Severity Index Based Adaptive Hardware Cryptographic System

1 Dr. Srividya B V
Lincoln Global Postdoctoral Research (LGPR), Lincoln University College, Malaysia
2 Upendra Kumar,
Lincoln Global Postdoctoral Research (LGPR), Lincoln University College, Malaysia
CA: Srividya B V, pdf.Srividya@lincoln.edu.my

Abstract:
In this work, an adaptive cryptographic system is designed using Finite State machine, for a secured and intelligent hardware based data protection. The proposed system dynamically selects cryptographic algorithms based on a severity index computed from the probability of malware and probability of anomaly detection. By continuously analysing security threats, the framework adjusts the encryption strength to provide efficient and reliable protection under varying attack conditions. The architecture integrates adaptive key management technique to improve system security while reducing computational overhead. The proposed approach enhances real-time cyber security performance and is suitable for secure healthcare, IoT, and embedded system applications. The work is carried out using Cadence NcLaunch for simulation and Genus tool for synthesizing RTL to gate level netlist. The performance of the adaptive cryptographic system is measured in terms of power, area and timing using 180nm, 90nm and 45nm technology for comparison. Also a GDS-II file is generated as a part of the final output.

Keywords: Cryptography, FSM, AES, ECC, Edwards curve, Severity Index

Introduction:
Finite State Machines are the basic building blocks in digital circuit design, providing a structured approach for modelling and controlling the sequential logic. FSM consists of finite number of states, transition between states triggered by input events. As the demand for physical design is increasing, FSM approach is used as it ensures high performance, low power consumption and reduced area.
This work presents, selection of a cryptographic algorithm based on the severity Index. The severity index is a weighted sum of Probability of malware and probability of anomaly.

$$SI = 0.6 \times Pm + 0.4 \times Pa$$

Selects of a particular algorithm is explained in Table 1.

Table 1: Mode selection based on Severity Index

Sl. No.	Severity Index	FSM State	Algorithm selected
1	$0 \le SI \le 0.3$	00	None
2	$0.3 \le SI \le 0.6$	01	AES 256
3	$0.6 \le SI \le 0.8$	10	ECC
4	$0.8 \le SI \le 1$	11	Edwards curve cryptography with Digital Signature Algorithm

Literature Survey:

This survey focuses on contribution made by researchers in the field of digital system design by implementing RTL to GDS-II using various technology files.

The authors of [1] have implemented AES encryption and decryption algorithms in Cadence Virtuoso by designing Shift register, Key generation module, XOR and NOR gates as leaf nodes. They have functionally verified working of the module and also have determined the power consumed for the complete analysis.

The authors of [2] have implemented Harvard structure RISC processor from RTL to GDS-II and have carried out the post layout simulations using 180nm Technology.

Amit Sohal in article [3], has integrated Finite State machine approach for designing a concurrent adder and counter using Cadence. The authors have synthesized the RTL using Cadence Genus and have performed post CDS optimization to obtain an improved performance. They have used 90nm technology.

The authors of [4], have implemented Telecommunication receiver from RTL to GDS-II, by using Cadence EDA tools. The authors of [5], has focused on FSM optimization using 32nm standard cell library, by adopting Moore FSM and gated data path control.

Proposed Method:

Figure 1 shows the Finite state machine approach for the adaptive cryptosystem. Based on the severity of threat in the health care infrastructure a suitable security algorithm is selected to protect the information on the compromised node.

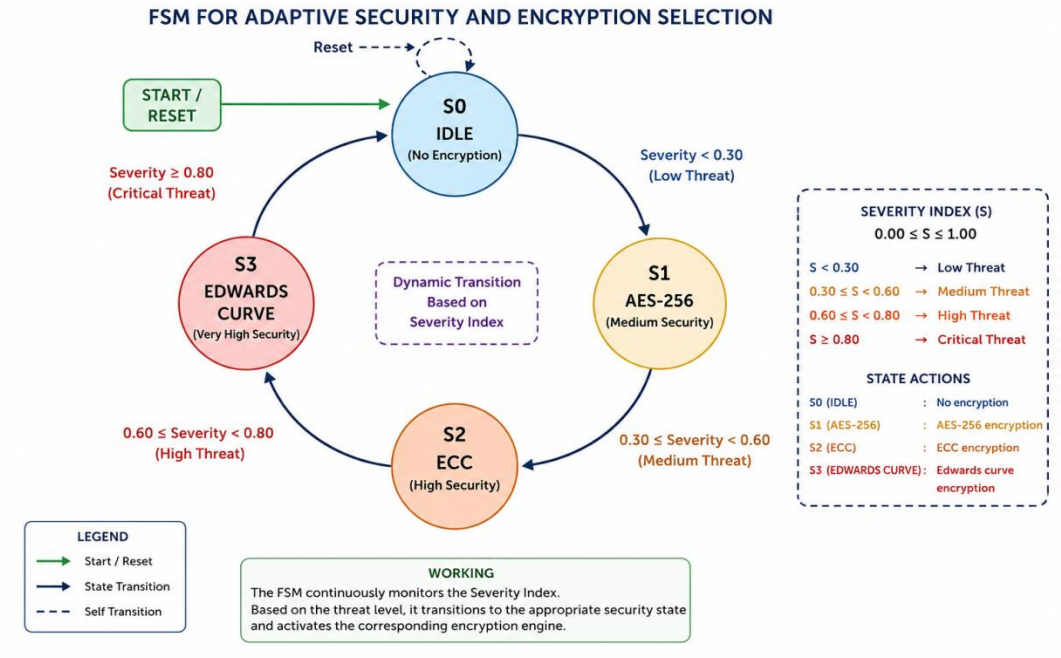

Figure 1: FSM for Adaptive Cryptosystem

The adaptive cryptosystem is also integrated with a key management module to generate the keys, followed by checking validity of the keys, which is based on number of iterations used, and time stamp.

Results:

Figure 2, shows the mode selection, based on the probability of malware (Pm) and probability of anomaly behaviour (Pa). The values are in hexadecimal representation. The correctness of results obtained ensures the functional verification of the system.

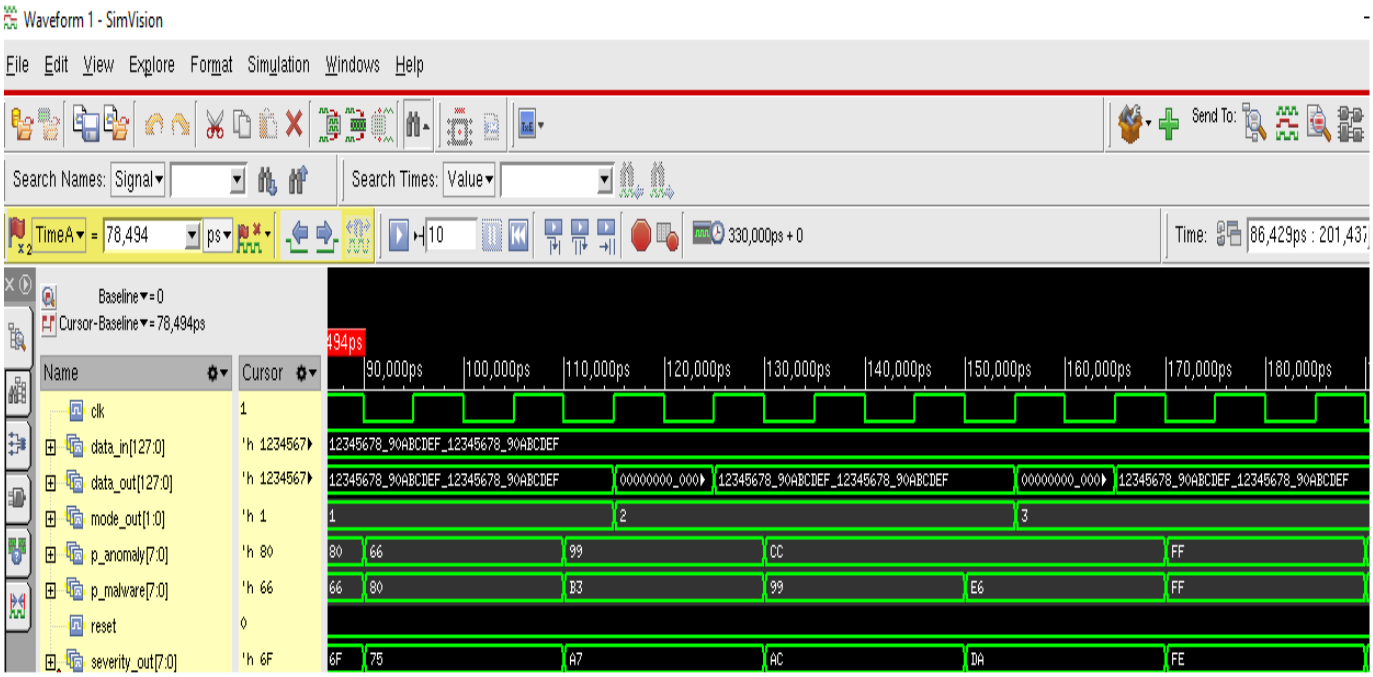

Figure 2: Mode selection. Encryption and decryption of the selected algorithm

Figure 3, shows the key generation for AES algorithm, mathematically related public key and private key for ECC and for Edwards curve cryptography.

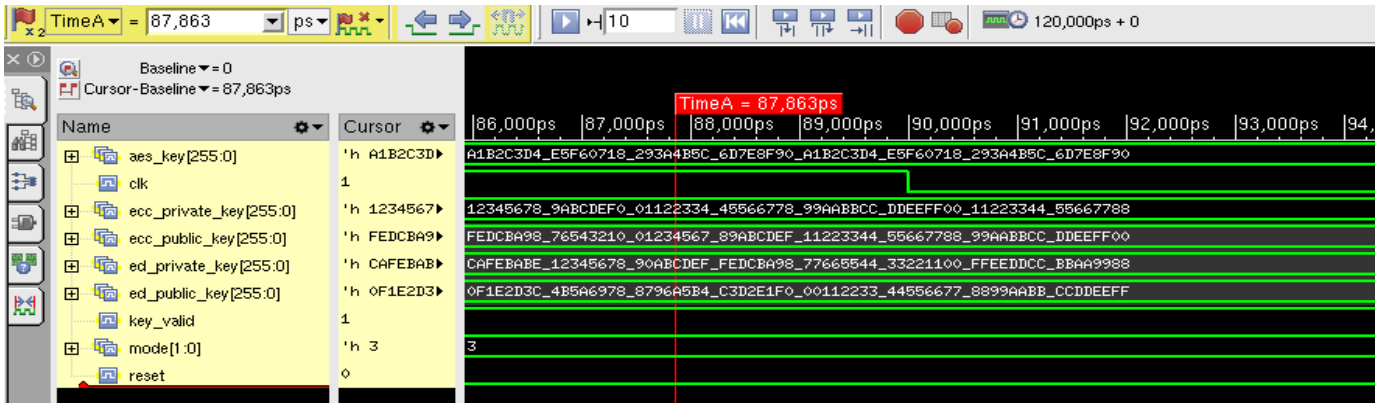

Figure 3: Key Generation and validity of the key

Table 2, 3, 4 and 5 depicts the variations in the performance parameters with respect to AES256, ECC, Edwards Curve and the adaptive cryptosystem respectively. Each parameter is evaluated using 45nm, 90nm and 180nm technology files.

Table 2: Performance of AES-256

Algorithm: AES-256	180nm	90nm	45nm
Area	28344.255um^2	28344.255um^2	28344.255um^2
Gate count	670	670	670
Leakage Power	9.26684e-07	4.91318e-05Watts	3.06873e-07
Internal Power	2.53750e-03	6.31502e-04 Watts	4.53298e-04
Total Power	2.99817e-03	7.71252e-04 Watts	5.40324e-04

Latency	6.373ns	4.676ns	3.657 ns
Frequency	156.9MHz	213.8 MHz	273.4 MHz

Table 3: Performance of ECC

Algorithm: ECC	180nm	90nm	45nm
Area	1818799.0 um^2	350730.804 um^2	350730.804 um^2
Gate count	92016	49067	49067
Leakage Power	8.87086e-05 Watts	1.82199e-03 Watts	1.25426e-05 Watts
Internal Power	1.02464e-01 Watts	1.19134e-02 Watts	1.58947e-02 Watts
Total Power	1.83602e-01 Watts	2.00981e-02 Watts	2.21914e-02 Watts
Latency	9.962ns	9.664 ns	9.684 ns
Frequency	100.38GHz	103.48 MHz	103.26 MHz

Table 4: Performance of Edwards Curve cryptography

Edwards Curve	180nm	90nm	45nm
Area	84573.721um^2	24361.583um^2	21362.392um^2
Gate count	4620	4368	4098
Leakage Power	2.28261e-06	1.18987e-04Watts	1.14365e-06
Internal Power	4.24196e-03	1.21494e-03Watts	1.36977e-03
Total Power	6.19048e-03	1.70447e-03Watts	1.84756e-03
Latency	9.296ns	9.554 ns	9.697 ns
Frequency	107.57MHz	104.67 MHz	103.12 MHz

Table 5: Performance of adaptive cryptosystem

Adaptive Cryptosystem	180nm	90nm	45nm
Area	53541.736 um^2	53541.736	53541.736
Gate count	1586	1586	1586
Leakage Power	1.60109e-06	1.60109e-06	1.60109e-06
Internal Power	8.82770e-03	8.82770e-03	8.82770e-03
Total Power	1.05923e-02	1.05923e-02	1.05923e-02
Latency	9.304ns	9.299 ns	9.299 ns
Frequency	107.48Mhz	107.54 MHz	107.54 MHz

From the comparison tables 2, 3, 4 and 5, it can be observed that number of gates almost remain the same for any technology file, because the RTL functionality and logic structure do not change. The chip area, slightly decreases as the technology scales down. The chip area for 180nm occupies the largest silicon area. There is a moderate reduction while using 90nm and 45nm technology.

Latency is the total time required to process the data and produce the output. The latency decreases as the technology scales down. Frequency of operation is inversely proportional to latency. As technology scales down, frequency increases, indicating more number of operations can be performed per clock period.

Conclusion:

The adaptive cryptosystem is suitable for real-time cryptographic applications such as secure communication, IoT security, and embedded systems. As technology scales down, performance of the system in terms of area, timing and power is significantly better.

References:

1. Deepa M, Varssha B, Abinaya E, “An Efficient Implementation of AES Algorithm for Cryptography Using CADENCE”, 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 1478-1484. https://doi.org/10.1109/iceca58529.2023.10395793, 2023
2. Aradhya, HV Ravish, Gopal Kanase, and Y. Vinayakgouda. “RTL to GDSII of Harvard Structure RISC Processor.” 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT). IEEE, 2021.
3. Shohal, A., & Kaur, J., “Efficient RTL to GDS II Flow for Finite State Machine Integration: A Physical Design Approach”, 2024 IEEE 5th India Council International Subsections Conference (INDISCON), 1-5. https://doi.org/10.1109/indiscon62179.2024.10744369.
4. K., J., R, A., & B.S., P. (2024). Area and Power Optimized RTL to GDS II Flow of a Telecommunication Receiver Core. 2024 5th International Conference on Circuits, Control, Communication and Computing (I4C), 207-212. https://doi.org/10.1109/i4c62240.2024.10748428.
5. Kumar, A., Somineni, R., & Kumar, R. (2025). Improved FSM-Based RTL-to-GDSII Flow: A Power Efficient Design. 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), 1-6. https://doi.org/10.1109/iacis65746.2025.11211479.