Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

SECURITY ANALYSIS AND EXPLOITATION OF IC CHIP LEVEL COUNTER QUANTITY AGAINST BODILY OCCURRENCES

SUMALATA KADIRE[1], V SAI ANJANI[2], P AKSHITHA[3], V RAMYA SRI[4]
ASSISTANT PROFESSOR 1, UG SCHOLAR 2,3,4
DEPARTMENT OF ECE, MALLA REDDY ENGINEERIGNG COLLEGE FOR WOMEN (UGC-AUTONOMOUS), MAISAMMGUDA, HYDERABAD, TELANGANA-500100

ABSTRACT - This article addresses the growing concern of security vulnerabilities in hardware systems, particularly in the context of integrated circuit (IC) chips used in cryptographic applications, which are increasingly susceptible to adversarial physical attacks in real-world environments. These attacks, often targeting the physical integrity of ICs, exploit weaknesses in both the design and manufacturing processes of cryptographic circuits. The paper provides a comprehensive overview of these threats, focusing on various physical attack methods, such as side-channel attacks, electromagnetic (EM) attacks, and laser fault injection attacks, which compromise the confidentiality and functionality of secure systems. It also highlights the vulnerabilities inherent in IC chips, particularly in relation to how attackers can manipulate or exploit system weaknesses during operation. The article delves into the protection mechanisms that are being integrated into modern cryptographic IC chips to prevent or mitigate these physical threats. One of the key strategies discussed is the use of on-chip monitoring circuits, which can actively sense and respond to adversarial attempts, providing an early warning or immediate countermeasures. These monitoring circuits are designed to detect unusual patterns that could indicate an ongoing attack, such as fluctuations in power or electromagnetic emissions, enabling dynamic protection of the system during operation. Additionally, the paper explores innovative physical structures, such as backside buried metal (BBM) wirings in silicon (Si) substrates, which are combined with frontside complementary metal–oxide semiconductor (CMOS) circuits to create robust defenses against a variety of physical attacks. This integration of backside metal wirings with frontside CMOS technology is a novel approach that enhances the IC's resilience by providing a physical barrier that reduces the ability of attackers to exploit weaknesses in the power delivery network and other sensitive components. By creating a unified approach to IC design and packaging, the paper emphasizes the importance of incorporating multiple layers of protection, such as detection, avoidance, and resilience, against electromagnetic and laser-based attacks. The combination of these advanced technologies establishes a more secure architecture that can defend against multimodal attacks, thus ensuring the integrity of cryptographic systems. The article also highlights the practical implementation of these protective strategies, including tests with silicon demonstrators to validate the effectiveness of the proposed solutions. The results show promising outcomes, demonstrating the feasibility of creating secure hardware systems that can withstand physical attacks and provide reliable protection for sensitive data and cryptographic operations. Through the integration of on-chip monitoring, advanced IC design principles, and packaging innovations, this paper offers a roadmap for developing secure, resilient hardware systems capable of withstanding the evolving threat landscape posed by physical attacks on IC chips. Ultimately, the proposed protection schemes not only strengthen the security of cryptographic circuits but also contribute to the broader field of hardware security, providing insights for future designs and applications.

I. INTRODUCTION With the rapid expansion of Internet of Things (IoT) applications, cryptographic devices have become integral to modern daily life, ensuring the security and privacy of data exchanged across the network. The IoT ecosystem is composed of edge nodes—often small, wireless devices—that interact with cloud servers located remotely or internationally, exchanging sensitive private information. This massive scale of data exchange necessitates robust encryption and decryption protocols to maintain privacy and prevent unauthorized access. Among the various encryption methods, symmetric ciphers are favored for IoT communications due to their relatively low processing overhead and smaller transistor requirements, making them efficient for real-time applications. The Advanced Encryption Standard (AES) has become one of the most widely adopted symmetric ciphers, known for its strong performance and implementation on integrated circuits (ICs) and field-programmable gate arrays (FPGAs). However, as the demand for greater security grows, particularly with more sophisticated IoT applications, the role of public-key ciphers, such as those used for digital signatures, encryption for group entities, and homomorphic encryption, becomes increasingly important. These ciphers offer enhanced security functionalities, providing solutions to challenges such as secure data computation over encrypted data without requiring decryption. Despite their advantages, implementing public-key ciphers on semiconductor IC chips comes with significant challenges, particularly related to minimizing power consumption, maintaining small footprint, and ensuring resilience against various types of attacks, including side-channel attacks. This is crucial for IoT devices, which are

https://doi.org/10.36893/IEJ.2024.V53I12.020

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

typically resource-constrained and must operate securely and efficiently within their limited hardware capabilities. As IoT applications expand further, particularly in critical domains such as autonomous vehicles, healthcare systems, and machine learning environments, the need for secure and reliable cryptographic hardware becomes more pressing. These applications often operate in environments where security breaches could result in catastrophic consequences, thereby necessitating stringent protections against physical and side-channel attacks on the cryptographic circuits. The rise of such systems demands continuous research into improving the security of cryptographic hardware, focusing on ensuring the resilience of IC chips against various physical attacks like power analysis and fault injection. This article specifically addresses the implementation of protection techniques at the IC-chip level to safeguard cryptographic systems in IoT environments. It explores the design of physical protection schemes that help secure cryptographic circuits against attacks, enabling secure communications and data handling in IoT devices. As IoT applications become integral to everyday life and increasingly critical sectors, protecting the hardware implementations of cryptographic algorithms has become essential. This article provides an overview of the existing threats to cryptographic systems at the hardware level, reviews techniques to mitigate these threats, and discusses emerging research to improve the security of cryptographic IC chips, particularly in the face of adversarial attempts to compromise the integrity and confidentiality of IoT data exchanges. The growing need for such secure systems underscores the importance of continuing to innovate and refine the security protocols and protections in hardware to ensure the confidentiality, integrity, and availability of IoT services.

II.IMPLEMENTATION

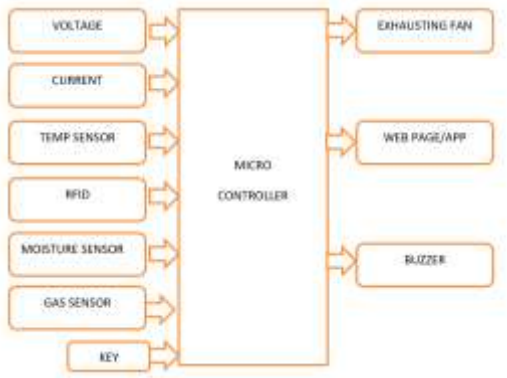


Fig: Block diagram

DESCRIPTION

POWER SUPPLY

A **regulated power supply** transforms unregulated AC (Alternating Current) into a stable DC (Direct Current). It guarantees consistent output despite variations in input. A regulated DC power supply is also known as a linear power supply, it is an embedded circuit and consists of various blocks

- **Regulated Power Supply Definition**: A regulated power supply ensures a consistent DC output by converting fluctuating AC input.
- **Component Overview**: The primary components of a regulated power supply include a transformer, rectifier, filter, and regulator, each crucial for maintaining steady DC output.
- **Rectification Explained**: The process involves diodes converting AC to DC, typically using full wave rectification to enhance efficiency.
- **Filter Function**: Filters, such as capacitor and LC types, smooth the DC output to reduce ripple and provide a stable voltage.
- **Regulation Mechanism**: Regulators adjust and stabilize output voltage to protect against input changes or load variations, essential for reliable power supply

SENSORS

Sensors are used for sensing things and devices etc. A device that provides a usable output in response to a specified measurement. The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity. The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance, etc.

Voltage Sensor

Generally, a sensor is an electrical device used to detect as well as respond to a particular type of signal like optical or electrical. Implementation of sensor techniques in voltage or current has become an outstanding option toward the measurement of voltage & current methods. The advantages of sensors over conventional methods for measuring mainly include less size and weight, high safety, high accuracy, nonsaturable, eco-friendly, etc. It is feasible to merge both the current and voltage measurement into a physical device with tiny and solid dimensions. This article discusses an overview of the voltage sensor and its working.

https://doi.org/10.36893/IEJ.2024.V53I12.020

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

What is a Voltage Sensor?

This sensor is used to monitor, calculate and determine the voltage supply. This sensor can determine the AC or DC voltage level. The input of this sensor can be the voltage whereas the output is the switches, analog voltage signal, a current signal, an audible signal, etc. Some sensors provide sine waveforms or pulse waveforms like output & others can generate outputs like AM (Amplitude Modulation), PWM (Pulse Width Modulation) or FM (Frequency Modulation). The measurement of these sensors can depend on the voltage divider.

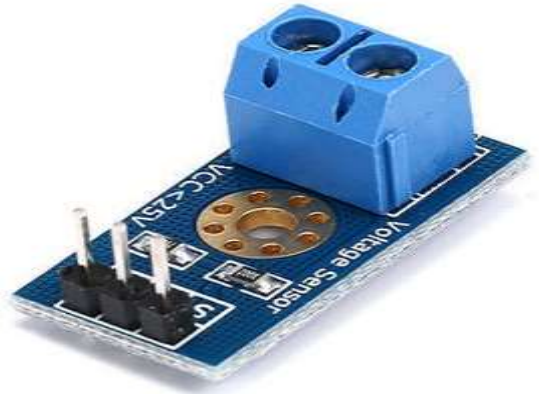


Fig: voltage-sensor

This sensor includes input and output. The input side mainly includes two pins namely positive and negative pins. The two pins of the device can be connected to the positive & negative pins of the sensor. The device positive & negative pins can be connected to the positive & negative pins of the sensor. The output of this sensor mainly includes supply voltage (Vcc), ground (GND), analog o/p data

Current Sensor and It's Application

Sensing variable current flow is a major requirement in frequent electronics systems and the strategies to do so are as an assortment of the applications themselves. A sensor is a unit that can determine a physical phenomenon and compute the latter, in other words, it gives a measurable demonstration of the wonder on a particular scale or range. A current sensor is a device that recognizes electrical current in a wire or a system whether it is high or low and creates an indicator relative to it. It might be then used to presentation the measured current in an ammeter or might be archived for further classification in a data acquisition system or might be used for control purposes. The current sensor is "disturbing" as it is an incorporation of some of the sensors, which may cause system performance. There is a wide variety of current sensors to monitor alternating or direct the current and its measurement is required in many applications be it in industrial, automotive, or household fields.

Principle:

The current sensor is a device that detects and converts current to get an output voltage, which is directly proportional to the current in the designed path. When current is passing through the circuit, a voltage drops across the path where the current is flowing. Also, a magnetic field is generated near the current-carrying conductor. These above phenomena are used in the current sensor design technique.

IR SENSOR

In the electromagnetic spectrum, the infrared portion divided into three regions: near infrared region, mid infrared region and far infrared region.

In this blog we are talking about the IR sensor working principle and its applications.

What is an IR Sensor?

IR sensor is an electronic device, that emits the light in order to sense some object of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. Usually, in the infrared spectrum, all the objects radiate some form of thermal radiation. These types of radiations are invisible to our eyes, but infrared sensor can detect these radiations.

Fig: IR Sensor

MQ2 GAS SENSOR

Sensors are the electronic devices used for interaction with the outer environment. There are various types of sensors available that can detect light, noise, smoke, proximity etc… With the advent in technology, these are available as both analog and digital forms. Besides forming a communication with the outer environment, sensors are also a crucial part of safety systems. Fire sensors are used to detect the fire and take appropriate precautions on time. For smooth functioning of control systems and sensitive electronics, humidity sensors are used for maintaining humidity

https://doi.org/10.36893/IEJ.2024.V53I12.020

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

in the unit. One of such sensor used in safety systems to detect harmful gases is MQ2 Gas sensor.

What is an MQ2 Gas Sensor?

MQ2 gas sensor is an electronic sensor used for sensing the concentration of gases in the air such as LPG, propane, methane, hydrogen, alcohol, smoke and carbon monoxide.

MQ2 gas sensor is also known as chemiresistor. It contains a sensing material whose resistance changes when it comes in contact with the gas. This change in the value of resistance is used for the detection of gas.

Fig: MQ2 Gas Sensor

MQ2 is a metal oxide semiconductor type gas sensor. Concentrations of gas in the gas is measured using a voltage divider network present in the sensor. This sensor works on 5V DC voltage. It can detect gases in the concentration of range 200 to 10000ppm.

RFID READER

Active RFID and Passive RFID technologies, while often considered and evaluated together, are fundamentally distinct technologies with substantially different capabilities. In most cases, neither technology provides a complete solution for supply chain asset management applications. Rather, the most effective and complete supply chain solutions leverage the advantages of each technology and combine their use in complementary ways. This need for both technologies must be considered by RFID standards initiatives to effectively meet the requirements of the user community.

RFID Reader Module, are also called as interrogators. They convert radio waves

Returned from the RFID tag into a form that can be passed on to Controllers, which can

Make use of it. RFID tags and readers have to be tuned to the same frequency in order to

Communicate. RFID systems use many different frequencies, but the most common and

Widely used & supported by our Reader is 125 KHz.

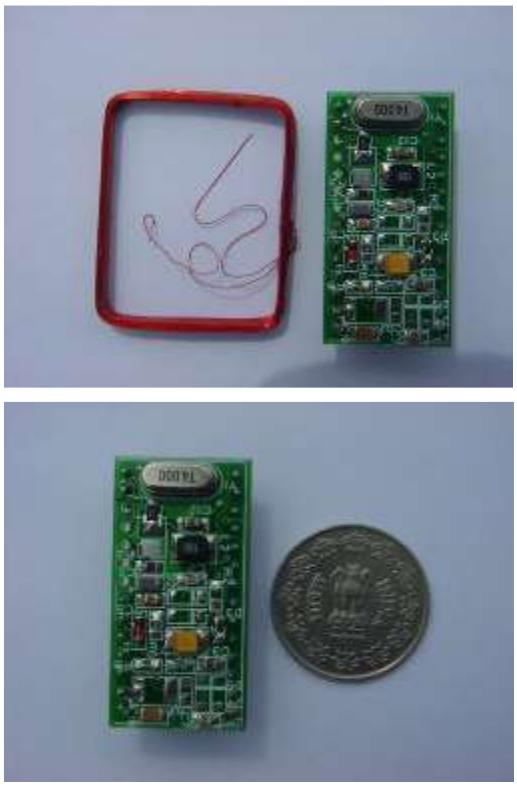


Fig: RFID MODULE

RPI –PICO

A Raspberry Pi Pico is a low-cost microcontroller device. Microcontrollers are tiny computers, but they tend to lack large volume storage and peripheral devices that you can plug in (for example, keyboards or monitors).

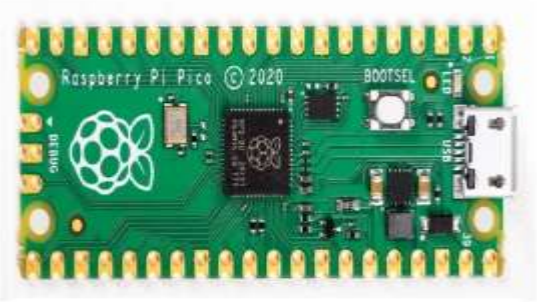
A Raspberry Pi Pico has GPIO pins, much like a Raspberry Pi computer, which means it can be used to control and receive input from a variety of electronic devices

Raspberry Pi Foundation is well known for its series of single-board computers (Raspberry Pi series). But in **January 2021 they launched their first micro-controller board known as Raspberry Pi Pico**.

It is built around **the RP2040 Soc, a very fast yet cost-effective microcontroller chip packed with a dual-core ARM Cortex-M0+ processor.** M0+ is one of the most power-efficient ARM processorRaspberry Pi PICO board

https://doi.org/10.36893/IEJ.2024.V53I12.020

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024



Raspberry Pi PICO board

Fig: Raspberry Pi Pico Board

Raspberry **Pi Pico is a small, fast, and versatile board that at its heart consists of RP2040**, a brand-new product launched by Raspberry Foundation in the UK. It can be programmed using MicroPython or C language

III. LITERATURE SURVEY

A. L. Uhsadel, A. Georges, and I. Verbauwhede, "Exploiting hardware performance counters," in Proc. 5th Workshop Fault Diagnosis Tolerance Cryptography, Aug. 2008, pp. 1–9.

The paper by L. Uhsadel, A. Georges, and I. Verbauwhede, titled "Exploiting Hardware Performance Counters," explores the use of hardware performance counters (HPCs) as a means to enhance the security of cryptographic systems. Hardware performance counters are specialized registers embedded in modern processors, designed to monitor low-level hardware activities, such as instruction execution, memory accesses, and cache hits/misses. The authors investigate how these counters, traditionally used for performance optimization, can be leveraged to detect fault injections and other side-channel attacks that target cryptographic hardware. They emphasize that attackers can manipulate the hardware to induce faults in cryptographic operations, leading to vulnerabilities in the system. However, by utilizing performance counters, it is possible to monitor the behavior of the system in real-time and identify abnormal patterns that may indicate an ongoing attack. The paper suggests that by integrating fault detection mechanisms using HPCs, the security of cryptographic systems can be significantly improved without incurring significant overhead. The authors discuss the potential of using hardware performance counters for both fault detection and system diagnosis. They propose a methodology for integrating these counters with cryptographic systems to enable the identification of anomalies that could suggest the presence of an attack, such as timing discrepancies or irregularities in memory access patterns. The paper provides insights into how such a monitoring system could be implemented in real-world cryptographic devices and highlights the practical challenges associated with this approach. Specifically, the authors examine the trade-offs between the effectiveness of fault detection and the computational resources required for monitoring. They also suggest that further research is needed to refine the use of performance counters in cryptographic hardware, including the development of more sophisticated detection algorithms and improved counter configurations. The paper concludes by advocating for the broader adoption of HPCs in the design of secure cryptographic systems, particularly as the need for enhanced security grows in response to increasingly sophisticated hardware attacks.

B. F. Liu, Y. Yarom, Q. Ge, G. Heiser, and R. B. Lee, "Last-level cache side-channel attacks are practical," in Proc. IEEE Symp. Secur. Privacy, May 2015, pp. 605–622.

The paper by F. Liu, Y. Yarom, Q. Ge, G. Heiser, and R. B. Lee, titled "Last-Level Cache Side-Channel Attacks Are Practical," explores the practical vulnerabilities in modern processors, specifically focusing on last-level cache (LLC) side-channel attacks. The authors investigate how attackers can exploit the shared last-level cache in multi-core processors to gain unauthorized access to sensitive information. These attacks leverage the timing discrepancies in cache access patterns, which can reveal secret data, such as cryptographic keys, in a system. The paper highlights that LLC side-channel attacks are practical and can be performed without requiring direct access to the target system or its physical memory. This makes them a serious threat to system security, especially for environments that rely on shared resources, like cloud computing or virtualized systems, where multiple tenants share the same hardware. The authors present a detailed analysis of the LLC side-channel attack, describing the mechanics of how data can be extracted through cache access patterns, such as cache hits and misses. They demonstrate that such attacks are effective in real-world systems, showing that even with software-level countermeasures or hardware-based protections, attackers can still extract sensitive information. The paper also discusses several defense mechanisms that could mitigate the risk of these attacks, including techniques like cache partitioning and cache flushing, but notes that these solutions often come with trade-offs in terms of performance. In conclusion, the paper emphasizes the need for more robust security mechanisms to protect against LLC side-channel attacks, particularly as processors continue to evolve and the number of cores in modern systems increases, making such attacks more feasible.

https://doi.org/10.36893/IEJ.2024.V53I12.020

C. P. Pessl, D. Gruss, C. Maurice, M. Schwarz, and S. Mangard, "DRAMA: Exploiting DRAM addressing for cross-CPU attacks," in Proc. 25th USENIX Secur. Symp., Aug. 2016, pp. 565–581.

The paper by Pessl et al., titled "DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks," explores a novel side-channel attack technique that targets modern processors by exploiting vulnerabilities in DRAM (Dynamic Random Access Memory) addressing. Specifically, the authors introduce the DRAMA attack, which allows an attacker to infer the memory layout of one CPU core from another, even when the attacker does not have direct access to the victim's memory. This is accomplished by leveraging the DRAM addressing scheme, where certain physical memory addresses correspond to specific locations in memory. DRAMA takes advantage of this to map memory regions that are used by different CPU cores in a system. The attack is particularly dangerous in multi-core systems, where memory is shared across processors, as it enables cross-CPU information leakage without requiring the attacker to have direct access to the memory itself. The authors demonstrate that the DRAMA attack can be used to extract sensitive information, such as encryption keys, by analyzing memory access patterns and using the DRAM addressing mechanism to link physical addresses from different cores. This cross-CPU attack bypasses traditional memory isolation protections and highlights vulnerabilities in shared hardware environments. The paper provides a thorough analysis of how DRAMA works, detailing the techniques used to carry out the attack and the potential security risks associated with it. The authors also explore mitigation strategies, such as hardware modifications and software techniques that could reduce the effectiveness of DRAMA attacks. However, the paper notes that these countermeasures are not foolproof, and attackers may still find ways to bypass them. The findings underscore the growing need for enhanced memory security techniques in modern computing systems to prevent unauthorized data extraction through side-channel attacks like DRAMA.

IV. DESCRIPTION

The paper "Physical Attack Protection Techniques for IC Chip Level Hardware Security" provides an in-depth examination of the growing threats posed by physical attacks on integrated circuits (ICs) and the associated protection mechanisms for securing cryptographic devices, particularly in the context of modern applications like the Internet of Things (IoT). As these technologies become increasingly integrated into daily life, the need for robust security measures to protect sensitive data transmitted through IoT networks becomes paramount. The authors focus on physical attacks that target the hardware itself, exploiting vulnerabilities in IC chips, which can be compromised through methods such as electromagnetic analysis, fault injection, and reverse engineering. These types of attacks are particularly concerning for cryptographic systems, where the confidentiality and integrity of the data are critical. The paper highlights various attack vectors, including side-channel attacks like electromagnetic (EM) and laser fault injection, which can potentially leak private key information or disrupt the normal operation of cryptographic algorithms. To address these threats, the authors discuss a range of protection techniques that aim to prevent, detect, and mitigate the impact of these attacks at the IC chip level. One of the key strategies explored is the design of on-chip monitoring circuits that can sense physical attacks in real time, enabling immediate countermeasures such as data scrambling or fault detection. Another important defense discussed is the use of backside buried metal (BBM) wirings in silicon substrates, which are designed to provide an additional layer of physical security against various forms of attack, particularly those targeting the chip's power delivery network or the circuits used for cryptographic processing. These security enhancements are integrated with the chip's CMOS circuits to ensure that even if an attacker tries to manipulate the hardware, the system can maintain its resilience against such incursions. The paper also covers the concept of multimodal security, which combines various techniques like EM shielding, fault tolerance, and monitoring systems to create a more robust defense against a wide range of attack methods. By incorporating these approaches, IC chips can achieve a higher level of security, safeguarding them against physical threats while ensuring that sensitive data remains protected during transmission or storage. The authors emphasize that the increasing demand for secure hardware in applications such as autonomous vehicles, medical devices, and military systems necessitates the development of more advanced protection strategies to safeguard against physical attacks. Finally, the paper outlines the potential future directions for hardware security, suggesting that further research is needed to develop new materials, techniques, and methodologies that can effectively counter emerging attack vectors and enhance the overall security of cryptographic ICs in a rapidly evolving technological landscape. The paper thus serves as a comprehensive guide to the state-of-the-art in IC-level security, providing insights into both the challenges and solutions for securing the next generation of cryptographic devices against physical attacks.

https://doi.org/10.36893/IEJ.2024.V53I12.020

CONCLUSION

In this paper, the authors have thoroughly examined the physical vulnerabilities of integrated circuits (ICs) and highlighted the various attack methodologies that adversaries may utilize to exploit these vulnerabilities, with a particular focus on cryptographic devices. The analysis emphasizes that, as technology advances, adversaries will become more proficient in executing multimodal attacks, combining various sophisticated techniques to breach security systems. This evolving threat landscape requires the development of more complex and diversified protection schemes tailored to the specific security functionality of the cryptographic algorithms being used. A key aspect of this paper is the proposal of a secure packaging technology that unifies backside metal wirings with frontside complementary metal–oxide semiconductor (CMOS) devices. This innovative packaging solution is designed to enhance the physical security of IC chips, making it more difficult for attackers to access critical components or induce faults in the system. The authors also introduce the design and implementation of on-chip monitoring circuits, which are crucial for sensing attacks in real time and ensuring that the system can react to potential threats. These circuits are specifically developed to detect and counteract both electromagnetic (EM) emission and laser injection attacks, demonstrating the system's resilience against such physical intrusion methods. The combination of on-chip monitoring and advanced packaging technology provides a robust defense against a variety of attack techniques, offering both preventive and reactive measures to protect cryptographic systems. Furthermore, the paper underscores the importance of recognizing the increasing complexity of physical attack methodologies, which necessitate a more comprehensive approach to hardware-level security. It highlights that the future of hardware security in very large-scale integration (VLSI) systems will hinge on the ability to detect, recognize, and obviate potential threats, with mechanisms that are capable of identifying and mitigating attacks at multiple levels, from the device and circuit design to the system architecture. The authors also point out that future research will need to extend beyond traditional approaches, integrating knowledge from diverse fields such as material science, device engineering, packaging technologies, and circuit/system design to develop even more resilient physical protection strategies. In addition to these hardware-based defenses, the paper calls for a continuous exploration of new methods and materials that can better withstand emerging attack vectors, including those targeting vulnerabilities at the intersection of hardware and software. As the demand for secure hardware increases, particularly in sectors like IoT, autonomous vehicles, and medical devices, the need for comprehensive protection strategies will only grow. To meet this demand, further innovation is required to strengthen physical security measures and make cryptographic devices more resistant to attacks. By presenting a clear roadmap for enhancing hardware-level security, the authors emphasize the importance of a holistic approach that combines security at the circuit, system, and package levels. Ultimately, the development of secure IC chips will be a crucial component in ensuring the privacy, integrity, and resilience of sensitive data in the face of increasingly sophisticated physical attacks. The paper concludes by highlighting the need for ongoing research and development in this area to stay ahead of potential threats, underscoring the importance of collaboration between experts from various domains to address the challenges posed by physical vulnerabilities in modern cryptographic systems.

REFERENCES

[1] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Standard FIPS PUB 197, Nov. 2001.

[2] S. K. Mathew et al., "53 Gbps native GF(24) 2 composite-field AESencrypt/decrypt accelerator for content-protection in 45 nm highperformance microprocessors," IEEE J. Solid-State Circuits, vol. 46, no. 4, pp. 767–776, Apr. 2011.

[3] R. Ueno et al., "High throughput/gate AES hardware architectures based on datapath compression," IEEE Trans. Comput., vol. 69, no. 4, pp. 534–548, Apr. 2020.

[4] P. Chodowiec and K. Gaj, "Very compact FPGA implementation of the AES algorithm," in Proc. IACR CHES, in Lecture Notes in Computer Science, vol. 2779. Springer, 2003, pp. 319–333.

[5] T. Good and M. Benaissa, "AES on FPGA from the fastest to the smallest," in Proc. IACR CHES, in Lecture Notes in Computer Science, vol. 3659. Springer, 2005, pp. 427–440.

[6] National Institute of Standards and Technology. Computer Securrity Resource Center, Lightweight Cryptography.Accessed:Mar.1,2021.[Online]. Available: https://csrc.nist.gov/projects/lightweightcryptography

[7] A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher," in Proc. IACR CHES, in Lecture Notes in Computer Science, vol. 4727. Springer, Sep. 2007, pp. 450–466.

https://doi.org/10.36893/IEJ.2024.V53I12.020

[8] J. Borghoff et al., "PRINCE—A low-latency block cipher for pervasive computing applications," in Proc. IACR ASIACRYPT, in Lecture Notes in Computer Science, vol. 7658. Springer, Dec. 2012, pp. 208–225.

[9] N. Miura et al., "A 2.5ns-latency 0.39pJ/b 289μm2/Gb/s ultra-lightweight PRINCE cryptographic processor," Proc. Symp. VLSI Circuits, Jun. 2017, pp. C266–C267.

[10] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)," IEEE Syst. J., vol. 14, no. 3, pp. 3440–3450, Sep. 2020.

[11] T. Matsumoto, M. Ikeda, M. Nagata, and Y. Uemura, "Secure cryptographic unit as root-of-trust for IoT era," IEICE Trans. Electron., early access, Jan. 28, 2021, doi: 10.1587/transele.2020CDI0001.

[12] I. M. R. Verbauwhede, Secure Integrated Circuits and Systems. Cham, Switzerland: Springer, 2010.

https://doi.org/10.36893/IEJ.2024.V53I12.020