Optimizing System Performance using AES for Hardware Trojan Detection with Minimizing the Area

LOHITH S, LOKITH N, MADHANKUMAR M, HARI KUMAR S
[1] *Student, Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India*
[2] *Student, Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India*
[3] *Student, Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India*
[4] *Assistant professor,*
Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

ABSTRACT: Hardware Trojan (HT) poses a recent and significant challenge in computer systems, especially those crucial for mission-critical functions like medical or military applications. Proposed effects range from complete gadget malfunction to the potential leakage of sensitive information, impacting the device's dependability. Despite numerous algorithm types, this study focuses on the AES algorithm, known for utilizing a substitution permutation network concept through a chain of linked operations that replace and shuffle input data. The study systematically reviews various Hardware Trojan areas within the AES algorithm, highlighting potential vulnerabilities. Alongside this analysis, the research explores strategies to prevent these Trojan attacks, emphasizing the need for robust security measures. The recommended efforts aim to decrease the average area, contributing to enhanced reliability in the face of Hardware Trojan threats. The observation of the AES algorithm input-output requirements, even for 128-bit encryption, underscores the critical importance of these findings for future security considerations.

I. INTRODUCTION

A specific kind of malicious circuitry that affects the reliability and efficiency of an electrical system is called a Hardware Trojan (HT). The physical characteristics and actions of a Hardware Trojan are what completely identify it. All of a trojan's activation-related activities are incorporated in its payload, which is an HT. Trojans try to breach or deactivate security measures on a system. There are several potential consequences for this Trojan. They might cause a denial of service, affect system performance, or even monitor confidential information that is computed inside. Unreliable foundries may use hardware Trojans in the design phase of manufacturing to prevent designers from adhering to hardware obfuscation. The ultimate goal of installing a Trojan is to damage the system or (expose. As Trojans first emerged, there were lots of worries about potential risks to defence systems. Undefined functionality is a prevalent characteristic of hardware that may be used as a backdoor for intrusions or as a channel for information leaks. The trojan is identified by the Advance Encryption System AES) algorithm in the chip's input and output ports, where it is joined by an additional trojan circuit that is linked to the AES algorithm.

Hardware Trojans can be added to computer chips as covert "Front-doors" through the use of application-specific integrated circuits (ASIC) or semiconductor intellectual property cores (IP-Internet Protocol Cores) from dubious sources, or by rogue employees installing them themselves or through spying and surveillance. The most widely used cryptographic method that is vulnerable to hardware trojans in cryptographic cores is AES. Side channel attacks are common in the field of hardware security. The trigger and payload are the two primary components of the Trojan, according to the hardware structure. Many ways of detection, a classification of Trojans, and some strategies to stop the HT, like as logical coking. In addition, trojans can be activated by irregular signals, and the diversity of these signals makes it challenging to create a single, comprehensive detection technique. Unreliable designers may include RTL-level trojans, and HT may include soft IP core from third parties. Logic testing HT detection is used to enable the HT with unusual inputs and compare the results with benchmark values on automated tests. Metrics including route delays, leakage, and transient currents are compared with data from golden chips that are produced in a dependable environment. It is difficult to identify minute changes because of noise and process variations. trojans in deep submicron designs, and there is a considerable chance of a false positive. It's still difficult to find the little trojans inserted during production, therefore you need to establish the right side-channel technique and logic testing procedures. Techniques for verification look at the intended functionality of RTL implementation. Difficulties in Detecting

Hardware For verification specialists, RTL implementation is still a relatively new technology, hence it is imperative that verification search for any unfavourable behaviour in the RTL implementation. Examining if hardware Trojans may be found in external IP cores The challenge of locating trojans in third-party IP cores will include the use of code coverage and system Verilog assertions.

II. AES ALGORITHM

In accordance with AES-128/198/256 bits, the entire process requires 10/12/14 rounds. For AES-128 bit, both the input data and key are 128 bits, and a single cycle is needed to finish each round. With the exception of round 10, each AES algorithm round consists of the following steps: add round key, sub bytes, shift rows, and mix-columns. AES is widely employed in data security. Applications of the AES algorithm include storage encryption, database encryption, and self-encrypting disc drivers. In the Add-Round Key transition, the State receives a Round Key using a simple bitwise XOR operation. All that's involved in the first stage of the AES algorithm is an XOR operation. The S-primary Box's function is to transform 8-bit input data into 8-bit secret data (LUT) by using a pre-generated look-up table. Transformation of Bit Substitution: Using the Galois Field (28) and the irreducible polynomial x8 + x4 + x3 + x +1, AES generates the S-Box. The rows and columns of the AES S-Box matrix, which has 16 × 16 = 256 elements, can have values between 0 and 15. In hexadecimal, 0 to f. The replacement of an S-box value for a byte is a non-linear transformation. For the S-box, its usage in the algorithm is predefined. Data S-box is utilised for substitute. The work is accomplished by a series of connected procedures that include the replacement and shuffling of the input data. When encrypting data, AES works with bytes rather than bits. You may think of the S-box as a lookup table. In the same way that we may regard the first four bits of each block as the row index and the final four bits as the column index, bytes can also be used to replace blocks. The outcome of the S-box may be retrieved by the designer by using those same row and column indices.

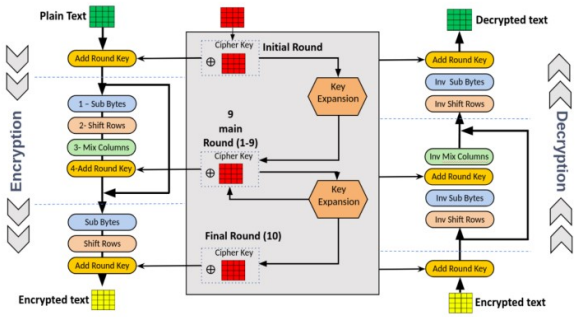

Fig 1: AES architecture flow

This procedure periodically shifts each row of the state to the left, depending on the row index. There has been a 0 space leftward shift of the first row. To the left of the second row, there is an additional space. To get to the third row, go two spaces to the left. The fourth row is moved three places to the left. Column per column, the Mix Columns translation operates on the State by treating each column as a four-term polynomial. The columns are considered as polynomials over GF (28), multiplied by a fixed polynomial modulo x4 + 1. The AES key expansion algorithm takes a 4-word key as input and returns a 44-word linear array. Every round, four of these words are utilised.

AES Benchmark Circuits: There are 21 circuits to gauge trust-hubs. The purpose of the additional 18 Trojan benchmarks is to incentivize side channels to divulge private data, such as cryptographic keys. For DoS, three distinct kinds of Trojan benchmarks have been created. Three other Trojans are simulated alongside the AES HTs (T100, T200, and T300) for reference. For a few cycles, there is hardly any geographic shift. Modifications to the design limitations may cause slight variations in the area values. The introduction of a Trojan won't have a major impact on the area. Additionally, it displays how much electricity a Trojan-infected circuit and a golden circuit use dynamically. The dynamic power is computed for the RTL implementation using a Verilog testbench. For the purpose of computing dynamic strength, The same test bench is used to run Golden Design with all 21 AES Trojan benchmarks and without any modifications to the input stimulus vectors. The two primary categories of the Benchmarks are always-active HT and conditionally-triggered Trojans. not concentrated on Rivest Shamir Adleman, or RSA. With the exception of the three AES HT benchmarks (T100, T200, and T300), which are always active, the next three benchmarks are conditionally engaged. Benchmarks fall into two categories: denial-of-service (DoS) attacks and trojans that leak information, depending on how

they are meant to be used. The trojan benchmarks are used in these assaults.

AES Benchmarks	Outcomes	Side Channel	DESCRIPTION	REFERENCE
T100	Information Leaking	Based on Power	A CDMA code sequence was created by the Trojan using a pseudo-random number generator. When a sequence of CDMA is delivered to a circuit with a leak, a covert power side-channel technique is produced. A predefined value was used to set up the PRNG. (always on Trojan)	[1][5]
T200	Information Leaking	Based on Power	Similar to T100, Initialization text for the PRNG is predetermined. (always being on HT)	[15][17]
T300	Information Leaking	Based on Power	The Trojan uses a leaking circuit to leak single byte depends key schedule.	[14]

Table I: Selected Benchmarks for AES from Trust-Hub are described

III. PROPOSED ALGORITHM

The little difference between golden and benchmarks renders impossible to determine whether a design is Trojan-infected based just on area and power measures. The dynamic power levels showed little variation between the on and off states of Trojan. Table II shows the average area and dynamic power following the modelling of HT impacted with and HT free circuit with different input circumstances. The area little changes across only a handful of circuits. Design limitations may also cause the area values to change somewhat. When using the golden tree strategy, the area and power are smaller than with other methods. The article identifies the RTL analysis detection, and the World Wide Web protocol is used With the objective to expedite the process. Glitches in FPGAs mostly result from mismatched signal arrival timings at LUTs. A LUT output may experience many transitions in response to changes in the input because of this issue. Pipelines prevent mistakes because they prevent errors from passing through edge-triggered flip-flops before the clock signal is received. ASICs provide a more convenient way to generate clocks and allow for precise control over delay times.

The loop unwinding approach is utilised, but the area is less and the power decreases as the speed increases. Additionally, the number of repetitions in the AES algorithm is reduced, and as a result, the registers and FF that are not in use are used as delays in trojan circuits. The trojan circuit uses less trojans when the circuit's triggering is postponed. It could be difficult to tell whether a Trojan has penetrated the third party's IP core or RTL code based on the erratic power use. By removing loop control and loop test instructions, loop unwinding speeds up the design process. It improves the effectiveness of the programme. It lowers the overhead of the loop.

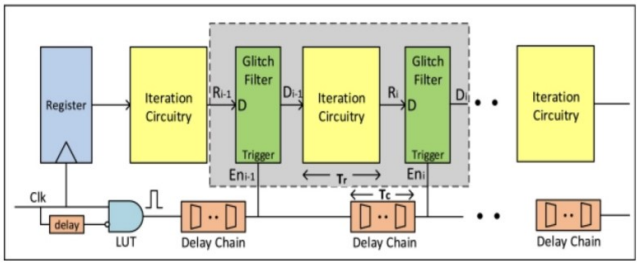

Fig 2: Loop Unwinding algorithm

IV. RESULT AND DISCUSSION

The Hardware Description Language (HDL) Verilog was used to code the AES algorithm, and the Xilinx VIVADO 2019.2 tool was used to simulate it. The tool's simulation output is shown in Fig. 3. The AES technique, shown in Fig. 3, is used to determine the cypher key when the clock is on the positive edge and the reset is zero. The cypher key is then encrypted using Sbox and shown in the load pin when it happens. Figure 3 shows an AES circuit that is free of trojans as a result of changing the other benchmark AES circuits. Xilinx VIVADO 2019 was used to synthesise the AES algorithm for FPGA implementation for AES-T100, AES-T200, and AES-T300.There are two tools in figs. 4, 5, and 6.

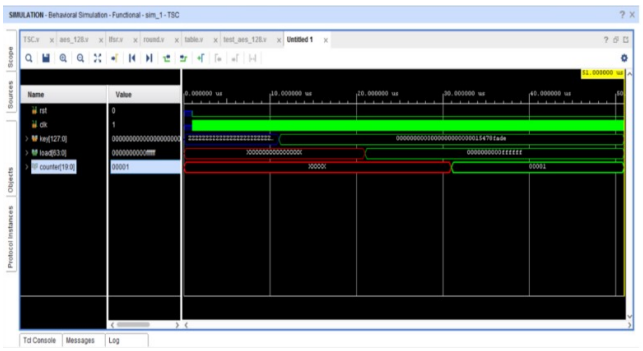

Fig 3: stimulated output of AES algorithm

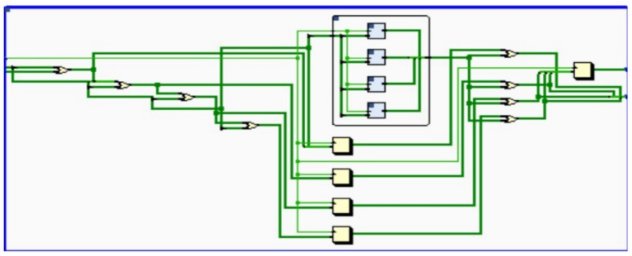

Fig 4: AES-T100 circuit

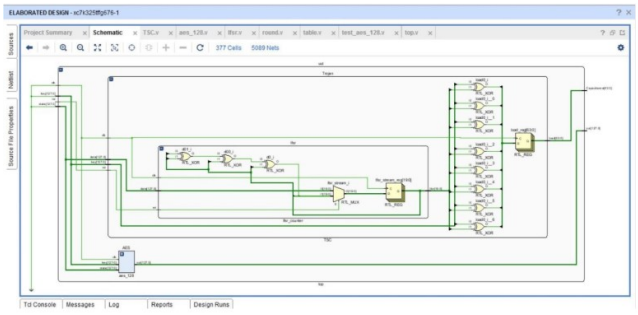

Fig 5: AES-T200 circuit

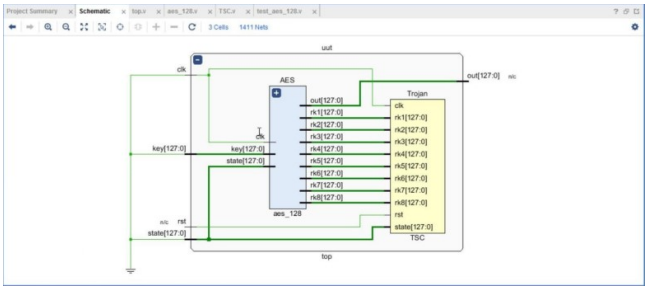

Fig 6: AES-T300 circuit

When performing RTL analysis, hardware trojans are detected 100% of the time (with 99% confidence and 1% mistake rate) of the incorrect attack that allowed the attacker to obtain information. The size and dynamic power analysis of the AES Trojan delayed and impacted circuits are displayed in Table 2.

BENCHMARKS	AREA(μm^2)	AREA*	POWER[1]	POWER*(mW)
AES-T100	636.828	630.815	185.0515	192.522
AES-T200	655.548	648.295	185.1306	190.1562
AES-T300	379.280	360.598	184.5204	187.1296

Table 2: Area and power analysis

According to Table 2, the average area decreases by 2.6% while maintaining a fair power usage. With regard to the FF and registers, the loop unwinding approach reduces the iterations of the AES algorithm, and the unused FF and registers are thus employed as trojan circuit delays, which increase power consumption.

V. CONCLUSION

The research paper compared the 128 bit encryption and decryption FPGA implementations of the Advanced Encryption Algorithm. Power analysis has allowed for its observation. Static and leaky power dissipation are greatly outweighed by dynamic power usage. The CPU is the target of the Trojan assault. It recognises both flaw-based and Trojan-activated assaults. 100% (99% confidence and 1% error) of the inappropriate attack that allowed the attacker to access information has been detected. This conclusion is derived from the finding that the AES algorithm's input/output requirements, even for 128 bit encryption, It has been proven that use the area and dynamic power consumption criteria to forecast or discover Trojans in a circuit is quite challenging. It has been shown that the area and dynamic power consumption criteria are met. There is a 2.9% reduction in average area and a 3.5% rise in average power. In the future, the AES algorithm's security will be improved by working with various benchmarks.

REFERENCES

[1] Bhasin, Francesco Regazzoni, and Shivam. "A survey on hardware trojan detection techniques." The International Conference on Circuits and Systems (ISCAS) 2015, IEEE. 2015 IEEE.
[2] Cho, Mingi, et al "Towards bidirectional LUT -level detection of hardware Trojans," Security & Computers 104 (2021): 102223
[3] Cruz, Jonathan, et al. "Automatic Hardware Trojan Insertion using Machine Learning." arXiv preprint arXiv:2204.08580 (2022).
[4] Dhanalakshmi, K. S., and R. Anusha Padmavathi. "A Survey on VLSI Implementation of AES Algorithm with Dynamic S-Box." Journal of Applied Security Research 17.2 (2022): 241-25
[5] Ganbaatar, Ganbat, and colleagues "Implementation of RSA cryptographic algorithm using SN P systems based on HP/LP neurons", Membrane Computing Journal 3.1 (2021): 22–34.
[6] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.
[7] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[8] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[9] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical &Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
[10] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.
[11] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.
[12] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756
[13] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749
[14] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
[15] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
[16] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019
[17] Hu, Wei, et al. "Detecting hardware trojans with gate level information-flow tracking. Computer 49.8 (2016): 44–52.
[18] Imam, Raza, and colleagues, "Systematic and critical review of rsa based public key cryptographic schemes: Past and present status." IEEE Access (2021).
[19] Jayant Rohankar, Mukul Pande, Kaluse, and Miss Dipali. "A Review on IOT Based Irrigation System by Using AES Algorithm." (2021).
[20] Khalid, Faiq, Khalid, et al. "Runtime hardware Trojan monitors through modelling burst mode communication using formal verification." 2018; Integration 61: 62–76.

[21] Taifeng, Hu, et al. "Equipment Horse Identification incorporates with Artificial Learning: an Isolated Forestbased Detection Method." The 14th worldwide symposium on Big Data Sciences and Engineering (BigDataSE) of the IEEE in 2020. IEEE, 2020.