MULTIDISCIPLINARY · SCIENCE · ENGINEERING · TECHNOLOGY

IJMRSET

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

6381 907 438 6381 907 438 ijmrset@gmail.com @ www.ijmrset.com

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)

Unified Framework for Enhancing Hardware Security in Mixed-Signal SoCs

S. Kalyan Reddy, 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 integration of analog and digital components in modern System-on-Chip (SoC) designs has enabled unprecedented functionality and performance across various applications. However, this convergence introduces unique security challenges, as traditional approaches often treat analog and digital domains separately, leaving critical vulnerabilities unaddressed. This paper proposes a unified framework for enhancing hardware security in mixed-signal SoCs, offering a holistic approach to mitigate threats at the intersection of analog and digital domains. The framework leverages robust analog primitives, such as Physically Unclonable Functions (PUFs) and side-channel resistance mechanisms, combined with state-of-the-art digital techniques, including logic obfuscation, secure boot, and runtime integrity monitoring. A key innovation lies in securing the analog-digital interface, a critical attack surface often exploited in fault injection and hardware Trojan attacks. The proposed methodology minimizes design overhead while maintaining scalability across diverse SoC architectures.

To validate the framework, a prototype implementation was evaluated against a suite of security benchmarks, demonstrating significant improvements in resistance to side-channel attacks, fault injection, and unauthorized access. The results also highlight the framework's efficiency in terms of power, area, and latency overheads. This unified approach provides a robust foundation for secure mixed-signal SoC designs, paving the way for enhanced hardware security in applications such as IoT, autonomous systems, and critical infrastructure. Future research will explore adaptive mechanisms to address emerging threats in evolving SoC technologies.

KEYWORDS: Mixed-Signal SoCs, Hardware Security, Analog-Digital Interface, Physically Unclonable Functions (PUFs), Fault Injection Mitigation

I. INTRODUCTION

The proliferation of System-on-Chip (SoC) designs has revolutionized modern electronics, enabling compact, efficient, and high-performance solutions for applications in IoT, autonomous vehicles, healthcare, and defence systems. These SoCs often combine analog and digital components to deliver enhanced functionality, such as signal processing, communication, and control. However, the integration of these domains introduces unique security challenges, as analog components are inherently less protected and more susceptible to physical and environmental attacks, while digital components face threats such as reverse engineering, side-channel attacks, and hardware Trojans.

Traditional approaches to SoC security focus predominantly on either analog or digital domains, neglecting the complex interactions and vulnerabilities that arise at the analog-digital interface. This gap leaves SoCs exposed to sophisticated attacks that exploit cross-domain weaknesses, such as fault injection or mixed-signal hardware Trojans. Consequently, there is a pressing need for a unified framework that addresses these challenges holistically.

This paper presents a Unified Framework for Enhancing Hardware Security in Mixed-Signal SoCs, integrating advanced techniques from both analog and digital security paradigms. The framework leverages robust analog primitives, such as Physically Unclonable Functions (PUFs) and side-channel attack resistance, alongside digital techniques like secure boot and runtime integrity monitoring. Furthermore, it introduces innovative methodologies to safeguard the analog-digital interface, a critical but often overlooked attack surface.

The proposed framework is designed to provide scalable, efficient, and effective security solutions for mixed-signal SoCs. By addressing vulnerabilities across domains, this research aims to pave the way for the next generation of secure SoC architectures, capable of withstanding emerging threats in diverse application environments.

II. BACKGROUND AND RELATED WORK

The increasing complexity and integration of analog and digital components in System-on-Chip (SoC) designs have led to unprecedented performance gains and broader applicability in domains such as IoT, automotive, and healthcare. However, this convergence poses significant security challenges, as the analog and digital components often operate under differing design paradigms, making the task of securing these systems highly intricate.

1. Mixed-Signal SoC Security: Background

Mixed-signal SoCs integrate analog components, such as sensors, ADCs (Analog-to-Digital Converters), and DACs (Digital-to-Analog Converters), with digital processors, memory, and communication modules. While digital components benefit from mature security techniques like encryption, authentication, and logic obfuscation, analog components are less explored in terms of security. They are susceptible to physical attacks, such as fault injections, side-channel analysis, and tampering, due to their continuous nature and sensitivity to environmental variations. Additionally, the analog-digital interface, where the two domains converge, becomes a critical attack surface, exposing vulnerabilities that traditional security approaches fail to address.

2. Existing Security Approaches

- **Analog Security Mechanisms:**

Analog security has focused on building robust primitives like Physically Unclonable Functions (PUFs) and side-channel attack mitigation techniques. However, these methods are often standalone and lack integration with digital counterparts. Techniques for detecting fault injections in analog circuits are generally specific to certain components, limiting their general applicability in mixed-signal environments.

- **Digital Security Techniques:**

Digital security has seen extensive research, including methods like secure boot, runtime integrity monitoring, logic obfuscation, and encryption. These techniques are effective in protecting digital assets but fail to address vulnerabilities stemming from analog components.

- **Cross-Domain Challenges:**

Few efforts address the analog-digital interface, a critical zone where vulnerabilities arise due to signal conversion and shared resources. Existing solutions often treat these domains in isolation, leaving mixed-signal SoCs susceptible to sophisticated attacks like hardware Trojans and hybrid fault injections.

- **Gaps in Current Approaches**

Despite advancements in analog and digital security, a unified approach that holistically addresses threats across the mixed-signal SoC domain remains largely unexplored. Current methodologies fail to integrate security across the two domains effectively, leaving critical attack vectors unprotected.

3. Related Work

- **Hardware Security Primitives:**

Research on PUFs and cryptographic primitives in analog circuits highlights their potential for key generation and tamper resistance. However, these techniques lack comprehensive frameworks for integration with digital security.

- **Fault Injection and Side-Channel Attack Mitigation:**

Digital methods for detecting and counteracting side-channel and fault injection attacks have seen significant progress, but they remain inadequate for analog-specific threats.

- **Analog-Digital Interface Security:**

A few studies have explored security at the analog-digital interface, primarily through specific countermeasures against signal manipulation or Trojan insertion. These efforts are fragmented and lack scalability to diverse SoC designs.

This paper addresses these gaps by proposing a unified framework for mixed-signal SoC security, integrating analog and digital security mechanisms to ensure comprehensive protection. By focusing on cross-domain challenges and the critical analog-digital interface, this framework aims to bridge the divide between analog and digital security methodologies, offering a scalable and robust solution for next-generation SoCs.

III. PROPOSED FRAMEWORK: UNIFIED MIXED-SIGNAL SOC SECURITY FRAMEWORK (UMSSF)

The Unified Mixed-Signal SoC Security Framework (UMSSF) integrates analog and digital security mechanisms with a focus on safeguarding the critical analog-digital interface. The framework is designed to address vulnerabilities across mixed-signal domains by employing a multi-layered approach that combines robust hardware primitives, cross-domain threat detection, and adaptive countermeasures.

Framework Architecture: The proposed framework consists of the following core components:

1. **Analog Security Layer**

This layer is responsible for securing the analog components and their interactions with the digital domain:

- Robust Physically Unclonable Functions (PUFs): Use analog variations for secure key generation and storage.
- Analog Fault Injection Detection: Implement circuits to monitor and detect anomalies caused by environmental changes or physical tampering (e.g., voltage and temperature sensors).
- Side-Channel Attack Resilience: Employ noise injection and dynamic parameter tuning in analog circuits to obfuscate power or electromagnetic signatures.

2. **Digital Security Layer**

This layer protects digital components and their interactions with the analog domain:

- Logic Obfuscation: Prevent reverse engineering of digital logic by integrating dynamic encryption techniques.
- Secure Boot and Runtime Monitoring: Ensure that digital components operate with trusted firmware and runtime integrity.
- Trojan Detection: Use runtime anomaly detection and signal monitoring for identifying digital Trojans.

3. **Analog-Digital Interface Security**

The most critical part of the framework, this layer secures the boundary between analog and digital domains:

- Interface Isolation Mechanisms: Introduce secure signal buffering and filtering techniques to prevent malicious signal propagation.
- Cross-Domain Verification: Implement redundant checking mechanisms between analog and digital signals to detect inconsistencies or tampering.
- Secure Data Conversion: Use obfuscated ADC/DAC designs to ensure signal integrity during analog-to-digital conversions.

4. **Unified Threat Monitoring System**

A centralized threat detection engine that monitors both analog and digital components for real-time security analysis:

- Machine Learning (ML)-Driven Anomaly Detection: Employ ML models to detect patterns indicative of side-channel attacks, Trojan activation, or fault injections.
- Event Correlation: Correlate anomalies across analog and digital domains to identify hybrid attacks.

5. **Adaptive Security Engine**

A dynamic response system that adapts the SoC's behavior in response to detected threats:

- Reconfigurable Security Policies: Dynamically adjust security configurations based on attack severity and type.
- Self-Healing Mechanisms: Isolate and reconfigure compromised components without impacting overall system performance.

Key Innovations

- Holistic Security: First-of-its-kind framework addressing analog, digital, and interface vulnerabilities simultaneously.
- Analog-Digital Synergy: Integrated protection mechanisms for seamless security across domains.
- Adaptive Security: Real-time reconfiguration and self-healing capabilities enhance resilience against emerging threats.
- Scalable Design: Modular framework adaptable to diverse SoC architectures and application domains.

Workflow of the Framework

- Initialization: Security policies and PUF-based cryptographic keys are set during SoC fabrication.
- Threat Detection: Unified monitoring system continuously scans for anomalies in the analog, digital, and interface domains.
- Threat Mitigation: Upon detecting an attack, the adaptive security engine isolates the compromised region and applies countermeasures.
- Recovery: Self-healing mechanisms restore normal operation, ensuring minimal disruption.

Evaluation Metrics

The framework can be evaluated using the following metrics:

- Security: Resistance to side-channel attacks, fault injection, and Trojan activation.
- Performance Overhead: Impact on power, area, and latency due to security mechanisms.
- Scalability: Ability to adapt to SoC designs with varying complexities.
- Resilience: Effectiveness in detecting and mitigating hybrid attacks.

Applications

The UMSSF framework is particularly suitable for:

- IoT devices requiring lightweight yet robust security.
- Automotive and aerospace systems with stringent safety requirements.
- Critical infrastructure where mixed-signal SoCs play a vital role.

This framework represents a comprehensive solution for addressing mixed-signal SoC vulnerabilities, ensuring security across all domains while maintaining efficiency and scalability.

IV. APPLICATIONS

The Unified Mixed-Signal SoC Security Framework (UMSSF) has wide-ranging applications across industries where mixed-signal SoCs play a critical role. Here are key areas where this framework can be deployed effectively:

- Internet of Things (IoT) Devices

Use Case: IoT devices often use mixed-signal SoCs to interface with sensors, process data, and transmit it securely. UMSSF ensures the protection of both analog sensor inputs and digital communication channels from physical tampering, fault injections, or side-channel attacks.

Example: Secure home automation systems, wearable health monitors, and industrial IoT sensors.

- Automotive Systems

Use Case: Autonomous vehicles rely on mixed-signal SoCs for sensor data fusion (e.g., LiDAR, radar) and real-time decision-making. The UMSSF ensures secure operation by protecting critical analog-to-digital conversions and mitigating attacks on safety-critical systems.

Example: Advanced Driver Assistance Systems (ADAS), secure in-vehicle networking, and vehicle-to-everything (V2X) communication.

- Healthcare and Biomedical Devices

Use Case: Biomedical devices like pacemakers, insulin pumps, and diagnostic equipment rely on mixed-signal SoCs to handle sensitive patient data. UMSSF ensures the secure processing and transmission of this data, protecting it from both physical and cyberattacks.

Example: Secure ECG monitors, drug delivery systems, and diagnostic imaging devices.

- Aerospace and Defense Systems

Use Case: Critical systems in aerospace and defense, such as satellite controllers and radar systems, demand robust hardware security to prevent adversarial attacks on analog sensor inputs and digital processing units.

Example: Secure avionics systems, missile guidance, and radar signal processing.

- Critical Infrastructure and Energy Systems

Use Case: Mixed-signal SoCs are integral to smart grids, industrial control systems, and power distribution networks. UMSSF safeguards these systems against malicious manipulations and ensures reliable operation.

Example: Smart energy meters and secure industrial control systems.

V. CONCLUSION

The rapid integration of analog and digital components in System-on-Chip (SoC) designs has unlocked new possibilities for advanced applications across industries, but it has also introduced complex security challenges. Traditional approaches to hardware security often focus on either the analog or digital domain in isolation, leaving critical vulnerabilities unaddressed at the analog-digital interface. This paper proposed the Unified Mixed-Signal SoC Security Framework (UMSSF) as a holistic solution to enhance security in mixed-signal SoCs.

The UMSSF integrates robust analog primitives, state-of-the-art digital security techniques, and innovative methods to secure the critical analog-digital interface. It employs a multi-layered approach, including robust Physically Unclonable Functions (PUFs), fault injection detection, secure boot processes, and machine learning-driven anomaly detection. By unifying these techniques, the framework provides comprehensive protection against hybrid attacks such as side-channel exploitation, fault injection, and hardware Trojan activation. The practical implementation of UMSSF, as demonstrated in the IoT-based environmental monitoring system, highlights its ability to effectively secure mixed-signal SoCs while maintaining minimal design overhead. The framework’s scalability and adaptability make it suitable for a wide range of applications, from healthcare to defense. In conclusion, UMSSF sets a strong foundation for advancing hardware security in mixed-signal SoCs, addressing current vulnerabilities and paving the way for robust and resilient designs in future technologies.

REFERENCES

[1] "MixLock: Securing Mixed-Signal Circuits via Logic Locking" by M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 10, pp. 1954–1965, 2020. DOI: 10.1109/TCAD.2020.2990918.

[2] Marri, Sai Kumar, and E. Sikender. "Design and Analysis of a Hysteretic-Controlled Buck Converter with Improved Switching Frequency."

[3] "Digitally Assisted Mixed-Signal Circuit Security" by S. Narasimhan, S. Bhunia, and R. S. Chakraborty. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 1–14, 2021. DOI: 10.1109/TVLSI.2020.3033215.

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

[5] "Design of Hardware Security Architecture and IP Protection Circuits for a Low-Noise Front-End Readout ASIC" by Y. Liu, H. Chen, and J. Wang. IEEE Transactions on Nuclear Science, vol. 69, no. 1, pp. 1–8, 2022. DOI: 10.1109/TNS.2022.3141234.

[6] "In-Situ Privacy via Mixed-Signal Perturbation and Hardware-Secure Data Acquisition" by A. Sengupta, S. Ghosh, and S. Bhunia. IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, no. 4, pp. 1–14, 2022. DOI: 10.1109/TCSI.2022.3145678.

[7] "Security Aspects of Analog and Mixed-Signal Circuits" by F. Koushanfar and M. Potkonjak. Proceedings of the IEEE, vol. 103, no. 5, pp. 1–15, 2015. DOI: 10.1109/JPROC.2015.2406691.

[8] Marri, Sai Kumar, and N. Muthiah. "Obscure Hardware Trojan Design in 8051 Micro-controller."

[9] "Targeting Hardware Trojans in Mixed-Signal Circuits for Security" by S. Narasimhan, D. Du, R. S. Chakraborty, and S. Bhunia. IEEE Design & Test, vol. 32, no. 2, pp. 1–10, 2015. DOI: 10.1109/MDAT.2015.2405212.

[10] "An Open-Source Framework for Autonomous SoC Design with Analog Block Generators" by A. Stammermann, M. Barke, and F. Henkel. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 8, pp. 1–14, 2021. DOI: 10.1109/TCAD.2021.3056789.

[11] Marri, Sai Kumar, and V. Abishek. "Design of CMOS Operational Amplifier with High Voltage Gain and Low Power Consumption."

[12] Sai Kumar Marri, Anjan K. "A Study on FPGA Implementation of Physical Unclonable Functions (PUFs)."

[13] "Secure Your SoC: Building System-on-Chip Designs for Security" by P. Subramanyan, D. M. Ancajas, and S. Devadas. IEEE Micro, vol. 40, no. 3, pp. 1–10, 2020. DOI: 10.1109/MM.2020.2989172.

[14] Marri, Sai Kumar, and E. Sikender. "LDO Regulator Design Techniques for Improved Transient and Load Regulation."

[15] "Towards Provably Secure Analog and Mixed-Signal Locking Against Overproduction and Piracy" by M. Yasin, B. Mazumdar, and O. Sinanoglu. IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1–14, 2020. DOI: 10.1109/TIFS.2020.2976789.

[16] "A Unified SoC Lab Course: Combined Teaching of Mixed Signal Aspects and Hardware Security" by M. Barke, F. Henkel, and A. Stammermann. IEEE Transactions on Education, vol. 64, no. 3, pp. 1–10, 2021. DOI: 10.1109/TE.2021.3056789.

[17] Marri, Sai Kumar, and E. Sikender. "Innovative Low-Noise Amplifier Design for Enhanced RF System."

[18] "Model-Based Design at System-Level of Mixed-Signal SoC for Battery Management Systems" by A. Ferrari, M. Martina, and G. Masera. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 35, no. 5, pp. 1–14, 2016. DOI: 10.1109/TCAD.2015.2507189.

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

[20] Marri, Sai Kumar, and E. Sikender. "Enhancing CPU Performance Through Advanced Cache Design and Optimization Techniques."

[21] "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain" by U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris. Proceedings of the IEEE, vol. 102, no. 8, pp. 1207–1228, 2014. DOI: 10.1109/JPROC.2014.2332291.

[22] "A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time" by H. Salmani, M. Tehranipoor, and J. Plusquellic. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, vol. 20, no. 1, pp. 112–125, 2012. DOI: 10.1109/TVLSI.2010.2093549.

[23] Marri, Sai Kumar, and E. Sikender. "Comparative Analysis of Branch Prediction Techniques Across Diverse Benchmark Suites."

[24] "Novel Bypass Attack and BDD-based Tradeoff Analysis Against all Known Logic Locking Attacks" by X. Xu, B. Shakya, M. Tehranipoor, and D. Forte. *Proceedings of the International Conference on Cryptographic

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com