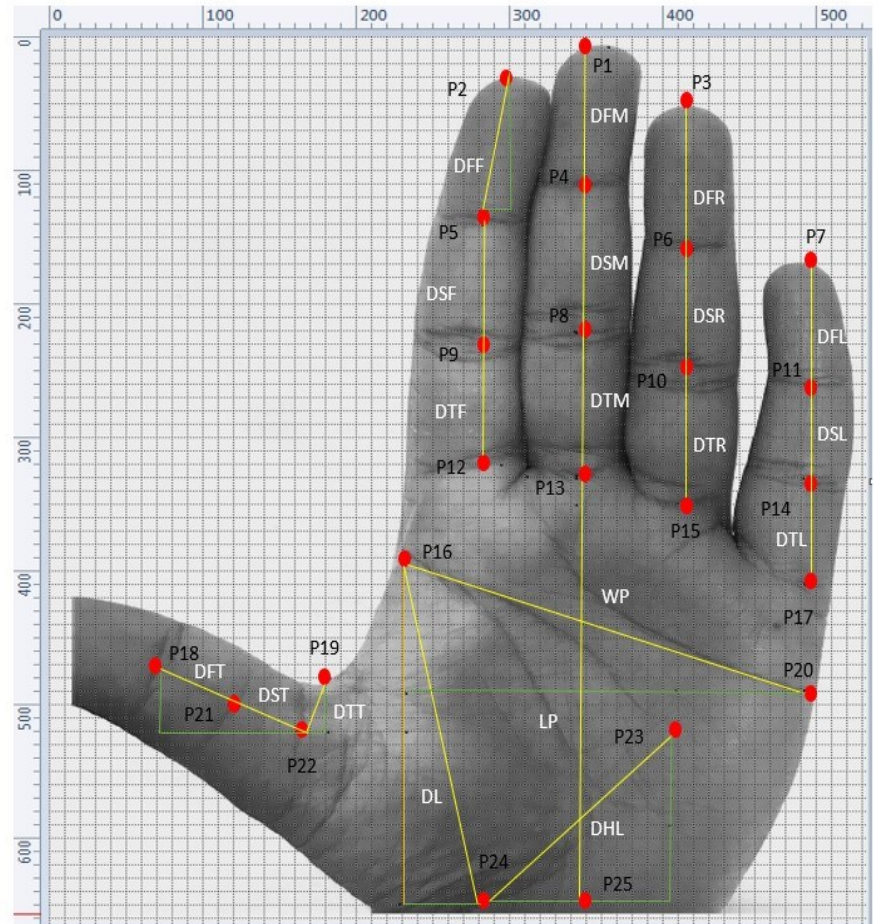
- At first the palmprint biometric of the authentic vendor or designer is captured and subsequently image of the captured palmprint is subjected to a specific grid size/spacing.
- This helps in generating the nodal points precisely.



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.



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)

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 $\neq$ DHL --- $\neq$ DTT”. Where, ‘ $\neq$ ’ 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	100011011.0011110101110000101
F4	LP	325	101000101
F5	DFD	101.11	1100101.00011100001010001111
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	110111.1110011001100110011
F18	DST	51.45	110011.01110011001100110011
F19	DTT	42.72	101010.10111000010100011111

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:

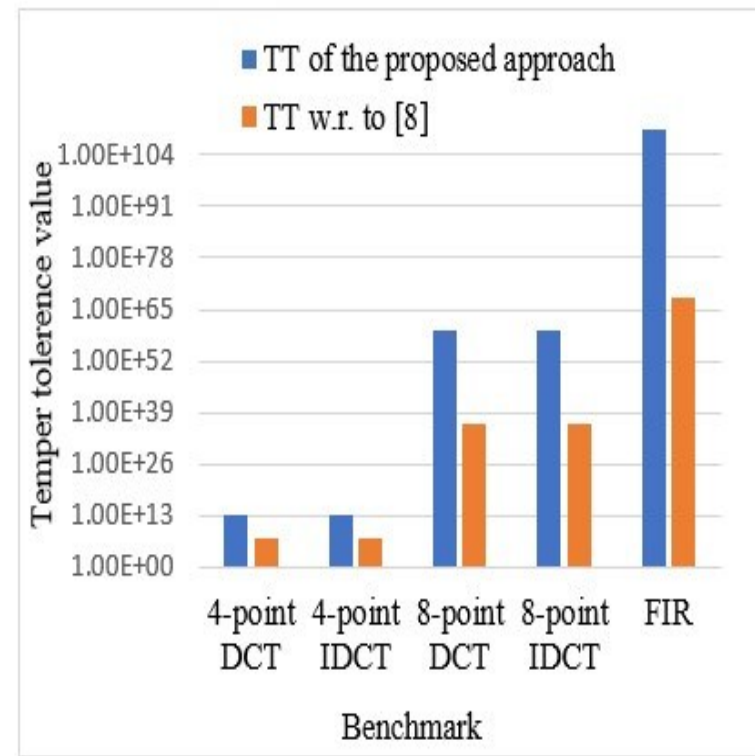
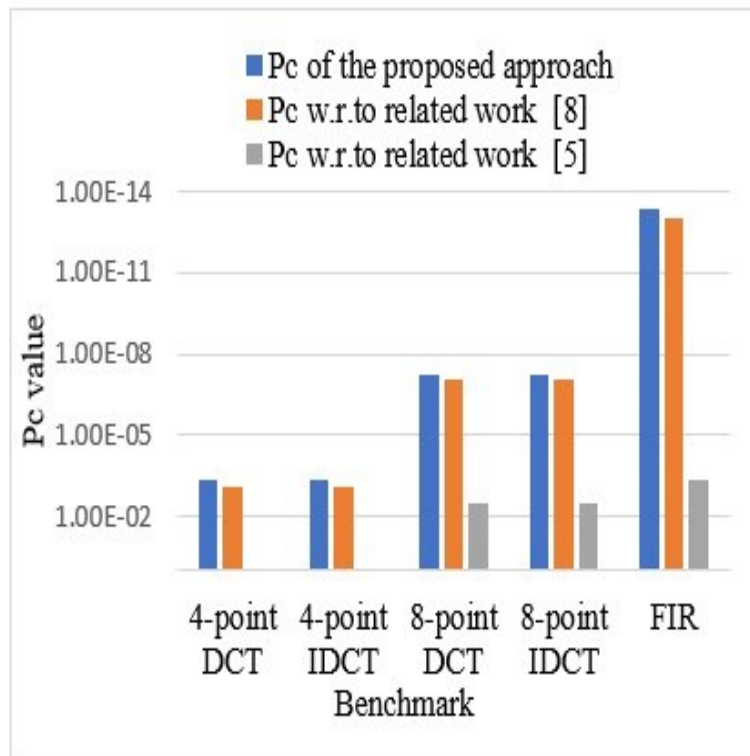
- The security of the proposed approach is analyzed in terms of probability of coincidence (Pc) and temper tolerance (TT) ability.
- The Pc metric is formulated as follows:

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

- The TT metric is formulated as follows:

$$TT = P^Q \quad (2)$$

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:

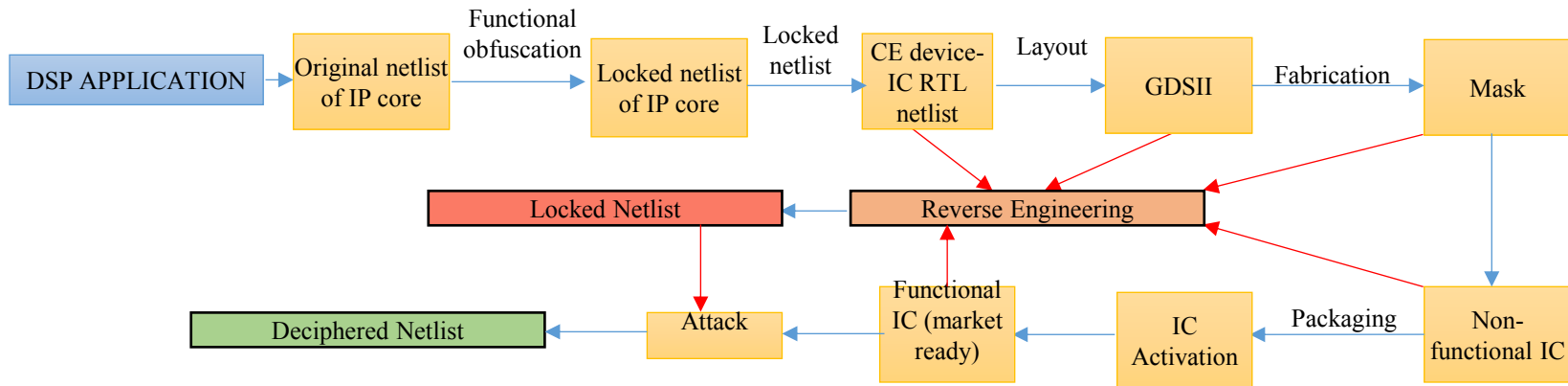
$$Z = h1 \frac{\nabla t}{\nabla_{\max}} + h2 \frac{\Delta t}{\Delta_{\max}} \quad (3)$$

- 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

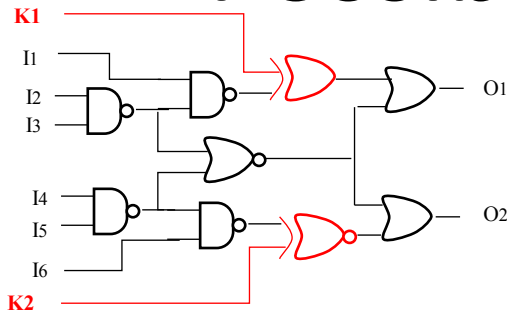
Benchmarks	Design cost of baseline	Design cost of palmprint implanted design	% Cost overhead
4-pointDCT	0.5611	0.5623	0.2%
4-point IDCT	0.5611	0.5623	0.2%
8-pointDCT	.4721	.4740	0.4%
8-point IDCT	.4721	.4740	0.4%
FIR	.4443	.4479	0.8%

How Hardware of a CE device can be compromised ?

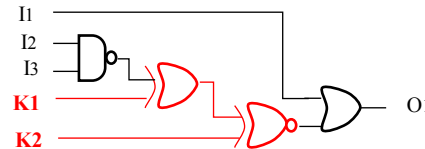


- Reverse engineering (RE) of a DSP core is a process of gaining the complete understanding of its **functionality, design** and **structure**.
- However, RE can be used for dishonest intention such as **overbuilding, piracy**, or **counterfeiting** a DSP core or inserting a **hardware Trojan**.

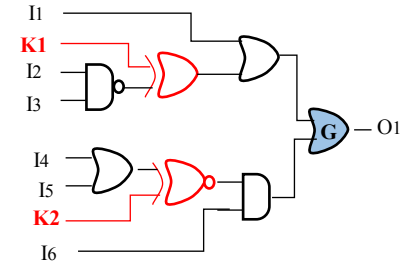
Possible Threat Scenarios



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.

The Vulnerability of Functional Obfuscation towards Different Attacks

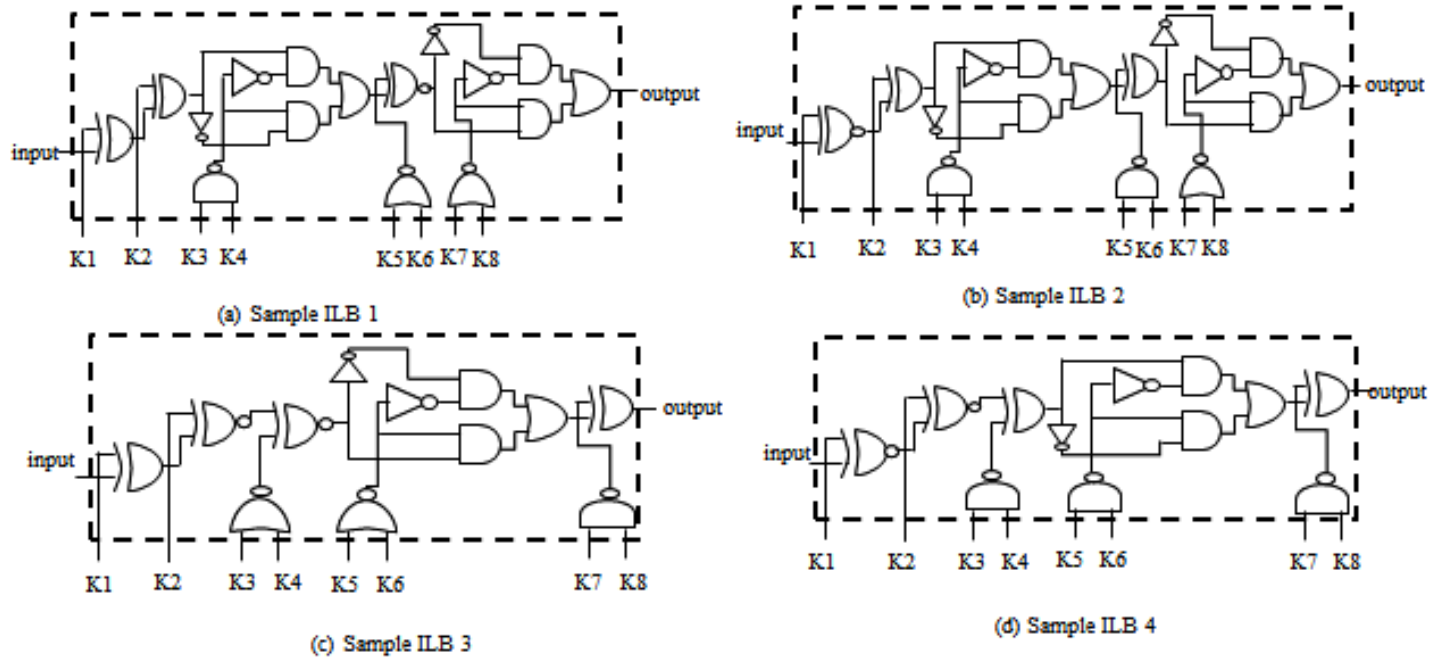
❑ **Key sensitization attack:**

- 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 :**

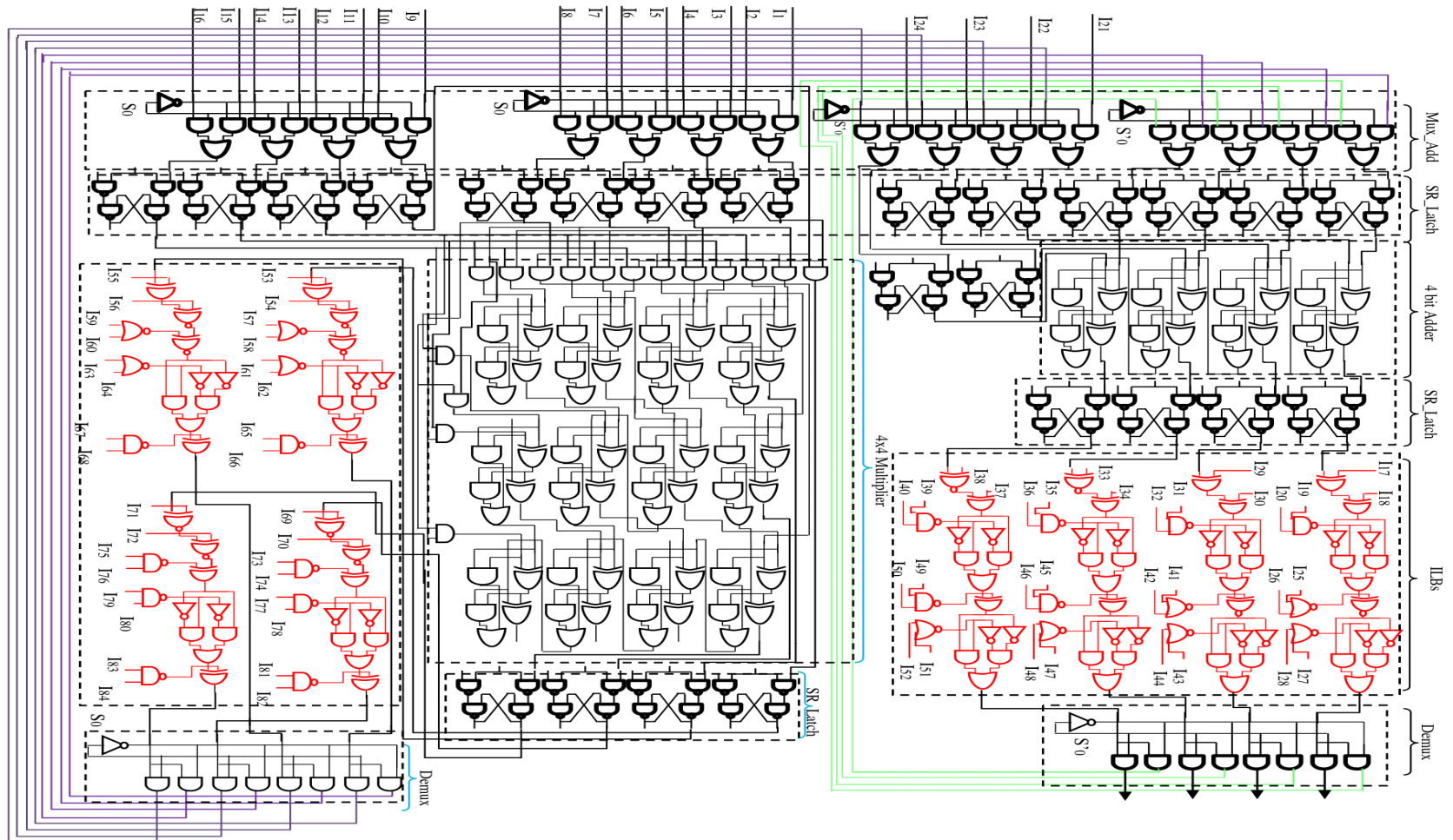
- The attacker can sensitize a key-bit at primary output by controlling the primary inputs of the design. To do so, the attacker needs to identify the input pattern that can sensitize the correct key-bits to the primary output.
- The Attacker tries to find isolated key-gates in the obfuscated netlist. 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)



- 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



References

- Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9
- Anirban Sengupta, Mahendra Rathor "Protecting DSP Kernels using Robust Hologram based Obfuscation", IEEE Transactions on Consumer Electronics, Volume: 65, Issue: 1, Feb 2019, pp. 99-108
- Anirban Sengupta, Saraju P. Mohanty "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", The Institute of Engineering and Technology (IET), 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0
- Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 37, Issue: 4, April 2018, pp. 742 – 755
- Anirban Sengupta, Mahendra Rathor, "IP Core Steganography using Switch based Key-driven Hash-chaining and Encoding for Securing DSP kernels used in CE Systems", IEEE Transactions on Consumer Electronics (TCE), 2020
- Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", IEEE Transactions on Consumer Electronics (TCE) , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 – 515
- <https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool>
- Anirban Sengupta, Rahul Chaurasia, Tarun Reddy "Contact-less Palmprint Biometric for Securing DSP Coprocessors used in CE systems", IEEE Transactions on Consumer Electronics (TCE) , Volume: 67, Issue: 3, August 2021, pp. 202-213
- Rahul Chaurasia, Aditya Anshul, Anirban Sengupta "Palmprint Biometric vs Encrypted Hash based Digital Signature for Securing DSP Cores Used in CE systems", IEEE Consumer Electronics (CEM) , Volume: 11, Issue: 5, September 2022, pp. 73-80
- Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 38, Issue 4, April 2019, pp. 604 - 616
- Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", IEEE Transactions on Very Large Scale Integration Systems , Vol 28, Issue: 9, 2020, pp. 1979-1992
- Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", IEEE Transactions on Consumer Electronics (TCE), Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

Conclusion

The future is:

HLS based hardware IP design with Energy-Security Tradeoff..

Thank you