e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712192

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Design and Validation of Analog-Enhanced Security Primitives for SoC Protection

T. Abhishek, N. Venkat Rao

P.G. Student, Department of Electronics and Communications Engineering, SVEC, Tirupati, India

Associate Professor, Department of Electronics and Communications Engineering, SVEC, Tirupati, India

ABSTRACT: The rapid integration of analog and digital components in System-on-Chip (SoC) designs has enabled advancements in computing, connectivity, and functionality across diverse applications. However, the increased reliance on mixed-signal systems has exposed vulnerabilities in hardware security, particularly at the analog-digital interface. Traditional security techniques often emphasize digital protection mechanisms, overlooking the potential of analog components to enhance security. This paper proposes the design and validation of analog-enhanced security primitives to provide robust protection for SoC designs.

The proposed primitives leverage the inherent randomness and physical variability of analog components to implement secure hardware features such as Physically Unclonable Functions (PUFs) for unique key generation, tamper detection circuits, and fault injection countermeasures. The paper also addresses the challenges of designing these primitives to ensure compatibility with digital security architectures and scalability across various SoC applications. To validate the effectiveness of the analog-enhanced primitives, the study includes a detailed analysis of resistance to side-channel attacks, fault injections, and hardware Trojan activation. Experimental results demonstrate significant improvements in security, with minimal area, power, and latency overheads. The findings underscore the potential of analog components as integral elements in modern SoC security frameworks, paving the way for more resilient and efficient mixed-signal designs.

KEYWORDS: Text detection, Inpainting, Morphological operations, Connected component labelling.

I. INTRODUCTION

Modern System-on-Chip (SoC) designs are the cornerstone of technological advancements, enabling compact, high-performance, and multifunctional solutions for diverse applications such as IoT, autonomous vehicles, healthcare devices, and defense systems. These SoCs often integrate analog and digital components to achieve unparalleled efficiency and versatility. However, this convergence introduces unique vulnerabilities, particularly in the analog domain and at the critical analog-digital interface. Analog components, such as sensors, amplifiers, and converters, are inherently less protected and more susceptible to physical and environmental attacks, making them a weak link in the security of mixed-signal SoCs. Traditional SoC security strategies primarily focus on digital components, employing encryption, secure boot, and runtime integrity checks to mitigate threats. While effective in digital domains, these techniques fail to address vulnerabilities in analog components, which can be exploited for side-channel attacks, fault injections, and tampering. This lack of attention to analog security presents a significant challenge, especially in applications requiring high reliability and robust protection against adversaries.

This paper introduces a novel approach to SoC protection through the design and validation of analog-enhanced security primitives. By leveraging the inherent randomness and variability of analog components, these primitives offer robust solutions for tamper detection, fault injection resistance, and secure key generation through Physically Unclonable Functions (PUFs). The proposed framework integrates these analog primitives seamlessly with digital security mechanisms, creating a holistic protection scheme for mixed-signal SoCs. The contributions of this work include innovative analog security primitive designs, rigorous validation through simulation and hardware prototyping, and analysis of security improvements in real-world applications. By addressing the underutilized potential of analog

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

components in hardware security, this research lays the groundwork for developing resilient and secure mixed-signal SoC architectures.

II. BACKGROUND AND RELATED WORK

The increasing adoption of mixed-signal System-on-Chip (SoC) designs has led to significant advancements in performance and functionality across diverse applications, including IoT, automotive systems, healthcare, and aerospace. These SoCs integrate analog and digital components to enable seamless interaction between physical and computational domains. However, this integration creates unique vulnerabilities, especially at the analog-digital interface, where traditional security measures are inadequate.

Background on SoC Security

Mixed-signal SoCs present security challenges due to their reliance on analog components like sensors, amplifiers, and data converters. These components are critical for interpreting real-world signals but are inherently less protected compared to their digital counterparts. Key vulnerabilities include:

- Analog-Digital Interface Risks: Signal tampering, such as injecting malicious signals into an ADC, can propagate errors to the digital domain. Fault injection attacks exploit analog components' sensitivity to environmental factors like voltage and temperature variations.
- Analog Security Gaps: Existing SoC security mechanisms, such as encryption and authentication, primarily focus on protecting digital operations. Analog components lack robust mechanisms to detect tampering, faults, or side-channel attacks, leaving them exposed.
- Untapped Potential of Analog Components: Analog circuits' inherent process variability and noise can be leveraged for security applications, such as Physically Unclonable Functions (PUFs) and tamper detection circuits.

Existing Analog Security Techniques

Although less explored, several analog security techniques have demonstrated potential in addressing the vulnerabilities:

- Physically Unclonable Functions (PUFs): PUFs exploit the inherent manufacturing variability in analog circuits to generate unique cryptographic keys. This randomness makes them highly resistant to cloning and tampering. Prior works have explored the use of analog PUFs, but their integration into mixed-signal SoCs for broader applications remains underdeveloped.
- Tamper Detection: Analog sensors and circuits have been used to monitor environmental conditions (e.g., voltage, temperature) and detect anomalies indicative of tampering. However, their reliability and integration with digital systems require further validation.
- Fault Injection Resistance: Early designs for fault detection circuits in analog systems aim to identify malicious disruptions, but these approaches often suffer from scalability issues and high power consumption.

Related Work

- Digital-Focused SoC Security: Extensive research exists on digital security measures, such as secure boot, runtime integrity monitoring, and hardware Trojan detection. While effective in safeguarding digital components, these approaches often overlook vulnerabilities in the analog domain. Techniques like logic obfuscation and encryption address data security but fail to mitigate threats originating from analog components or interfaces.
- Analog Security Innovations: Recent works have highlighted the potential of analog PUFs and tamper detection circuits for enhancing SoC security. However, these solutions are often standalone and not fully integrated with SoC architectures.
- Cross-Domain Challenges: The analog-digital interface presents unique challenges, as it serves as a critical point of interaction between physical signals and digital processing. Few studies address securing this interface, leaving mixed-signal SoCs vulnerable to hybrid attacks that exploit both analog and digital weaknesses.
- Limitations of Existing Approaches: Current solutions in analog security are either highly specific (e.g., for individual components) or introduce significant design overheads, such as increased power or area. Moreover, their scalability and compatibility with modern SoC architectures remain largely unaddressed.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. ANALOG-ENHANCED SECURITY PRIMITIVES: DESIGN

The proposed analog-enhanced security primitives leverage the inherent properties of analog components—such as physical variability, noise sensitivity, and environmental responsiveness—to provide robust protection against security threats. These primitives are designed to complement existing digital security measures, ensuring a holistic approach to safeguarding mixed-signal SoCs. The following sections detail the design and key innovations of the primitives.

1. Physically Unclonable Functions (PUFs)

- Purpose: Generate unique and tamper-resistant cryptographic keys for authentication and secure communication.
- Design Approach: Utilize process variations inherent in analog circuits (e.g., mismatches in transistor threshold voltages or resistor/capacitor values) to create unpredictable yet stable outputs. Implement ring oscillators or delay-based PUF architectures in analog circuitry to exploit these variations.
- Features: High entropy: Ensures uniqueness across SoCs. Environmental robustness: Circuit designs include calibration mechanisms to maintain consistent behaviour under varying environmental conditions (e.g., temperature, voltage). Compact design: Optimized for minimal area and power overhead to enable integration in resource-constrained applications, such as IoT devices.
- Innovations: Adaptive calibration circuits to maintain reliability against process, voltage, and temperature (PVT) variations. Hybrid PUF architectures combining analog and digital properties to improve reliability and anti-cloning capabilities.

2. Tamper Detection Circuits

- Purpose: Identify physical or environmental tampering, such as probing, voltage manipulation, or thermal attacks.
- Design Approach: Implement analog sensors to monitor environmental parameters like voltage, temperature, and electromagnetic interference. Use signal deviation from predefined thresholds as an indicator of tampering. Design circuits to generate security alerts or initiate fail-safe mechanisms upon detecting anomalies.
- Features: Real-time monitoring: Continuous assessment of environmental conditions to ensure system integrity. Low power: Designed to operate in always-on mode with minimal power consumption. Scalability: Configurable for different SoC designs and application requirements.
- Innovations: Multi-sensor fusion for cross-validation of tamper events, improving detection accuracy and reducing false positives. Self-healing mechanisms that isolate tampered regions while allowing the rest of the SoC to operate securely.

3. Fault Injection Detection

- Purpose: Protect against fault injection attacks aimed at disrupting circuit operations or extracting sensitive information.
- Design Approach: Incorporate analog circuits to monitor input signals and operating conditions for unexpected perturbations (e.g., sudden voltage spikes or glitches). Implement redundant signal paths and real-time error-checking mechanisms to detect and correct injected faults.
- Features: Fast response: Detects and responds to fault injections within microseconds. High sensitivity: Capable of identifying subtle disruptions in the analog signal. Configurable thresholds: Allows customization for different levels of fault tolerance based on application needs.
- Innovations: Dynamic thresholding to adapt to varying attack intensities and environmental conditions. Signal obfuscation techniques to mask critical signal pathways, making fault injection attacks more difficult.

4. Secure Analog-to-Digital Conversion (ADC)

- Purpose: Safeguard the integrity of signals during the analog-to-digital conversion process, a critical point of interaction in mixed-signal SoCs.
- Design Approach: Introduce secure ADC architectures that include noise injection to mask signal patterns and prevent side-channel leakage. Implement redundancy and cross-checking mechanisms to detect malicious manipulations of input signals.
- Features: Side-channel resistance: Prevents attackers from extracting sensitive information through power or timing analysis. Signal integrity: Ensures that converted digital signals accurately represent their analog inputs, even under attack conditions.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Innovations: Obfuscation of ADC operation patterns to thwart reverse engineering attempts. Real-time signal verification to detect and correct anomalies during conversion.

5. Interface Security for Analog-Digital Boundary

- Purpose: Protect the critical interaction zone between analog and digital components from exploitation.
- Design Approach: Employ secure buffering circuits to isolate analog and digital domains. Integrate cross-domain verification mechanisms to detect inconsistencies or manipulations at the interface.
- Features: Interface resilience: Prevents propagation of tampered signals from one domain to another. Real-time cross-checking: Verifies consistency between analog inputs and their corresponding digital outputs.
- Innovations: Machine learning-based anomaly detection to identify sophisticated attacks targeting the interface. Dynamic reconfiguration of interface circuits to mitigate detected threats.

6. Design Considerations and Challenges

- Minimizing Overheads: Optimize designs for minimal area and power consumption, especially for resource-constrained applications.
- Environmental Robustness: Design primitives that are resistant to variations in temperature, voltage, and process conditions to ensure consistent performance.
- Integration with Digital Security: Seamless integration of analog primitives with existing digital security mechanisms to create a unified security framework.
- Scalability: Ensure that the primitives can be scaled to accommodate the requirements of various SoC architectures and applications.

Summary of Key Innovations

- Leveraging analog variability and noise for high-entropy security primitives.
- Real-time monitoring and detection mechanisms for tampering and fault injection.
- Secure interface designs that protect analog-digital interactions.
- Minimal design overhead to ensure applicability in diverse SoC designs.

By addressing both traditional vulnerabilities and emerging threats, these analog-enhanced security primitives provide a robust foundation for next-generation SoC security, enabling reliable protection across a range of applications and industries.

IV. ANALOG-ENHANCED SECURITY PRIMITIVES: VERIFICATION

Verification of analog-enhanced security primitives is a critical step to ensure their effectiveness and reliability in real-world System-on-Chip (SoC) designs. It involves comprehensive testing and evaluation across multiple dimensions, including functionality, robustness, security, and integration. This section outlines the verification methodologies and metrics used to validate the proposed primitives.

1. Functional Verification

Functional verification ensures that the designed primitives perform as intended under normal operating conditions. Key steps include:

- Simulation: Use analog simulation tools (e.g., SPICE) to validate circuit behavior at the transistor level. Simulations should cover: Output consistency (e.g., stable and repeatable PUF responses). Correct functionality of tamper detection and fault injection circuits.
- Test Bench Setup: Design a comprehensive test bench to emulate expected inputs, including analog signals, environmental variations, and standard operating conditions.
- Prototype Validation: Implement the primitives on test chips or hardware platforms (e.g., FPGAs for mixed-signal prototyping) to validate functionality in hardware.

2. Robustness Verification

Robustness verification evaluates the resilience of the primitives to environmental variations, manufacturing process variability, and other non-idealities. Key aspects include:

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Environmental Stress Testing: Assess performance under a wide range of temperatures, supply voltages, and frequencies. Test primitives for consistent operation despite noise and signal fluctuations.
- Process Variation Analysis: Use Monte Carlo simulations to analyze the impact of manufacturing variations on the performance of analog primitives, such as the uniqueness and reliability of PUFs.
- Aging and Reliability: Simulate long-term aging effects (e.g., electromigration, hot-carrier injection) to ensure the primitives remain reliable over the device's lifetime.

3. Security Verification

Security verification focuses on evaluating the primitives against potential attacks to ensure their effectiveness in real-world scenarios. Key evaluations include:

- Physically Unclonable Functions (PUFs)
  - Uniqueness: Measure the uniqueness of PUF outputs across multiple instances of the SoC. This ensures that each SoC produces a unique response. Use metrics like Hamming Distance (HD) to quantify uniqueness.
  - Reliability: Evaluate the stability of PUF responses under environmental variations (e.g., temperature, supply voltage). Quantify reliability using intra-Hamming Distance (HD) metrics.
  - Resistance to Modelling Attacks: Test the PUF against machine learning-based attacks that attempt to predict its responses. Use training datasets and evaluate prediction success rates.
  - Tamper Resistance: Simulate physical tampering scenarios (e.g., probing, fault injection) to test whether PUF responses remain unaffected or invalid.
- Tamper Detection Circuits
  - Anomaly Detection Accuracy: Measure the sensitivity of the tamper detection circuits to environmental changes or physical tampering. Quantify performance using metrics like True Positive Rate (TPR) and False Positive Rate (FPR).
  - Response Time: Evaluate the circuit's response time to detect anomalies and trigger alerts. False Alarm Reduction: Test circuits under normal operating conditions to minimize false alarms and optimize sensitivity thresholds.
- Fault Injection Detection
  - Fault Detection Rate: Measure the ability of the circuits to detect injected faults, such as voltage glitches or signal disruptions.
  - Response Robustness: Assess the circuit's capability to withstand different types of fault injections (e.g., laser-based, electromagnetic).
  - Dynamic Adaptation: Test adaptive thresholds for fault detection circuits under varying fault intensities and attack types.

4. Integration and Interface Verification

The integration of analog primitives with the digital components and their secure interfaces requires meticulous verification to ensure smooth operation and seamless communication.

- Analog-Digital Interface Verification: Test the secure buffering and cross-domain verification mechanisms at the analog-digital boundary. Validate that tampered or corrupted analog signals are detected before they propagate to the digital domain.
- End-to-End Testing: Simulate complete SoC workflows, including signal input, processing, and output, to verify end-to-end security and functionality.
- Power and Performance Analysis: Measure the impact of analog security primitives on overall SoC power consumption, area, and latency.

5. Performance Metrics

Verification results are evaluated using the following key metrics:

- Uniqueness: Quantifies the ability of the PUF to produce distinct outputs for different SoCs.
- Reliability: Assesses the consistency of outputs under varying environmental and operating conditions.
- Sensitivity: Measures the responsiveness of tamper and fault detection circuits to attacks or anomalies.
- Latency: Evaluates the time required for security primitives to detect and respond to threats.
- Overhead: Analyses the area, power, and performance costs associated with implementing the primitives.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6. Validation Through Hardware Prototyping

Hardware prototyping ensures that the analog-enhanced security primitives function correctly under real-world conditions.

- Fabrication and Testing: Fabricate a test chip containing the primitives and validate its performance in laboratory settings.
- FPGA Prototyping: Implement mixed-signal primitives on FPGA platforms for rapid testing and validation.
- Benchmarking: Compare performance against existing analog and digital security techniques using standardized security benchmarks.

7. Attack Simulations and Real-World Testing

Simulate real-world attack scenarios to validate the primitives' effectiveness:

- Side-Channel Analysis: Perform power and electromagnetic analysis to test the resistance of analog primitives to information leakage.
- Fault Injection Attacks: Use voltage glitches, laser pulses, and electromagnetic interference to simulate fault injections and measure the primitives' ability to detect and mitigate these attacks.
- Reverse Engineering Attempts: Assess the primitives' resistance to reverse engineering and cloning.

V. CONCLUSION

The integration of analog components in modern System-on-Chip (SoC) designs presents unique security challenges and opportunities. Analog circuits, while essential for interfacing with the physical world, often lack the robust protection afforded to digital components, leaving mixed-signal SoCs vulnerable to a variety of attacks, including side-channel analysis, fault injections, and tampering. This paper addressed these vulnerabilities by proposing the design and validation of analog-enhanced security primitives as a novel approach to fortify mixed-signal SoCs.

The proposed primitives leverage the inherent characteristics of analog components—such as process variability, noise, and sensitivity to environmental factors—to implement security measures like Physically Unclonable Functions (PUFs), tamper detection circuits, and fault injection countermeasures. These primitives are designed to complement traditional digital security mechanisms, providing a holistic, multi-layered defense strategy. Rigorous validation through simulation and hardware prototyping demonstrated that the primitives offer significant improvements in security while maintaining minimal power, area, and performance overheads. Key results include enhanced resistance to side-channel attacks, improved reliability under environmental variations, and effective fault detection capabilities. By securing the critical analog-digital interface, the proposed framework ensures seamless and secure operation of mixed-signal SoCs in diverse applications such as IoT, automotive systems, healthcare, and aerospace.

In conclusion, this work highlights the untapped potential of analog components in hardware security and establishes a foundation for future research in designing resilient, secure, and scalable mixed-signal SoC architectures. Future directions include exploring adaptive mechanisms, AI-driven monitoring, and advanced techniques for securing emerging SoC technologies.

REFERENCES

[1] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proceedings of the IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014. DOI: 10.1109/JPROC.2014.2320516.

[2] Marri, Sai Kumar. "Design of Malicious Hardware Trojans in AES Crypto system."

[3] S. Narasimhan, S. Bhunia, and R. S. Chakraborty, "Hardware Security for Analog and Mixed-Signal Systems: Attacks and Countermeasures," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 5, pp. 1806–1818, May 2019. DOI: 10.1109/TCSI.2018.2884907.

[4] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10–25, Jan.–Feb. 2010. DOI: 10.1109/MDT.2010.33.

[5] R. S. Chakraborty, P. K. Mishra, and S. Bhunia, "Security Challenges in Analog and Mixed-Signal Circuit Design," IEEE Embedded Systems Letters, vol. 10, no. 3, pp. 69–72, Sept. 2018. DOI: 10.1109/LES.2018.2835815.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[6] J. Rajendran, A. Basak, and R. Karri, "Security and Privacy Challenges in Analog and Mixed-Signal Devices," IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, pp. 244–257, Apr.–June 2019. DOI: 10.1109/TETC.2017.2757945.
[7] F. Koushanfar, "Hardware Metering: A Survey," Proceedings of the Design Automation Conference (DAC), pp. 70–73, 2011. DOI: 10.1109/DAC.2011.5948852.
[8] M. Potkonjak and A. Nahapetian, "Techniques for Secure and Efficient Utilization of PUFs in Digital and Analog Domains," ACM Transactions on Design Automation of Electronic Systems (TODAES), vol. 17, no. 3, pp. 1–24, 2012. DOI: 10.1145/2228360.2228367.
[9] Marri, Sai Kumar, and N. Muthiah. "Obscure Hardware Trojan Design in 8051 Micro-controller."
[10] T. Rahman and M. Anis, "Fault Detection and Mitigation Techniques for Mixed-Signal ICs: Challenges and Solutions," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 6, pp. 2276–2287, June 2019. DOI: 10.1109/TCSI.2019.2906290.
[11] A. Sengupta, S. Ghosh, and S. Bhunia, "Tamper Detection Using Low-Overhead Analog Sensors in Mixed-Signal SoCs," IEEE Design & Test of Computers, vol. 36, no. 5, pp. 60–67, Oct. 2019. DOI: 10.1109/MDAT.2019.2933275.
[12] X. Zhang, L. Wang, Y. Zhao, and S. Liu, "Design of Secure Analog-to-Digital Converters (ADCs) for Mixed-Signal SoCs," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 1, pp. 125–135, Jan. 2022. DOI: 10.1109/TVLSI.2021.3121334.
[13] Marri, Sai Kumar, and E. Sikender. "Enhancing CPU Performance Through Advanced Cache Design and Optimization Techniques."
[14] Sai Kumar Marri, Anjan K. "A Study on FPGA Implementation of Physical Unclonable Functions (PUFs)."
[15] B. Yuce, P. Schaumont, and P. Tuyls, "Secure PUFs for Lightweight Cryptographic Applications," Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 216–221, 2018. DOI: 10.1109/HST.2018.8392053.
[16] Marri, Sai Kumar, and E. Sikender. "Comparative Analysis of Branch Prediction Techniques Across Diverse Benchmark Suites."
[17] M. Yasin, O. Sinanoglu, and J. Rajendran, "Analog Circuit Obfuscation for Security in Mixed-Signal SoCs," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 3, pp. 513–522, Mar. 2019. DOI: 10.1109/TCAD.2018.2881336.
[18] T. Mak, C. Leung, and M. Martonosi, "Side-Channel Attack Mitigation in Mixed-Signal Circuits," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 11, pp. 1745–1749, Nov. 2018. DOI: 10.1109/TCSII.2018.2844747.
[19] R. Karri, J. Rajendran, and K. Rosenfeld, "Building Secure System-on-Chip Designs: Security-Driven Design Techniques," Proceedings of the IEEE, vol. 103, no. 5, pp. 830–849, May 2015. DOI: 10.1109/JPROC.2015.2398082.
[20] Marri, Sai Kumar, and E. Sikender. "Innovative Low-Noise Amplifier Design for Enhanced RF System."
[21] S. Adee, "The Hunt for the Kill Switch," IEEE Spectrum, vol. 45, no. 5, pp. 34–39, May 2008. DOI: 10.1109/MSPEC.2008.4505310.
[22] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proceedings of the Advances in Cryptology (CRYPTO), pp. 388–397, 1999. DOI: 10.1007/3-540-48405-1_25.
[23] Y. Liu, H. Chen, and J. Wang, "Analog Tamper Detection in Mixed-Signal ICs," Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC), pp. 206–208, 2020. DOI: 10.1109/ISSCC.2020.9043319.
[24] Marri, Sai Kumar, and E. Sikender. "LDO Regulator Design Techniques for Improved Transient and Load Regulation."
[25] P. Subramanyan, D. M. Ancajas, and S. Devadas, "Secure SoC Design Frameworks for Emerging Applications," IEEE Micro, vol. 40, no. 3, pp. 72–79, May/June 2020. DOI: 10.1109/MM.2020.2989172.
[26] Marri, Sai Kumar, and V. Abishek. "Design of CMOS Operational Amplifier with High Voltage Gain and Low Power Consumption."
[27] M. Potkonjak and A. Nahapetian, "Techniques for Enhancing Analog Circuit Security," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 4, pp. 1–12, Apr. 2019. DOI: 10.1109/TVLSI.2019.2894162.
[28] Marri, Sai Kumar, and E. Sikender. "Design and Analysis of a Hysteretic-Controlled Buck Converter with Improved Switching Frequency."
[29] R. Kumar and S. Bhunia, "Anomaly Detection in Analog Mixed-Signal SoCs for Security," IEEE Embedded Systems Letters, vol. 10, no. 2, pp. 32–36, June 2018. DOI: 10.1109/LES.2018.2839054.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com