Paper ID: 1570943403

Secured and Optimized Hardware Accelerators Using Key-Controlled Encoded Hash Slices and Firefly Algorithm Based Exploration

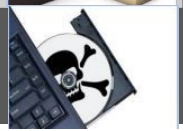
Anirban Sengupta, Aditya Anshul, Chirag Kothari, Sumer Thakur "Secured and Optimized Hardware Accelerators Using Key-Controlled Encoded Hash Slices and Firefly Algorithm Based Design Space Exploration", Proceedings of 35th IEEE International Conference on Microelectronics (ICM), Abu Dhabi, Dec 2023, pp. 149-152

Intellectual Property (DSP IP cores):

- Chips, Integrated circuits, and other designs owned by a company, designer, or manufacturer.
- Processors, Digital Signal Processors (DSP) and other Consumer Electronics hardware.
- These co-processors performs various data-intensive and power-hungry applications involving massive computations like data compression-decompression, digital data filtering, and different complex mathematical calculations.
- Due to globalization of design supply chain, the reusable **IP cores or ICs are prone** to various **hardware threats [1], [2].**

Figure 1: IC design process

Security Issues associated with hardware IP Cores :

Sr. No.		Security Issues	Descriptions
1.		Intellectual property(IP) Cloning:	Assigning different names to the same cloned product.
2.		IP Counterfeiting:	Using different products under the same brand name.
3.		Hardware Trojan Attack:	Malicious circuitry that damages the functionality and trustworthiness.
4.		Overproduction:	Production of IP Cores more than the specified IP vendor licensing limit.
5.		False claim of ownership:	An adversary can fraudulently claim the ownership of IP.

Related Work :

Sr. No.	Existing Work	Technique Used	Remarks
1.	Castillo *et. al.,* [5] (2008)	The paper [5] harnesses the power of MD5 and SHA1 to generate several blocks of signatures.	Fails to integrate a unique natural identity as a security parameter and leads to generation limited security constraints.
2.	F. Koushanfar, I. Hong, and M. Potkonjak [4] (2005)	Hardware watermarking using two-variable (0, 1) signature encoding process.	Weak watermarking mechanism due to involvement of only two variable signature encoding process. The watermark (original signature) inserted becomes vulnerable if relevant information (like signature size, digit encoding, and digit combination) gets leaked.
3.	(a) Sengupta et. al., [2] (2021) (b) Sengupta and Chaurasia [3] (2021)	(a) Palmprint biometric [2] and (b) DNA biometric [3] based hardware security approach.	[2] provides inferior security due to the generation of lesser security constraints than proposed work and incapable of generating optimal architecture solutions. Further, [3] incurs greater computational complexity in signature generation process due to involvement of DNA sequencing apart from generation of lesser security constraints than the proposed approach.

Proposed Work

- The proposed approach presents a hardware security framework capable of generating an optimal architecture solution corresponding to secure hardware IP using key-based encoded hash slices and firefly algorithm-based design space exploration with more robust security.

- The proposed hardware security approach presents a key-controlled encoded hash slice based security framework to generate a unique signature (or template).
- Further, the secret hardware security constraints are determined using obtained signature, which are embedded into the design of hardware IP cores using the register allocation table (RAT) framework of HLS process.
- The embedding of the IP seller's/vendor's authentic signature into the design of hardware IP core protects it from hardware security threats such as false claim of IP ownership and IP piracy.

Importance of Firefly based design space exploration (FF-DSE)

- The integration of the FF-DSE block with the proposed security methodology serves the objective of determining an optimized architectural solution.
- FF-DSE prunes the design search space based on IP vendor specified high level specification such as area, delay, energy, power, etc. corresponding to secured DSP design to generate an optimized low-cost design.

Advantage of FF-DSE over others such as genetic algorithm and bacterial foraging based DSE:

- FF-DSE incorporates essential hyperparameters, such as step-size control and absorption coefficient, to control randomness during the design search,
- FF-DSE employs a divide-and-conquer approach based on the attraction parameter. Fireflies with higher attractiveness gather around local optimums in separate subgroups, eventually leading to the discovery of the final optimal solution,
- The linearly decreasing step size control and absorption coefficient in FF-DSE strikes a balance between exploration and exploitation, ensuring faster convergence to the optimal solution.

Detailed flow diagram of the proposed approach

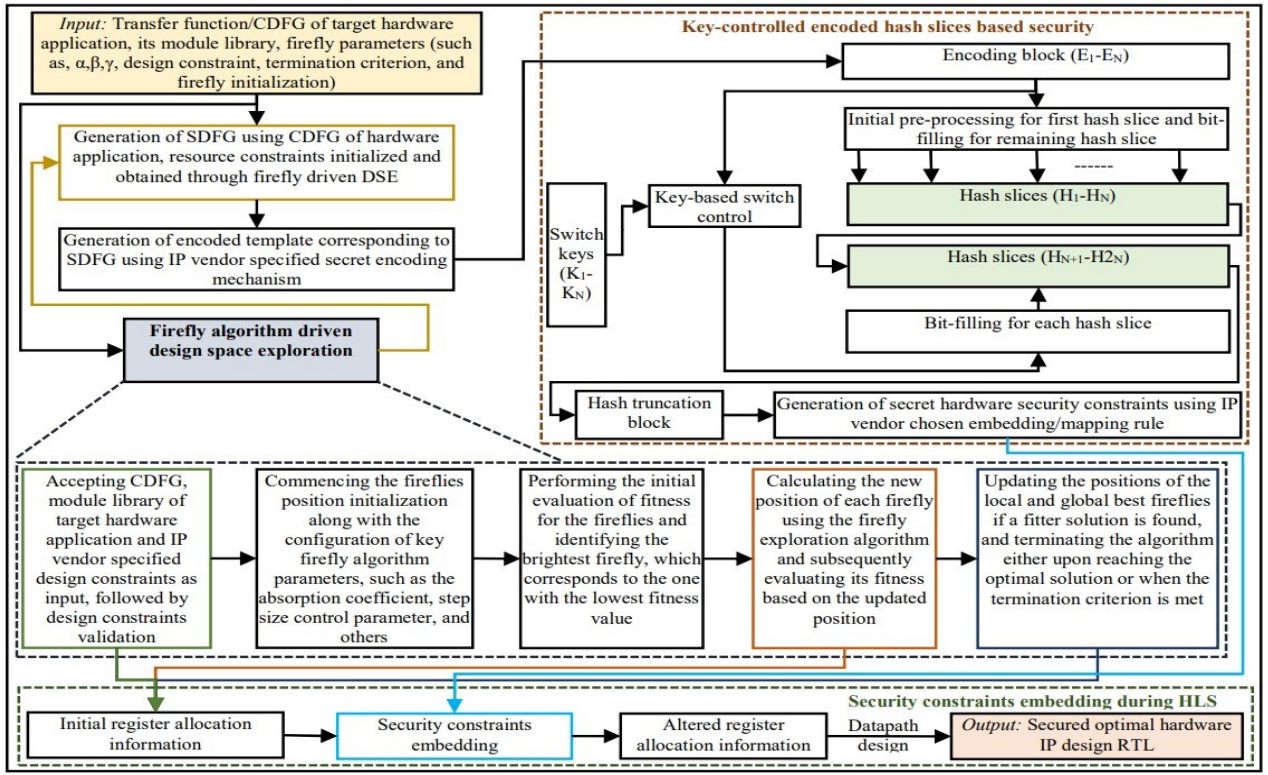


Figure 2: Details of the proposed hardware security framework

Details of Key Controlled Encoded Hash Slice based security module

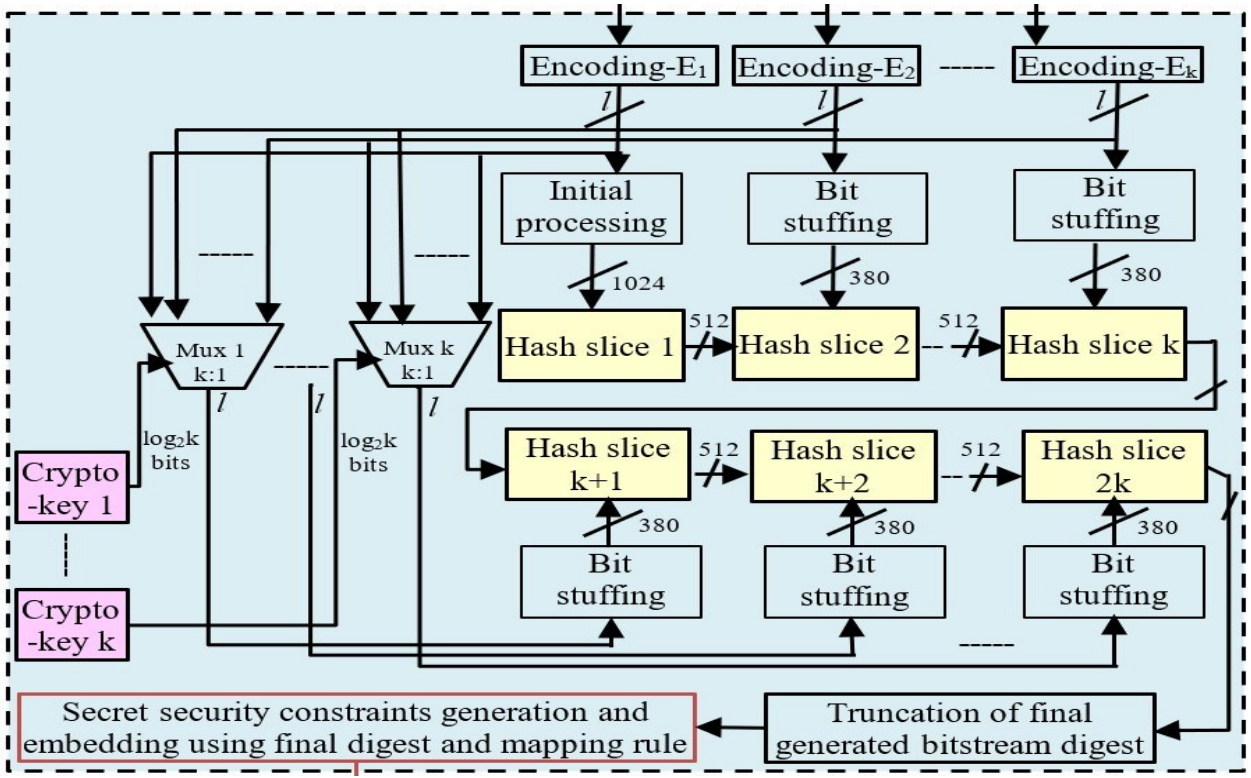


Figure 3: Detailed flow diagram of proposed key controlled encoded hash slice based security module

IP vendor selected encoding rules and scheduled data flow graph (SDFG) of 8-point DCT hardware application

IP vendor selected encoding rules

- En_1: The output bit is '0' if the control step number and the operation number in SDFG are both even, otherwise output bit is '1'
- En_2: The output bit is '0' if the control step number and operation number in SDFG are having same parity, otherwise output bit is '1'
- En_3: The output bit is '0' if the control step number and the operation number in SDFG are both odd, otherwise output bit is '1'
- En_4: The output bit is '0' if the control step number and operation number in SDFG are of different parity, otherwise output bit is '1'
- En_5: The output bit is '0' if the control step number and the operation number in SDFG are both prime, otherwise output bit is '1'
- En_6: The output bit is '1' if the control step number and the operation number in SDFG are both prime, otherwise output bit is '0'
- En_7: The output bit is '0' if GCD of the control step number and the operation number in SDFG is '1', otherwise output bit is '1'
- En_8: The output bit is '0' if the *(operation number) mod (corresponding control step number)* is '0', otherwise output bit is '1'
- En_9: The output bit is '0' if the control step number in SDFG is equal to 2nd odd sequence of operation no., otherwise output bit is '1'

Figure 4: IP vendor selected encoding rules

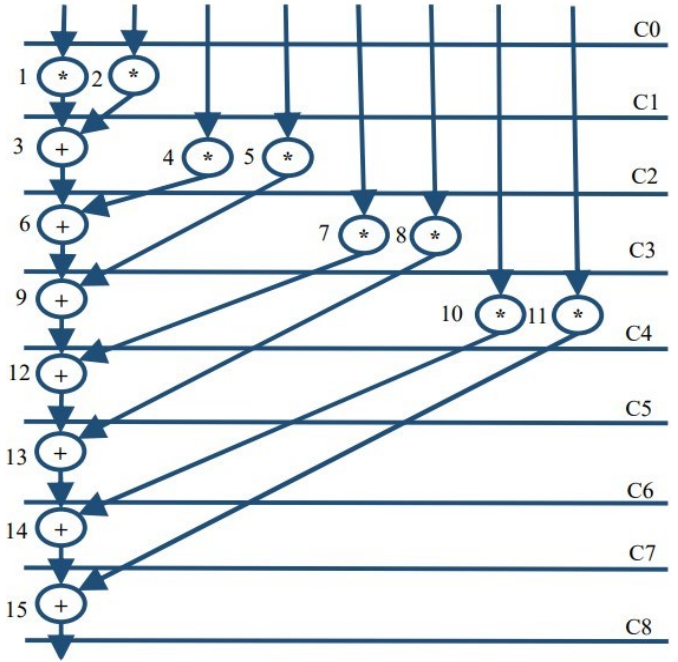


Figure 5: Scheduled data flow graph of 8-point DCT using 1(+) and 2(*)

Generation and embedding of signature as security constraints in the Register Allocation Table (RAT) corresponding to the SDFG of 8-point DCT

- The generated signature is further truncated and converted into covert hardware security constraints using IP vendor selected truncation length and mapping/embedding rule, respectively.
- ***Mapping/Embedding rule:*** Implant an additional artificial edge within (even, even) pairs of storage variables in the register allocation table (RAT) when the bit is '0'. Conversely, an edge is integrated between (odd, odd) storage variable pairs of the RAT when the bit is '1'. The final obtained security constraints are: *(D0,D2), ----- (D28,D30), (D1,D3), ----- ,(D25,D29).* The generated security constraints are embedded into the RAT of respective hardware application.

Table I
Register allocation table pre and post embedding generated signature

CS	*R*	*G*	*I*	*B*	*Y*	*Bl*	*V*	*P*	*L*	*O*	*A*	*T*	*G*	*M*	*S*	*K*
0	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15
1	D16/D17	D17/D16	D2	D3	D4	D5	D6	D7	-	-	-	-	-	-	-	-
2	D18	D19	D24/D19	D18	D4	D5	D6	D7	-	D24	-	-	-	-	-	-
3	D20	D19	D21/D19	D25	D21	D20	D6	D7	D25	-	-	-	-	-	-	-
4	D20	D22	D21	D23	D26/D21	D20	D23	D22	-	-	D27	-	-	-	-	-
5	D27	D22	D21	D23	-	-	D23	D22	-	-	-	-	-	D28	-	-
6	D28	D22	-	D23	-	-	-	-	-	-	-	-	-	-	-	-
7	D29	-	-	D23	-	-	D23	-	-	-	D29	-	-	-	-	-
8	D30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D30

Evaluation parameters [7]-[9]:

- **Tamper tolerance:**

$$TT = q^t$$

Where ‘q’ and ‘t’ are types of encoding bits present in the mapping rule and strength (size) of generated security constraints respectively.

- **Design cost:**

$$Cost = t1 * \frac{Area}{Max\ area} + t2 * \frac{Latency}{Maximum\ latency}$$

Where ‘area’ and ‘latency’ represents the total area and latency (delay) of the proposed methodology-based secured IP core design; ‘max area and max latency’ depict the maximum area and latency of the proposed secured design of IP core using maximum resource constraints possible. ‘t1 and t2’ are the weighing factors (weightage given to are and delay), which in the proposed approach is 0.5 each.

- **Entropy :**

$$X_E = ((1/2^d * 1/m!) * ((1/2^k)*(1/R)*(1/2^{64})))$$

*w*here '*d*' is the final generated palmprint template strength (magnitude) and '*m*' is the total number of features selected on the palmprint, '*k*' is the length of truncated encoded hash, '*R*' is the round computation's maximum value, and $(1/2^{64})$ is the probability of finding the exact key hash buffer initialized value in SHA-512 cryptographic module (each hash buffer is initialized with pre-defined 64-bit value).

Result

Table II
Comparison of entropy and tamper tolerance between the proposed approach, [2], [3], [4], [5], and [6] corresponding to 8-point DCT

Security approach	Security parameters		
	Embedded security constraints	Entropy	Tamper tolerance
Proposed approach	496	3.68E-172	2.04E+149
Palmprint biometric [2]	125	1.93E-55	4.25E+37
Encrypted signature [5]	160	2.01E-87	1.46E+48
Watermarking [4]	240	1.66E-111	1.76E+72
DNA biometric [3]	128	2.9E-39	3.40E+38
HDL watermarking [6]	256	5.85E-99	1.15E+77

Table III
Optimality analysis and design cost of proposed technique for 8-point DCT

Parameters	Values
Spacing (S_A)	0.48
Generational distance (G_D)	0
Weighted metric (W_M)	0.17
Spread (S_D)	0.34
Design cost	-0.132
Area	182.45 um^2
Latency	1324.85 ps

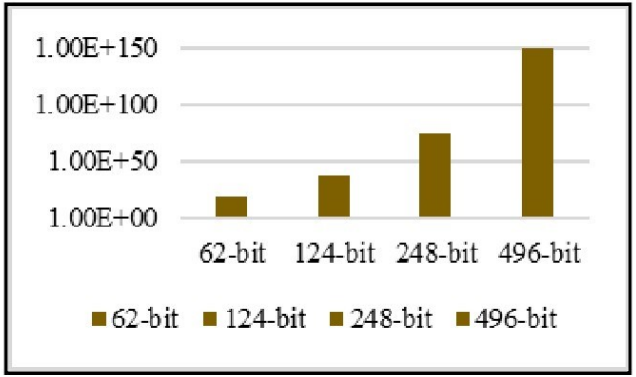


Figure 6: Security analysis of the proposed approach in terms of tamper tolerance with varying signature sizes

References

1. C. Pilato, S. Garg, K. Wu, R. Karri and F. Regazzoni, "Securing Hardware Accelerators: A New Challenge for High-Level Synthesis," *IEEE Embedded Systems Letters*, vol. 10, no. 3, (2018), 77-80, Sept.
2. A. Sengupta, R. Chaurasia, T. Reddy, "Contact-Less Palmprint Biometric for Securing DSP Coprocessors Used in CE Systems," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 3, (2021), 202-213.
3. A. Sengupta, R. Chaurasia, "Securing IP Cores for DSP Applications Using Structural Obfuscation and Chromosomal DNA Impression," *IEEE Access*, vol. 10, 2022, 50903-50913.
4. F. Koushanfar, I. Hong, M. Potkonjak, Behavioral synthesis techniques for intellectual property protection, *ACM Trans. Des. Autom. Electron. Syst*. 10, 3 (2005), 523–545, July.
5. E. Castillo, L. Parrilla, A. Garcia, U. Meyer-Baese, G. Botella, A. Lloris, "Automated Signature Insertion in Combinational Logic Patterns for HDL IP Core Protection," *2008 4th Southern Conference on Programmable Logic, Bariloche, Argentina*, (2008), 183-186.
6. T. Yu and Y. Zhu, "A new watermarking method for soft IP protection," 2011 International Conference on Consumer Electronics, *Communications and Networks (CECNet)*, China, 2011, 3839-3842.
7. Open Cell NanGate Library, 15 nm open cell library, Available: https://si2.org/open-cell-library/, last accessed on March 2023.
8. A. Sengupta, R. Chaurasia and A. Anshul, "Robust Security of Hardware Accelerators Using Protein Molecular Biometric Signature and Facial Biometric Encryption Key," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 6, 826-839, 2023.
9. B. L. Gal and L, Bossuet, Automatic low-cost IP watermarking technique based on output mark insertions. *Des. Autom. Embedded Syst.* 16, 71–92,2012.

Thank You!