Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting

Dr Anirban Sengupta

Professor, CSE,

IIT Indore, India

Outline

- ❑ Introduction
- ❑ Criteria for Optimal Fingerprint
- ❑ Comparison of Fingerprinting and Watermarking
- ❑ Overview of Crypto-based Multivariable Fingerprinting
- ❑ Fingerprint Methodology- Preprocessing Phase and Demonstration
- ❑ Fingerprint Methodology- Selection of Fingerprint and Embedding and Demonstration
- ❑ Analysis on Case Studies

Introduction

- The reusable IP cores not only increase the productivity of complex designs but also lead to the design cost reduction.
- However, the unremitting applications of reusable IP cores in SOCs raise the need of their protection against several hardware threats such as IP forgery, infringement and fraudulent claim of ownership.
- The protection is important from the perspective of both seller and buyer.
- For an IP owner/seller, deploying protection into IP cores is required in order to detect the piracy/counterfeiting/cloning and secure the ownership.
- This is required because the owner sends his IP core to a design house for the purpose of SoC integration or manufacturing. However, the design house may be deceitful, therefore the chances of forgery arises.

Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

Introduction

- From the buyer's perspective, protection is deployed in order to provide him/her exclusive buyer rights. This is required when an IP seller designs an IP core according to the buyer's specifications.
- Thereby, providing exclusive buyer/user rights thwarts the reselling of the IP core to other users.
- The common protection techniques such as copyrights, patents and trademarks etc. can also be used for intellectual properties. However, their limited applications render them unsuccessful to address the challenges.
- Therefore, a need of strong IP core protection measure from a buyer's perspective arises here.
- In order to ensure the exclusive buyer's rights over the IP cores, 'buyer fingerprint' is a promising alternative.

Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

Introduction

- A buyer's fingerprint is embedded onto the top of the existing design without affecting the functionality.
- The secret fingerprinting constraints are obtained through a signature chosen by the buyer and certain encoding scheme.
- These constraints are implanted covertly in addition to the usual design constraints.
- Thus generated reusable IP core belongs to a specific buyer.
- The fingerprint is able to thwarts the reselling or redistribution of illegal copies.
- In order to make IP rights protection schemes more secure, a cryptographic hashing algorithm can be integrated with the fingerprint scheme. The hashing is typically used to generate a secure hash digest.

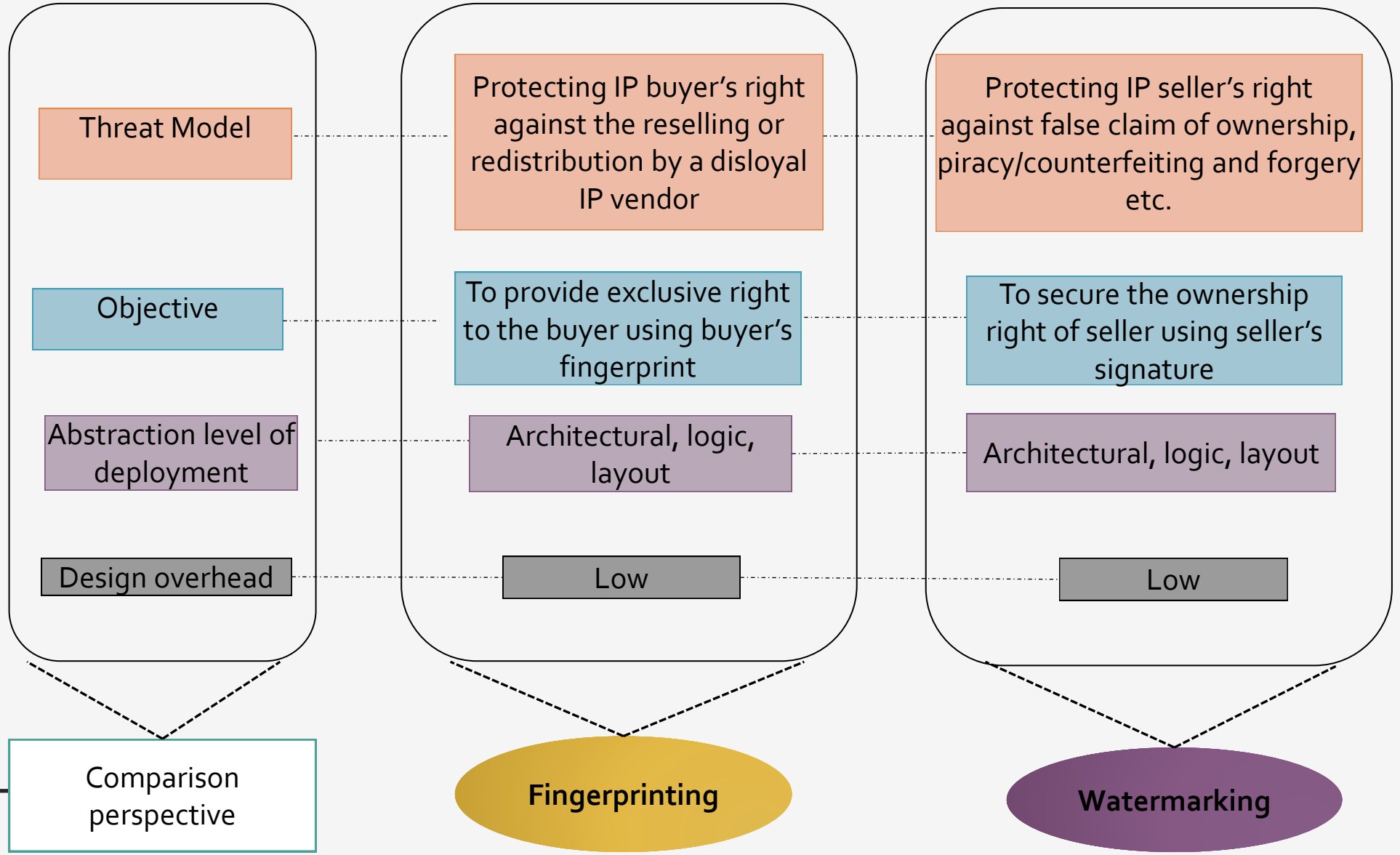
Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", IET Book "Frontiers in Securing Hardware IP Cores: Forensic detective control and obfuscation techniques", 2020, ISBN: 978-1-83953-031-9/978-1-83953-032-6

Criteria for an optimal fingerprint

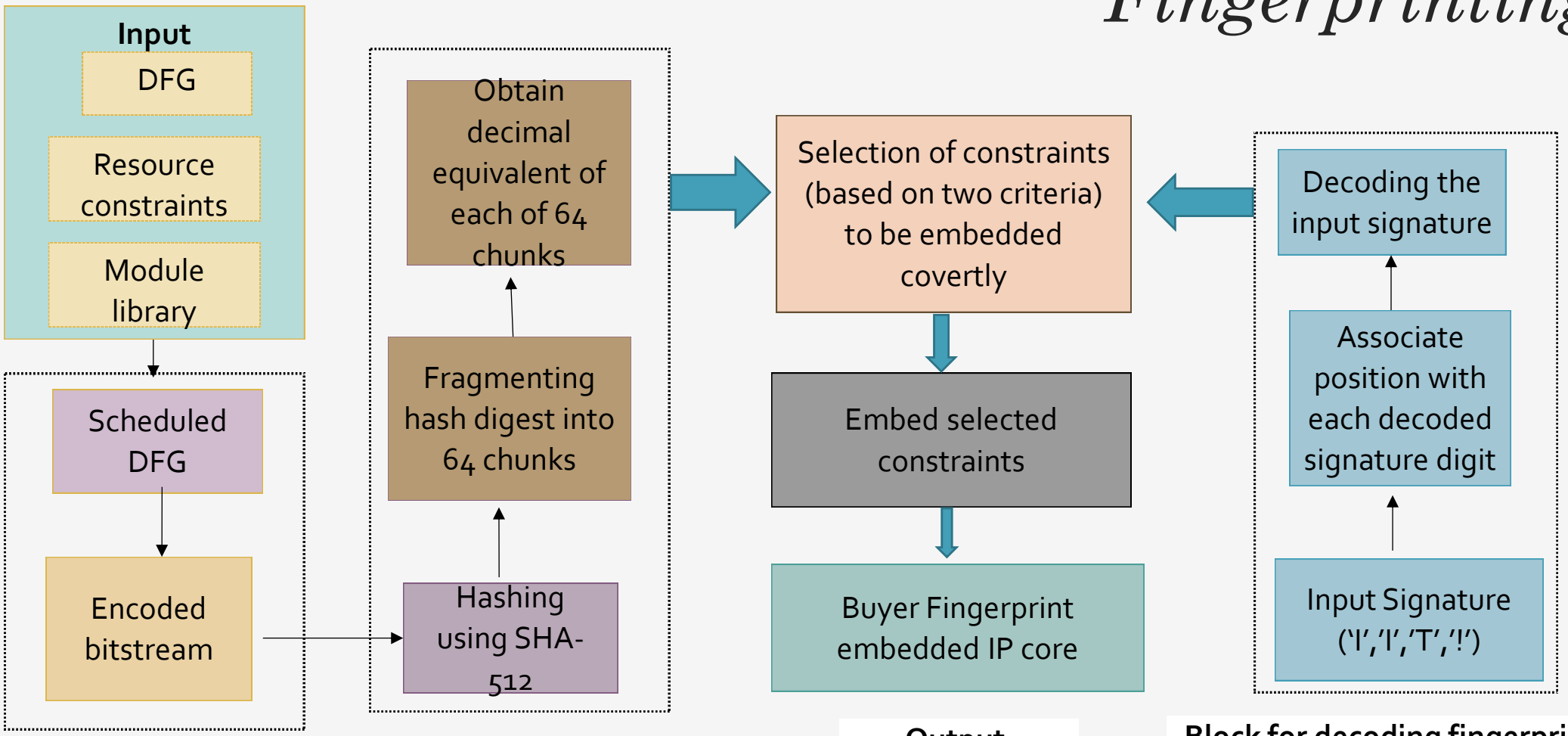
- An optimal fingerprint should result into highly secure and low-cost solution that not only satisfies the user's constraints but additional security constraints also.
- Fingerprint must be permanently embedded onto the IP core design.
- It must be unique for each buyer and harder to trace.
- It should not interfere with the vendor IP rights protection mechanism.
- It should incur minimal overhead post embedding.
- It should not affect the functionality of the IP core.

Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

Comparison of Fingerprinting with Watermarking



Overview of Crypto-System based Multi-Variable Fingerprinting



Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

- Primary input to the fingerprinting approach is a DFG representing a DSP application (to be protected), resource constraints and module library.
- The final output generated from this approach is a buyer's fingerprint protected IP core.
- With the aid of buyer's fingerprint, all the illegally resold pirated copies (by a dishonest vendor) of IP cores can be traced easily. Thus embedded fingerprint thwarts the illegally resold IP cores.
- In the crypto-system based multi-variable fingerprinting, the security constraints representing the buyer's fingerprint are implanted during register allocation phase of ESL synthesis.
- In order to implant constraints during register allocation phase, a CIG based framework is employed.
- The fingerprint constraints to be embedded are selected based on two criteria.
- The first criterion is the fingerprint size (total number of digits) in terms of variables: 'i', 'I', 'T' and '!'. Since, each variable of a buyer's fingerprint carries an encoded meaning, therefore it can be decoded in terms of security constraints for the purpose of implantation.
- However, all the constraints corresponding to all variables are not chosen to be implanted into the design.
- Out of all the fingerprint digits, the potential digits to be embedded as security constraints are decided by selection criteria 1 and 2 jointly.

Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

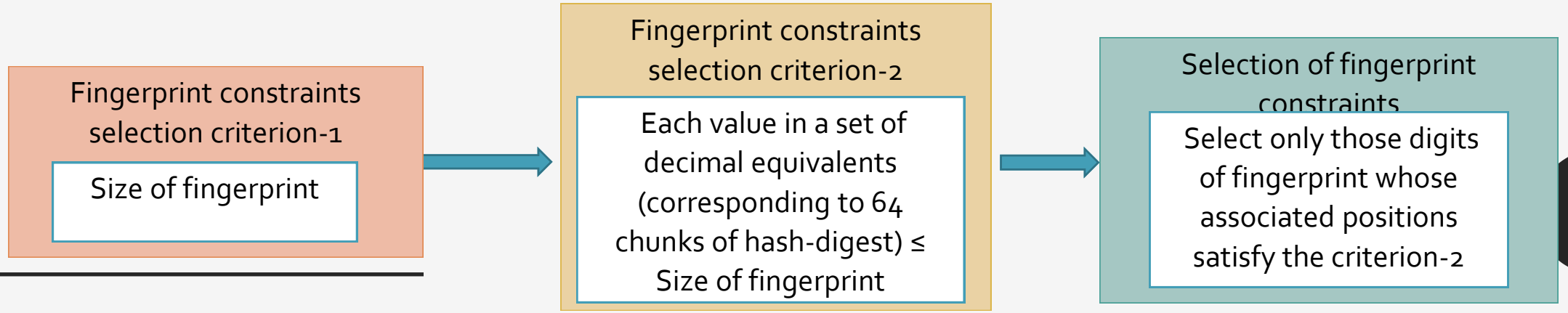
Step by Step Process

- In the first step, the DFG of the intended DSP core is scheduled based on resource (multipliers and adders) constraints.
- The output of this step is a scheduled DFG complying with resource constraints.
- In the next step, the scheduled DFG is encoded into bit-stream format according to certain encoding rules.
- Further, the next step performs a cryptographic hashing on encoded bit-stream of the design.
- This hashing transforms the bit-stream into a secure hash-digest of 512 bits.
- The motive of converting the bit-stream into a secure hash-digest is to obtain a unique and secure representation of the design.
- The collision resistance and pre-image resistance properties aid to fulfil the motive of employing hashing scheme.

Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

Step by Step Process

- Further, the secured hashed bit-stream is fragmented into 64 chunks, each of size 8-bit.
- The decimal equivalents of 8-bit chunks play an important role to determine the fingerprint constraints to be embedded.
- Each value in a set of decimal equivalents (corresponding to 64 chunks of hash digest) which is less than or equal to the size of fingerprint, is the constraints selection criterion-2.
- The process of selecting fingerprint digits based on criteria 1 and 2 is depicted in the Figure below.
- Only those digits of fingerprint whose associated positions satisfy the criterion-2 are eligible to act as security constraints.
- Once the set of selected fingerprint digits is determined, the corresponding security constraints are implanted into the CIG. Thus, fingerprint embedded DSP core is generated.



Selection process of fingerprint constraints based on two criteria

Fingerprinting Methodology- Pre-processing phase and Demonstration

- In order to embed fingerprint, the design needs to be transformed into a suitable format. This transformation phase is referred as pre-processing phase

❖Pre-processing phase

- Schedule the DFG representing the DSP application.
- The scheduling is responsible for performing time stamping of the operations in various control steps based on the algorithm chosen.
- There are several scheduling algorithms that can be used for time stamping such as: As Soon As Possible (ASAP), As Late As Possible (ALAP), LIST scheduling etc.
- LIST scheduling algorithm has been chosen because it allocates the critical operations first, resulting into minimization of latency or delay.

Fingerprinting Methodology- Pre-processing phase and Demonstration

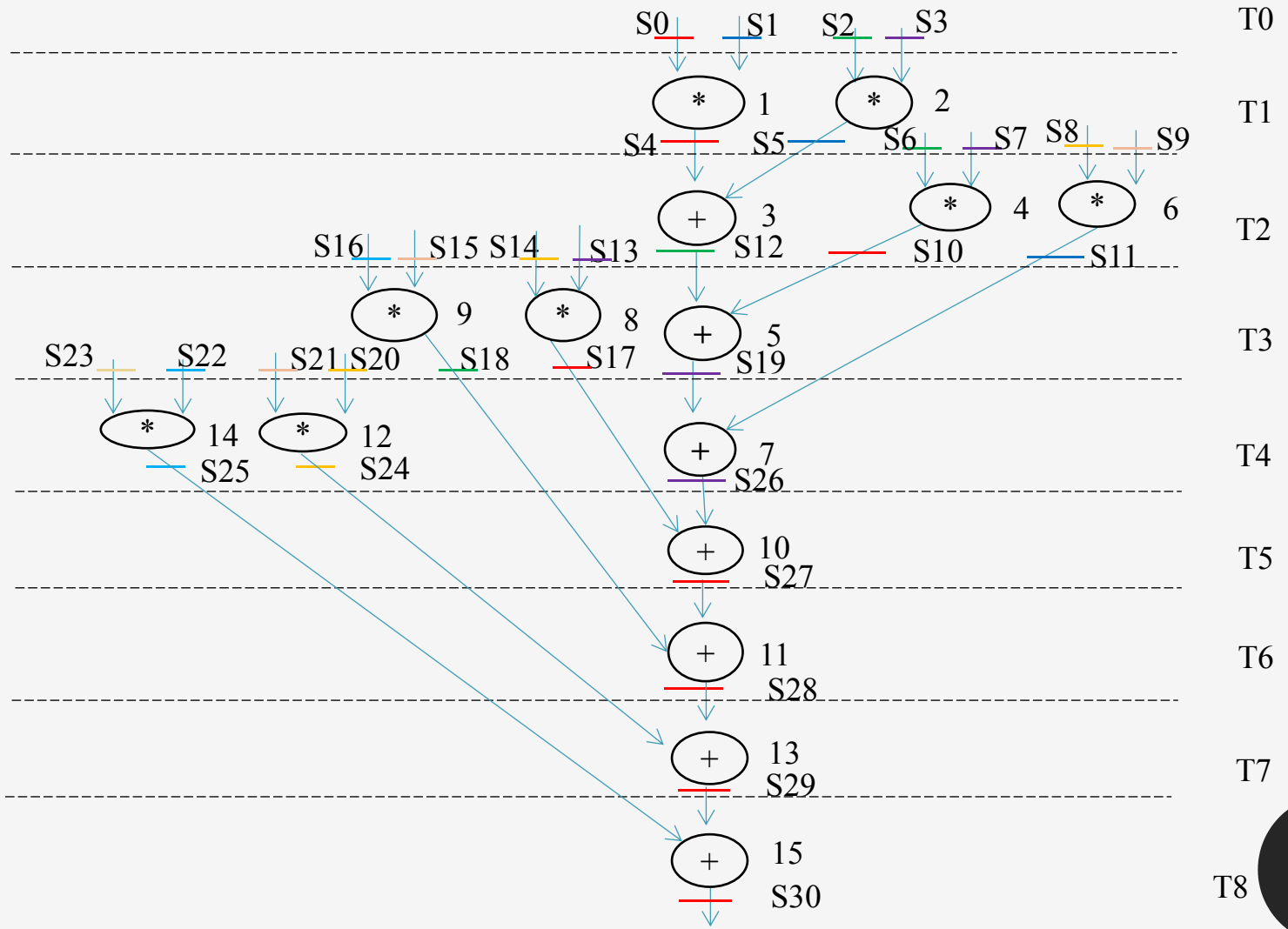
- Encode the scheduled DFG into a bit-stream format as per the table below:

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

- Generate 512-bit hash digest of the bit-stream using SHA-512 algorithm
- Fragment the hash digest into 64 chunks of data where each chunk of data is 8-bit in size.
- Convert each 8-bit chunk of data into corresponding decimal equivalent representation.

Fingerprinting Methodology- Demonstration

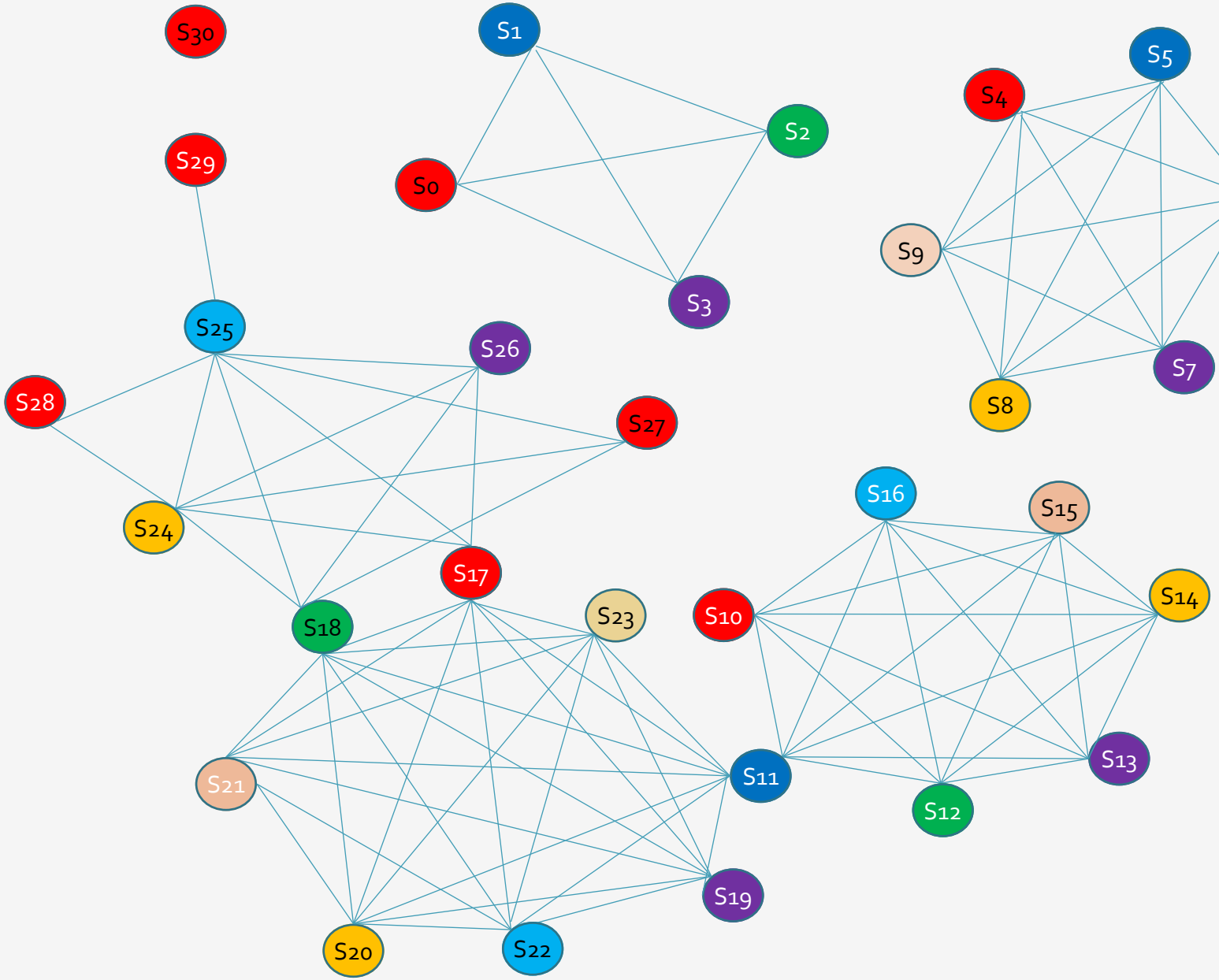
- **Demonstration on DCT core**



Scheduled and hardware allocated 8-point DCT using 1 (+) and 2 (*)

Demonstration

- there are 30 storage variables used for storing intermediate outputs and primary inputs/output.
- This scheduled design represents a baseline version as it does not embed a buyer fingerprint yet.
- The next step is to obtain a graph colouring framework corresponding to the scheduling with storage variables.
- The corresponding CIG is shown in Figure.



Colored interval graph of baseline 8-point DCT core (without fingerprint constraints)

Demonstration

- The corresponding register allocation of 8-point DCT

T	R0	R1	R2	R3	R4	R5	R6	R7
0	S0	S1	S2	S3	--	--	--	--
1	S4	S5	S6	S7	S8	S9	--	--
2	S10	S11	S12	S13	S14	S15	S16	---
3	S17	S11	S18	S19	S20	S21	S22	S23
4	S17	--	S18	S26	S24	--	S25	--
5	S27	--	S18	--	S24	--	S25	--
6	S28	--	--	--	S24	--	S25	--
7	S29	--	--	--	--	--	S25	--
8	S30	--	--	--	--	--	--	--

Demonstration

- In the next phase, the respective bit-stream format is generated using the scheduled design obtained before and the encoding rules shown in the Table .
- For example, in the DCT core scheduling, since opn 1 is executed in control step 1 (T1), thus the encoded value (Eopni) of this operation is 0.
- The detailed encoded values of all operations are shown in the Table. The encoded bits upon appending represent a bit-stream format that is fed into the SHA-512 algorithm.
- This bit-stream format is then converted into 1024 bits using standard appending rules of SHA.
- The SHA block is responsible for generating a 512-bit output that represents the design hash/digest.

Operation number (opn)	Encoded bit (E_{opni})
1	0
2	0
3	1
4	0
5	0
6	0
7	1
8	0
9	0
10	0
11	1
12	0
13	0
14	0
15	1

Demonstration

- The next step is to generate 64 decimal values by dividing the 512 bits into group of 8 bits each. This has been shown in the Table.
- Each decimal value obtained will represent a position in the buyer fingerprint to decide which digits of the buyer fingerprint will serve as secret constraints for embedding into the design.

D	151	124	167	96	57	38	190	63
B	10010111	01111100	10100111	01100000	00111001	00100110	10111110	00111111
D	39	246	226	195	165	143	115	172
B	00100111	11110110	11100010	11000011	10100101	10001111	01110011	10101100
D	132	227	166	22	220	48	109	85
B	10000100	11100011	10100110	00010110	11011100	00110000	01101101	01010101
D	254	68	77	79	150	31	234	53
B	11111110	01000100	01001101	01001111	10010110	11101010	11101010	00110101
D	173	150	63	85	143	224	100	185
B	10101101	10010110	00111111	10001111	10001111	11100000	01100100	10111001
D	221	227	133	114	206	30	106	2
B	11011101	11100011	10000101	01110010	11001110	00011110	01101010	00000010
D	131	117	128	103	63	28	252	84
B	10000011	01110101	10000000	01100111	00111111	00011100	11111100	01010100
D	82	197	40	201	117	200	13	142
B	01010010	11000101	00101000	11001001	01110101	11001000	00001101	10001110

Fingerprinting Methodology- Selection of fingerprint and Embedding process and Demonstration

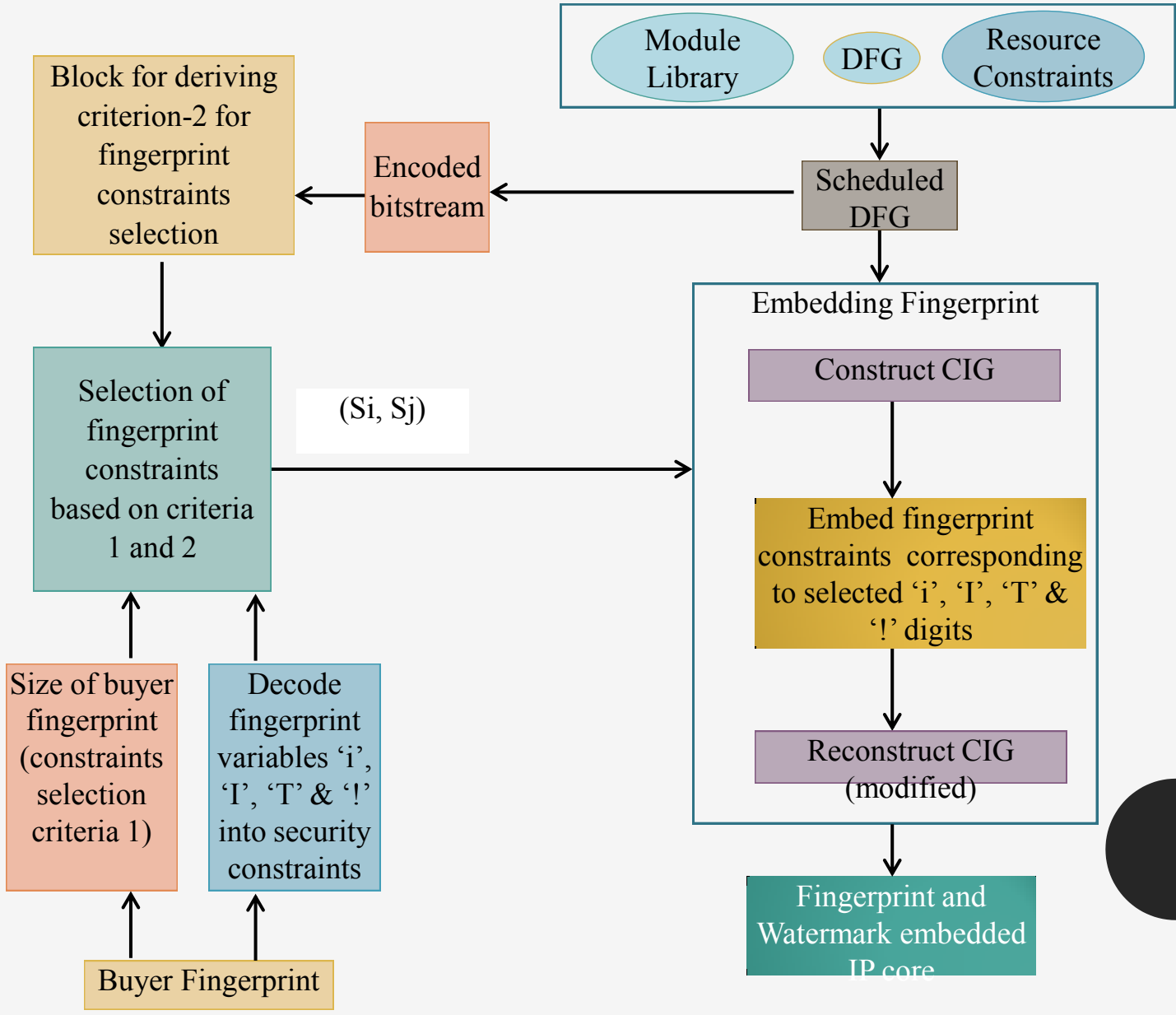
❖ Selection of a fingerprint and Embedding process:

- The first step is to choose a buyer's signature of fixed size consisting of four variables viz. i', 'I', 'T' and '!'.
- The encoding of each variable is shown in Table.
- According to the encoding rules, whenever digit 'i' occurs into the fingerprint, it is decoded as an edge between node pair (Si, Sj) of the form (prime, prime).
- Further, each occurrence of digits 'I', 'T' and '!' are decoded as an edge between node pair of the form (even, even), (odd, even) and (o, any integer) respectively.
- For example, let's consider a six-digit fingerprint "IiiT!I".
- The first digit 'I' is decoded as an edge between the node pair (S2, S4). Similarly, second digit 'i' is decoded as an edge between the node pair (S2, S3). Here, third digit is the second occurrence of 'i', therefore it is decoded as an edge between the node pair (S2, S5).

Variables of buyer's fingerprint	encoding
i	Encoded value of edge with node pair as (prime, prime)
I	Encoded value of edge with node pair as (even, even)
T	Encoded value of edge with node pair as (odd, even)
!	Encoded value of edge with node pair as (o, any integer)

Fingerprinting Methodology- Embedding

- Once a fixed size fingerprint is chosen, the next phase is to implant the fingerprint constraints into a DSP core design.
- Only those fingerprint digits which are selected based on selection criteria 1 and 2, are eligible to be embedded as constraints.
- The embedding process is shown in Figure.



Fingerprinting Methodology- Embedding

- Once the eligible fingerprint constraints are enlisted, they are implanted into the CIG.
- As a CIG represents the sharing of different registers among all the storage variables, implanting edges between node pairs should not result into conflict.
- A conflict occurs when an edge between two nodes of same colour is added.
- The reason is that two different storage variables executing in a same control step, cannot be stored in the same register.
- If an edge results into conflict then it is resolved by swapping of nodes within the same control step (T) so that both storage variables of conflicting edge could be executed through different registers.
- However, if resolving of conflict by swapping of nodes within the same T is not possible then an extra register is used to execute one of the nodes in the pair.
- Post embedding all the selected constraint edges, the CIG is modified.

Fingerprinting Methodology- Demonstration

- Let's assume the 80-digit fingerprint of a buyer is as follows:
- "TII!iiTTii!TITiiiIIIiTTiiiIiIiii!!!ii!IT!!iI!!!ITi!iiT!iiTT!iTiiTT!!!iTIII!Tii!"
- A position associated with each fingerprint digit is shown in Table.

1 T	**2** **I**	3 I	4 !	5 i	6 i	7 T	8 T	9 i	10 i	11 !	12 T	**13** **I**	14 T	15 i	16 i	17 i	18 I	19 I	20 I
21 i	**22** **T**	23 T	24 i	25 i	26 i	27 I	**28** **i**	29 I	**30** **i**	**31** **i**	32 i	33 !	34 !	35 !	36 i	37 i	**38** **!**	**39** **I**	**40** **T**
41 !	42 !	43 I	44 i	45 I	46 !	47 !	**48** **!**	49 I	50 T	51 i	52 !	**53** **i**	54 i	55 T	56 !	**57** **i**	58 i	59 T	60 T
61 !	62 i	**63** **T**	64 i	65 i	66 T	67 T	**68** **!**	69 !	70 !	71 i	72 T	73 I	74 I	75 I	76 !	**77** **T**	78 i	**79** **i**	80 !

- This buyer fingerprint is intended to be embedded into the CIG (corresponding to DCT core)

Fingerprinting Methodology- Demonstration

- Set of all the decimal values (corresponding to 64 chunks of hash) which are less than or equal to size of fingerprint is defined as the constraints selection criterion-2, where size of fingerprint is the criterion-1.
- These two criteria jointly decide the number of fingerprint constraints eligible to be embedded.
- Only those digits of fingerprint, whose associated positions satisfy the criterion-2, are selected as fingerprint constraints.
- Out of 64 decimal values, only 16 digits fall under the size (80) of fingerprint, thus are selected as valid digits.
- The selected digits with their associated positions have been highlighted in the Table in the previous slide.
- Further, the selected digits and their corresponding decoded edges (representing fingerprint constraints) are shown in Table here.

Digit of signature	Decoded edge	Digit of signature	Decoded edge
57	(S_5,S_{19})	22	(S_1,S_{12})
38	(S_0,S_6)	48	(S_0,S_{11})
63	(S_1,S_{26})	68	(S_0,S_{15})
39	(S_2,S_{20})	77	(S_3,S_6)
79	(S_7,S_{23})	2	(S_2,S_4)
31	(S_3,S_{17})	28	(S_3,S_{11})
53	(S_5,S_{13})	40	(S_1,S_{16})
30	(S_3,S_{13})	13	(S_2,S_8)

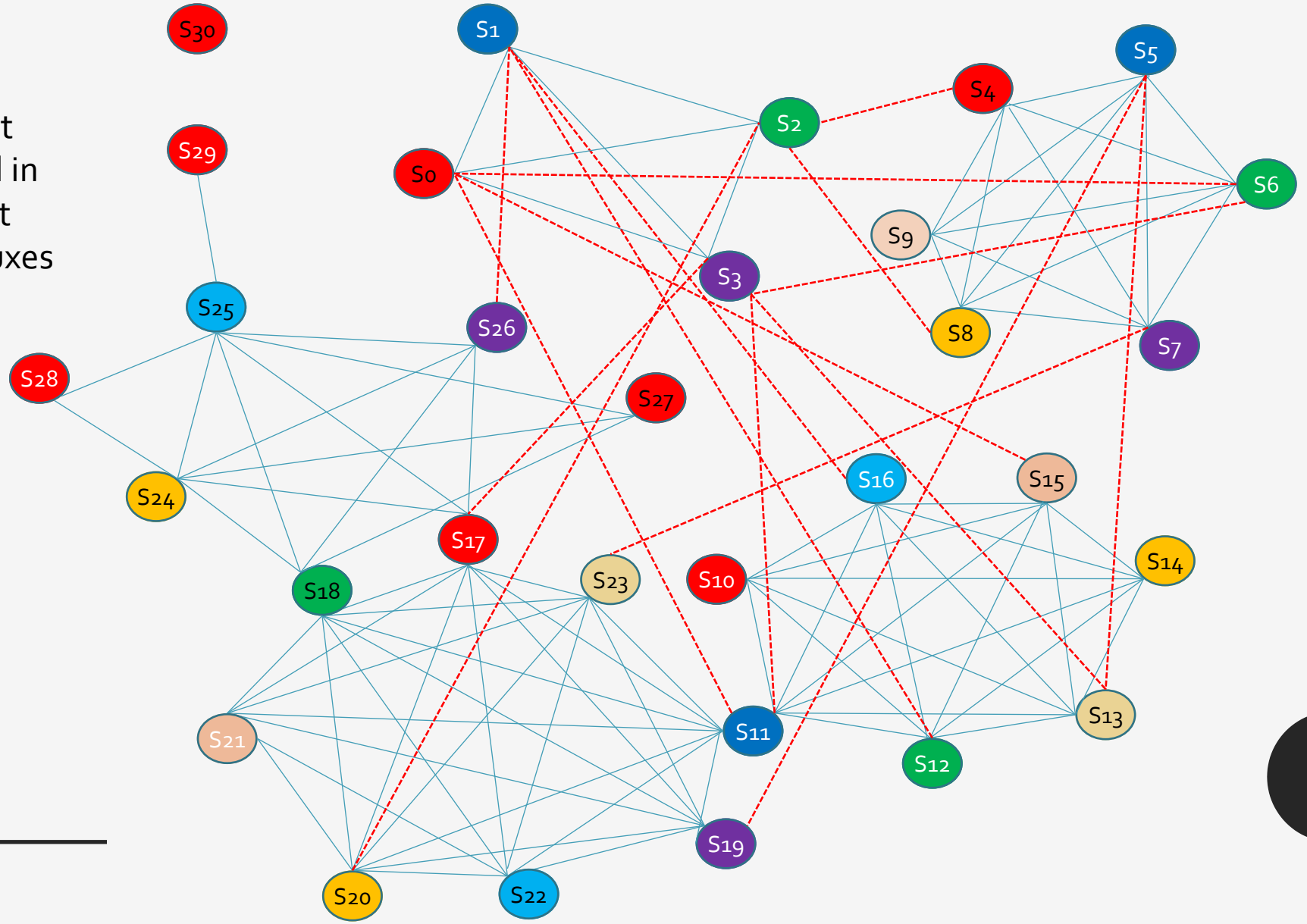
Fingerprinting Methodology- Demonstration

- The constraint edges are implanted into the CIG one by one.
- However, conflict may occur during implantation of some constraint edges.
- For example, direct implantation of edge (S3, S13) corresponding to fingerprint digit 30, is not possible. This is because, both nodes (S3 and S13) share same register R3.
- So, this conflict is resolved by assigning S13 to register R7 in the 2nd control step (T2).
- Likewise, conflict due to other constraint edges can be resolved. Thus all the constraint edges are implanted into the CIG one by one.
- Post embedding fingerprint constraints, modification in register allocation is presented in Table. Further, the impact of fingerprint constraints can also be observed in terms of changes in input-output connectivity of muxes and demuxes at register transfer level (RTL).

T	R0	R1	R2	R3	R4	R5	R6	R7
0	S0	S1	S2	S3	--	--	--	--
1	S4	S5	S6	S7	S8	S9	--	--
2	S10	S11	S12	--	S14	S15	S16	S13
3	S17	S11	S18	S19	S20	S21	S22	S23
4	S17	--	S18	S26	S24	--	S25	--
5	S27	--	S18	--	S24	--	S25	--
6	S28	--	--	--	S24	--	S25	--
7	S29	--	--	--	--	--	S25	--
8	S30	--	--	--	--	--	--	--

Fingerprinting Methodology- Demonstration

- The modified CIG is shown in Figure.
- Further, the impact of fingerprint constraints can also be observed in terms of changes in input-output connectivity of muxes and demuxes at register transfer level (RTL).



Security Analysis using Probability of coincidence (Pc)

$$Pc = \left(1 - \frac{1}{n}\right)^{k}$$

- Where, 'Pc' =probability of coincidence,
- 'n'= the number of colours used in the CIG before implanting fingerprint constraints
- 'k' =the number of additional constraints-edges added or effective fingerprint size (potential fingerprint digits selected through criteria 1 and 2)

Applications	# of registers	Fingerprint Signature Size =80		Fingerprint Signature Size =160		Fingerprint Signature Size =240	
		Effective size (k)	P^c	Effective size (k)	P^c	Effective size (k)	P^c
DCT	10	21	0.109	41	0.013	62	0.0014
IDCT	12	25	0.113	47	0.016	61	0.0049
WDF	7	17	0.072	38	0.002	48	0.0006
MESA	6	22	0.018	29	0.005	38	0.0009
FFT	8	23	0.046	40	0.004	58	0.0004

Security Analysis using Probability of coincidence (Pc)

- Here, probability of coincidence signifies the proof of buyer's right which indicates that a non-fingerprint solution carrying the fingerprint by coincidence.
- Thus probability of coincidence metric reflects the strength of fingerprint.
- As probability of coincidence decreases, the strength of proof of buyer's right increases.
- This is because as more number of fingerprint constraints is embedded into the CIG of the IP core, the likelihood of retaining the same colouring solution by co- incidence is very less.
- The number of effective constraints-edges essentially depends on the fingerprint size.
- The number of effective constraints-edges increases with the increasing fingerprint size as shown in the Table.
- This is because, increasing fingerprint size leads to increase the set of eligible decimal equivalent (based on constraint selection criteria 1 and 2) obtained from the SHA output.
- The impact of three different fingerprint sizes (Q=80, 160, 240) on probability of coincidence has been shown in the Table.
- Therefore, to achieve the stronger proof of buyer's right, a large fingerprint size should be selected.

Design cost (C_{fp}) Analysis

$$C_{fp} = \frac{w1(L_{fp}^{t})}{L_m} + \frac{w2(A_{fp}^{t})}{A_m}$$

- L_{fp}^{t} and A_{fp}^{t} = the total execution latency and area of the design respectively,
- L_m and A_m = the maximum possible latency and area.
- w_1 and w_2 =the weights for latency and area respectively. These weights are specified by the user and their values range between (0, 1) (*Note: To assign similar weightage to both latency and area during cost evaluation, both w_1 and w_2 are fixed at 0.5*).

Applications	Design Cost of Baseline design (no-fingerprint)	Fingerprint Signature Size =80		Fingerprint Signature Size =160		Fingerprint Signature Size =240	
		Effective size (k)	Cost	Effective size (k)	Cost	Effective size (k)	Cost
DCT	0.44	21	0.44	41	0.44	62	0.44
IDCT	0.33	25	0.33	47	0.33	61	0.33
WDF	0.61	17	0.61	38	0.61	48	0.61
MESA	0.64	22	0.64	29	0.64	38	0.64
FFT	0.59	23	0.59	40	0.59	58	0.59

Design cost (C_{fp}) Analysis

- The increase in fingerprint size may also affect the design cost of an IP core.
- However, the presented crypto-system based multi-variable fingerprinting approach does not increase the design cost with increasing fingerprint size.
- The design cost remains same as that of baseline counterpart .
- It is evident from the Table that the presented fingerprinting approach incurs zero or nominal cost overhead, hence leads to very low cost solution.

Comparative Study

- The crypto-system based multi-variable fingerprinting approach (Sengupta et al., 2019), it has been compared with the contemporary fingerprinting approach (Roy and Sengupta, 2017) for DSP cores.
- A comparison based on design cost of fingerprint embedded IP core, is shown in Table 6.12.

DSP applications	Effective # of fingerprint constraints	Design Solution	Design Cost (Sengupta et al., 2019)	Design Cost (Roy and Sengupta, 2017)	Percentage reduction in design cost
DCT	21	2 A, 2 M	0.44	0.46	4.35 %
IDCT	25	3 A, 3 M	0.33	0.37	10.81 %
WDF	17	2 A, 2 M	0.61	0.63	3.17 %
MESA	22	1 A, 2 M	0.64	0.66	3.03 %
FFT	23	4 A, 4 M	0.59	0.63	6.35 %

Comparative Study

- It is evident from the table that (Sengupta et al., 2019) is capable to achieve a lower design cost (post embedding fingerprint) compared to (Roy and Sengupta, 2017).
- This is because, once the effective fingerprint size is obtained, the number of constraints to be embedded remain fixed in the crypto-system based multi-variable fingerprinting approach.
- However for the same effective fingerprint size, the contemporary fingerprinting approach (Roy and Sengupta, 2017) can have numerous possible combinations of fingerprint digits.
- Therefore, number of constraints to be embedded vary and hence impose the various impact onto the design cost.
- Further, this is hard to estimate the optimal combination of the fingerprint digits that would result into lower design cost post embedding.
- Hence, the presented fingerprinting approach is more effective in contrast to contemporary approach

Conclusion

- ❑ This Module presents a fingerprinting approach that is capable to provide exclusive buyer rights protection using fingerprint.
- ❑ Embedded fingerprint helps in tracing the illegally resold IP cores by a disloyal seller, thus protects the buyers rights over the IP cores.
- ❑ At the end of this module, the learning outcome is as follows:
- ✓ Utility of the fingerprinting approach.
- ✓ Application of the fingerprinting approach to protect the buyers rights over IP cores.
- ✓ Desirable features of a buyer's fingerprint.
- ✓ Comparison between watermarking and fingerprinting
- ✓ Encoding rules of the fingerprint variables.
- ✓ Application of SHA-512 to generate unique fingerprint constraints.
- ✓ Design of the fingerprint embedded IP core demonstrated using a real life DSP core application (DCT core).
- ✓ Security and design cost analysis of the fingerprinting approach with respect to baseline counterpart.
- ✓ Comparative study of a fingerprint embedded DSP core with respect to a contemporary fingerprinting approach.

Anirban Sengupta "Protecting Right of an IP Buyer using Cryptosystem based Multi-variable Fingerprinting", 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

- E. Castillo, U. Meyer-Baese, A. Garcia, L. Parilla, A. Lloris (2007), 'IPP@HDL: Efficient intellectual property protection scheme for IP cores,'*IEEE Trans. Very Large Scale Integr. (VLSI) Syst*., vol. 15 (5), pp. 578–590.
- M.C. McFarland, A.C. Parker, R. Camposano (1988), 'Tutorial on high-level synthesis', *DAC '88 Proceedings of the 25th ACM/IEEE Design Automation,*vol. 27 (1), pp. 330-336.
- G. Martin, G. Smith (2009), 'High-level synthesis: Past, present, and future,' *IEEE Des. Test Comput*. vol. 26(4), pp. 18–25.
- A. Sengupta (2017), 'Hardware Security of CE Devices [Hardware Matters],'*IEEE Consumer Electronics Mag,* vol. 6(1), pp. 130-133.
- A. Sengupta (2016), 'Intellectual Property Cores: Protection designs for CE products, '*IEEE Consumer Electronics Mag*, vol. 5, no. 1, pp. 83-88.
- D. Roy, A. Sengupta (2017), 'Low Overhead Symmetrical Protection of Reusable IP Core using Robust Fingerprinting and Watermarking during High Level Synthesis', *Elsevier Journal on Future Generation Computer Systems*, vol. 71, pp. 89-101.
- A. Sengupta, U.K. Singh, P.K. Premchand (2019), 'Crypto based Multi-Variable Fingerprinting for Protecting DSP cores', *IEEE International Conference on Consumer Electronics (ICCE), Berlin*-2019.
- A. Sengupta, S. Bhadauria (2016), 'Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis,' *IEEE Access*, vol. 4, pp. 2198-2215,.
- A. Sengupta, S. P. Mohanty (2019), 'Advanced encryption standard (AES) and its hardware watermarking for ownership protection,' *Book: 'IP Core Protection and Hardware-Assisted Security for Consumer Electronics*', e-ISBN: 9781785618000, pp. 317-335.
- A. Sengupta, S. P. Mohanty (2019), 'IP core and integrated circuit protection using robust watermarking,' *Book: 'IP Core Protection and Hardware-Assisted Security for Consumer Electronics*', e-ISBN: 9781785618000, pp. 123-170.
- D. Roy, A. Sengupta (2019), 'Multilevel Watermark for Protecting DSP Kernel in CE Systems [Hardware Matters],'*IEEE Consumer Electronics Mag*, vol. 8(2), pp. 100-102.
- J. Lach, W.H. Mangione-Smith, M. Potkonjak (2001), 'Fingerprinting techniques for field-programmable gate array intellectual property protection', *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*., vol. 20(10), pp. 1253-1261.
- F. Koushanfar et al. (2005), "Behavioral synthesis techniques for intellectual property protection," *ACM Trans. Des. Autom. Electron. Syst*., vol. 10(3), pp. 523-545.
- A. Sengupta, D. Roy (2017), 'Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach [Hardware Matters],'*IEEE Consumer Electronics Mag*, vol. 6(2), pp. 118-124.

Thank You