The Era of Chip-Level Cybersecurity: Securing the Foundation of Modern Computing

Sai Sumanth Bommineni

A paper submitted to the Graduate Cybersecurity Program in partial fulfillment of the requirements for the M.S. degree at University of Maryland Baltimore County.

2024

* * * * *

By submitting this paper for grading, I affirm that this assignment contains no material previously created by any other person or platform except where due acknowledgment has been made. This paper contains no material that has been accepted for the award of any other degree or diploma from any university nor uses significant material previously submitted as part of prior coursework at UMBC or elsewhere.

TECHNICAL TOOLS CERTIFICATION

In researching and developing this paper (check one):

[■] NO, I did not use or receive technical assistance for this project other than standard onboard spell & grammar check and things like Google Scholar, academic library databases, or reference managers.

[ ] YES, I did use or receive technical assistance. In the area below, specify which service/system/tool(s) were used, and include all chat logs/prompts used in this project after your bibliography – which should not be considered in the expected page count for this assignment. *NOTE: If the use of generative technical assistance is discovered after paper submission, a failure to disclose the use of such tools will result in an immediate 'F' for your paper and an Academic Integrity report filed with the Graduate School. If in-doubt, report it here to be safe!*

Abstract:

Chip level cybersecurity opens completely new horizons in the protection of modern computing. This paper has outlined the critical need to integrate security right into chips in view of the inability of traditional software-based solutions and enhanced complexity in chip architecture. Key focus for this research involves automating the integration of security mechanisms on chips in a way that maintains high performance with increased security, covering all phases of a chip's lifecycle, from design to build to end. Discussing various current vulnerabilities and surveying both current and proposed chip-level security solutions, this paper will completely redefine how cybersecurity is approached in the digital world.

Keywords: Chip level cybersecurity, variety of advanced computing systems, security measures, computer chips, software-based solutions, chip architectures, automating of security integrations, higher performance, chip life cycle, vulnerabilities, methodologies, and cybersecurity approach.

Contents

1. Introduction:

Cyber security as one of the most important aspects of present-day computing needs no introduction, such is the threat to the digitized interconnected systems that run global economies, delivery of healthcare, critical infrastructures and defense mechanisms. The emphasize on digital technologies creates new risks that are exploited by the bad guys, threats act on hardware and software. While traditional software-based security controls are pervasive they are increasingly effectual when dealing with today's modern and sophisticated threats let alone embedded within the most fundamental of IT infrastructures – computer chips. Circuit-level security has therefore been realized as a key means for enhancing modern computing infrastructure against new generation cyber threats.

Traditionally, security measures have been focused primarily on applications – or programs in general, sphere. These include firewalls, specific antispyware and antivirus programs, as well as intrusion detection systems that protect from and at other layers of the computing stack. Nevertheless, when threats rise in complexity, hackers are targeting vulnerabilities at the system's hardware level. For example, Spectre and Meltdown that exploited microprocessor flaws prove that software-only protections are highly restrained. These events depict the necessity of a design that incorporates security components deeply into the chip fabrication and that risks are mitigated at their core. (Tomlinson et al.)

The transition to HW-based security solutions is an innovative breakthrough of the existing security model. This approach is much stronger and more active compared with integration of security features at the later stages of microchips' production. Hardware-based security increases an endpoint's ability to withstand attacks even further and minimizes how much an endpoint depends on post-deploy software updates, which are rely on patches. (Xi et al.)

Additionally, security integrated was the hardware is consistent with the concept of secure development that emphasizes protection in design and not merely an aftermath of an attack This research was set out to make three significant contributions to the field of chip-level cybersecurity.The first of these goals is to bring out the capability to integrate own measures into the chips themselves automatically. Automation helps to decrease the time needed, as well as the level of the expertise, to implement strong security for different applications. The second goal centers on an organization's performance while offering security to stakeholders. The main problem in employing ahardware-based security solution is that improving the security typically has a negative effect on the computational speed. The goal of creating solutions that sustain high performance, and strong securityis vital for the applicability to future sectors including the IoT and autonomous systems

Last, but not least, the research aims at covering the whole life cycle of the chip from initial design and production to its operation in the main field and retirement. The mitigation of threats in each phase of this lifecycle also implies that susceptibilities cannot manifest at any point hence strengthen system securities for the long haul. (Xi et al.)

Through synthesizing these objectives, this research seeks to make a call of a shift of the perception and practice of implementing cybersecurity. Instead of starting to consider security after the main development is complete, it emphasizes the importance of building protection measures into the keyhardware-software setup. But it also does not just increase defenses against current threats that facethe computing industry, but also prepares the computing industry for future forms of threats.Consequently, the time of enhanced chip-level protection is a breakthrough in assessing the security of the information era of the contemporary world.

2. Limitations of Traditional Software-Based Solutions

It is becoming increasingly clear, however, that software- based cybersecurity has its shortcomings. One is that a lot of software depend on reacting to threats as they progress instead of preventing them in the first place. Some of the most common categories of intrusion detection techniques, such as the signature-based techniques, need to have information about a threat to enablethe crafting of the signature. In turn, new forms of threats, including zero-day vulnerabilities, tend toavoid typical detection methods

Another limitation is based on the regular use of software patches and updates alone. Though an important aspect of asset management, patch management brings in the latency during which systemsare open to threat. Also, applying updates will always interrupt the running processes and in most instances, it will be interfering with the key running processes in vital areas like healthcare and industrialprocesses. This challenge is worsened by the increasing number of software vulnerabilities discoveredevery year, a problem that complicates the update calendar across all corporations

Software-based defenses also suffer from this compatibility problem. Various computing environments, including different OS, applications or devices must rely on integration of different security tools. But this integration is not easy to achieve, and when done so often leads to the formation of security flaws. Furthermore, applying several layers of security measures can cause slower operation with resource constraint systems such as the IoT devices, which have serious computing and energy constraints.

3. The Growing Complexity and Vulnerability of Chip Architectures

Chip architectures have changed significantly over the year due to the need for Capacity, Efficiency, and Size. Due to the processing power of microprocessors today, it means they feature exponential complexity, which stems from the Moore's Law that postulated the functionality growth, represented as the density of transistors chipped onto a planar base would roughly double every two years. These have in turn provided some modern features like multiprocessor capability, boosted artificial neural network and network functioning. However, they also brought a series of threats that have been followed by adversaries into the system

Another area which has been exposed due to chip architectures is the globalization of supply chain. Many computer chips at present are developed, built, and packaged in different areas of the globe andit is a multilateral process. This distributed supply chain opens the chance for an adversary to introduce hardware Trojans or designed backdoors or other malicious changes. Identifying such changes is highly challenging since they are hard to distinguish from genuine circuit components. (M. Reimann et al.)

There are many challenges such as the use of heterogeneous computing architectures has made it worse. The presence of different classes or types of processors, including CPUs, GPUs, and even FPGAs, are now incorporated into systems where each is suited for a particular kind of work. This improves itsperformance, in the process adding a new set of attack vectors. For example, threats can be directedto one type of processor and the whole system will be at risk

Another emerging threat type is side-channel attack based on embodied side information which includes current consumption, electromagnetic radiation, timing faults, etc. These attacks are very useful in pointing out areas in cryptographic operations, and the ability of the adversaries to guess the encryption keys or other secrets. Even more, these risks heightened with the enhanced use of various platform and application sharing in cloud systems; it can be for v Sphere shared computing resource; attackers may apply cross-tenant intrusive approaches. (Yuan et al.)

Additionally, as chips pull increasingly sophisticated functions, such as hardware accelerators and fixed-instruction security processors, it becomes difficult to guarantee their integrity. These features also contain design glitches, or are perhaps misconfigured on purpose, which can inadvertently lead to creation of certain vulnerabilities. For example, the Intel Management Engine (IME), a subsystem for remote management, has received records of possible backdoors that threaten the system's security.

The move to the latest generations of smaller transistors which is evolutionarily necessary forimprovement of device performance and power consumption leads to the problem of reduced reliability. The shrinking of the transistor length results in increased sensitivity to impurities and defectivity during processing, radiation, and thermal damage. The mentioned physical phenomena cannegatively affect the system reliability and introduce error that might be leveraged by an attacker.

4. Examples of Hardware attacks:

4.1 Spectre (CVE-2017-5753 and CVE-2017-5715)

Spectre is a class of vulnerabilities that exploits speculative execution. There are two main variants:

Spectre Variant 1 (Bounds Check Bypass, CVE-2017-5753), this variant allows an attacker to leverage branch prediction for leaking information from other process memory. It can be used to bypass user/kernel privilege boundaries and virtualization. (CVE, n.d.). Spectre Variant 2 (Branch Target Injection, CVE-2017-5715), this variant allows an attacker to force the victim process into executing speculatively certain memory locations, therefore potentially leaking sensitive data. (CVE, n.d.)

4.2 Meltdown (CVE-2017-5754)

Meltdown is a hardware vulnerability, and in most Intel processors, it enables an attacker to read privileged kernel memory from unprivileged user space. (CVE, n.d.)

Rowhammer (CVE-2020-10255)

Modern DRAM chips (DDR4 and LPDDR4 after 2015) include a vulnerability called Target Row Refresh (TRR), also known as the TRRes pass problem, which affects the deployment of internal mitigations against RowHammer assaults. To exploit this issue, the attacker must generate certain access patterns that cause bit flips on susceptible memory modules, known as a Many-sided RowHammer attack. (CVE, n.d.)

4.3 Thunderclap

Thunderclap was discovered in 2019 and exploited systems with Thunderbolt ports. The vulnerability allowed an attacker with physical access to perform DMA attacks for reading system memory and sensitive information. (CVE, n.d.)

4.4 Active and passive attack:

Several attempts have been made to extract secret key information from cryptographic circuits in operation. Passive assaults focus on physical side effects like power supply.

Side-channel (SC) assaults refer to the generation of noise and electromagnetic waves during circuit operation.

External observers can derive secret key bytes from power current waveforms captured by probing voltage changes at the power supply terminal or receiving EM emanations across an IC chip.

Active attacks compare erroneous outputs to accurate outputs following purposeful fault injections in fault attacks. When an observer purposefully injects flaws by switching internal values of memory macros or register files, the crypto processor may create incorrect output bits. (Nagata et al., 2021)

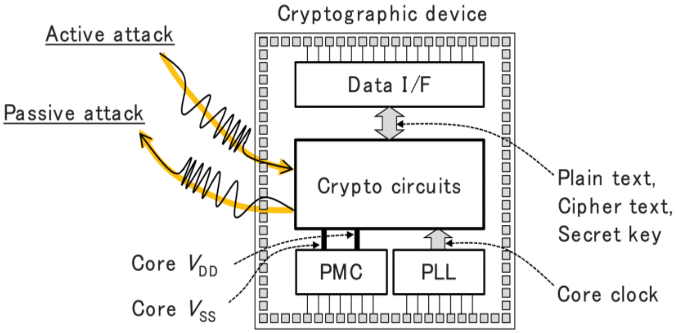


Figure 1: Physical attack isolation at chip level (Nagata et al., 2021)

The electrical features of power delivery networks (PDNs) make them inherently susceptible. The core VDD power current varies dynamically in response to cypher algorithm processing stages. Micro regulation of core VDD is commonly accomplished with an on-chip low-dropout linear regulator (LDO), which stabilizes VDD voltage via error feedback with on-chip RC components, reducing the need for massive off-chip capacitors. This enables detailed voltage control across core VDD regions with different workloads, while also reducing the visibility of the VDD voltage. However, the external power current (IEXT) reflects the digital circuit's power consumption inside the core VDD regulation bandwidth, leaving power and EM side-channel leakages unabated. (Nagata et al., 2021)

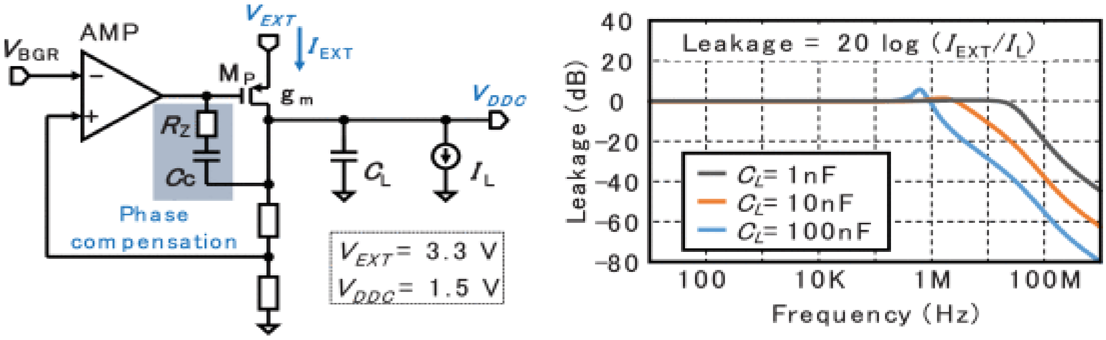


Figure2: LDO as an on-chip micro regulator. (Nagata et al., 2021)

4.5 Side-Channel Leakage in Cryptographic Circuits

Public-key cryptographic circuits, such as those used for the implementation of the Elliptic Curve Digital Signature Algorithm, are particularly vulnerable to SC leakage through LDOs. This type of leakage occurs due to differing utilization of clock cycles because of variable arithmetic operations. These operations generally rely on the polarity of the bit in the ECDSA for either elliptic curve point doubling or addition. (Nagata et al., 2021)

By analyzing EM waveforms, an adversary might discover computational patterns that leak the secret key bit-stream. The LDO's low-pass bandwidth allows most SC leakage frequencies-say <100 kHz for ECDSA running at 100 MHz-to pass through the on-chip and off-chip PDNs and become visible at the external supply terminals. The attack remains effective even with countermeasure techniques utilizing methods such as the Montgomery ladder approach. (Nagata et al., 2021)

In contrast, symmetric-key schemes like AES exhibit much weaker leakage: the operations occur in ~10 clock cycles, each at hundreds of megahertz, this pushes the power noise out of band. LDO, this rapidly reduces the leakage by ~20 dB/decade. Smaller circuit size (~\(10^3\) transistors) coupled with capacitor-based charge equalization further smoothest the power consumptions and further hardens

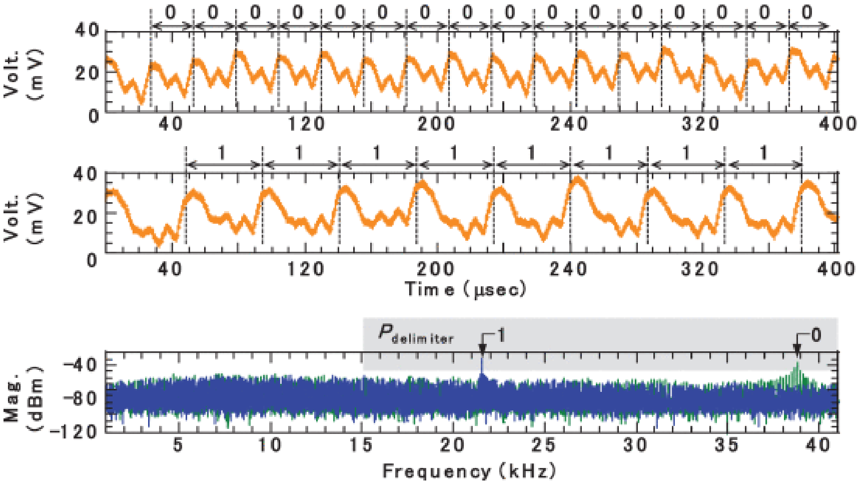


Figure 2: Electromagnetic signatures and frequency waves are measured on Printed circuit board from ECDSA engine at 50 MHz. (Nagata et al., 2021)

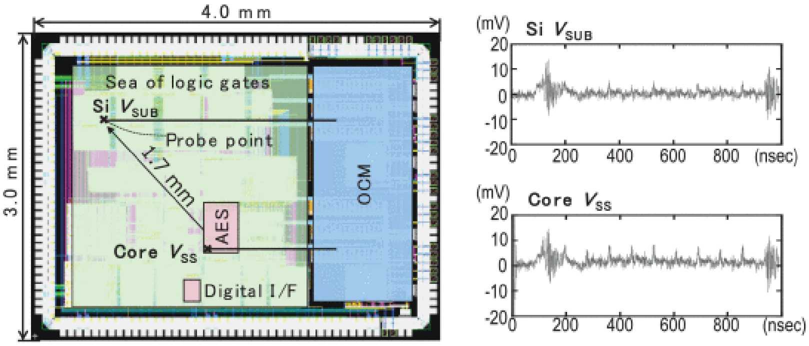
4.6 Vulnerabilities in Si Substrates of Crypto Circuit Implementations

In CMOS devices, the p-type doped silicon substrate Si serves as the base material, on top of which crypto circuits are implemented by instances of CMOS logic standard cells. Considering this layout, these naturally connect the VSS side to the p-type Si substrate through p+ ohmic contacts, while core VDD connects to n-type wells through n+ contacts. A consequence of this is that there is only one single VSS domain, which is part of the on-chip power delivery network. (Nagata et al., 2021)

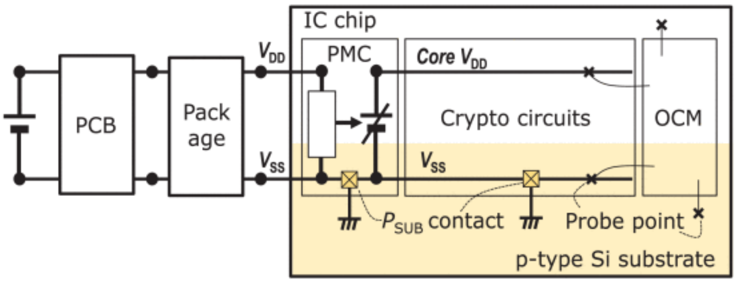
Voltage regulators isolate the core VDD, but the VSS side is yet open to SC leakage that can be exploited by an adversary via the shared Si substrate. Substrate engineering, such as the insertion of intermediate silicon oxide for capacitive isolation, provides limited attenuation, especially when cryptographic circuits of large area are under attack, like the implementations of EC algorithms. (Nagata et al., 2021)

OCM has demonstrated that the VSS voltage variations track the internal operation of a circuit, for instance, advanced encryption standard AES, incredibly well even for 1.7 mm, while measurable substrate variations allow the CPA to disclose the secret key bytes, which makes the substrate an unavoidable source of SC leakage. (Nagata et al., 2021)

For typical IC chip thicknesses of about 350 µm or less, the horizontal proximity of such circuit blocks, like AES and LDO, becomes large. More recently, advances in chip packaging also tend to further expose the backside of the IC chips as an attack surface, enhancing their vulnerability to SC leakage. Therefore, strong substrate and package design plays an important role in making cryptographic circuit security more robust. (Nagata et al., 2021)



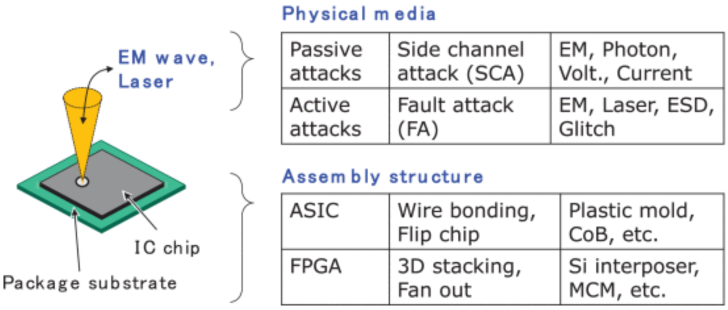
Fiqure 3: On-chip waveform in crypto operation (Nagata et al., 2021)



Fiqure 4: Power delivery and Si substrate network. (Nagata et al., 2021)

4.7 Vulnerability at packaging and assembly

An opponent can use physical assaults that are primarily centered on electromagnetic and optical, although thermal, acoustic, and mechanical qualities are also considered. As seen in the below Figure, the packaging and assembly architectures of a target IC chip must be evaluated in terms of protection. Electromagnetic measurements offer greater flexibility in picking locations, angles, and frequencies of interest over 100 µm or more in space, even without knowing surface materials. Optical measurements may localize assaults in space and time with a precision of 1 µm and 10 ns, respectively. However, this requires decapsulation of an IC chip due to the opaque nature of resin materials used in laminates and molding. (Nagata et al., 2021)



Physical media

Passive attacks	Side channel attack (SCA)	EM, Photon, Volt., Current
Active attacks	Fault attack (FA)	EM, Laser, ESD, Glitch

Assembly structure

ASIC	Wire bonding, Flip chip	Plastic mold, CoB, etc.
FPGA	3D stacking, Fan out	Si interposer, MCM, etc.

Fiqure 5: Precautions for attacks and structure packing. (Nagata et al., 2021)

4.8 Addressing the Challenges

Pursuing software-based solutions only and ignoring vulnerabilities emerging in modern chip architectures are impossible because of their specific shortcomings to overcome these and other shortcomings of the traditional paradigm of cybersecurity means, it is necessary to incorporate the new generation of chips and periphery into the cybersecurity environment. This means that security is integrated at the design level of the chip and all threats are then dealt with right from their root cause. For instance, secure firmware, hardware shielding, fixed security block, and advanced encryption standards at the present chip level protect against a range of threats (Mitra et al., 2021).

It is also important to include the security-aware design flow in the case with the lifecycle management. This makes it possible not only to provide chips the maximum protection at the stage of their manufacture, but also during their work in the system. To improve chip architectures' security, works like formal verification, threat modelling, or runtime monitoring can supplement such techniques (Smith et al., 2023).

5. Concepts of Hardware/Software Co-Design

Hardware software codesign is the process of designing the hardware and software components together to address a particular problem of system performance, functionality, and security. Unlike methodology that deals with hardware and the software separately, co-design seeks to integrate hardware and software, hence the dependency of the two. They are both valid at the system and component levels and this approach is especially relevant for the modern threats that can occur at both System and Component levels and must be addressed with the System-level approach only. (Varshika et al.)

In the case of chip level security, HW/SW co-design is the methodology that helps to incorporate security-related functions into the chip architecture and to guarantee the compatibility of the software with the functions implemented at the chip level. For instance, current processors can include hardware security blocks like Secure Isolated Regions or Trusted Execution Environment. These modular structures require both hardware and software to create safe realms for significant tasks, preventing the unauthorized review of sensitive information. This integration ensures good defense and is well blended with the systems performance plus the overhead since the security measures are contextual to the implemented hardware and software systems. (Varshika et al.)

6. Methodology

This research method explains the research strategy, sites, instruments, and assessment techniques that aided in the realization of the study goals. The emphasis is made on the chip level existing solutions review, creation of prototypes of on-chip security and intensive exploration of theeffectiveness of the prototypes.

6.1 Research Approach

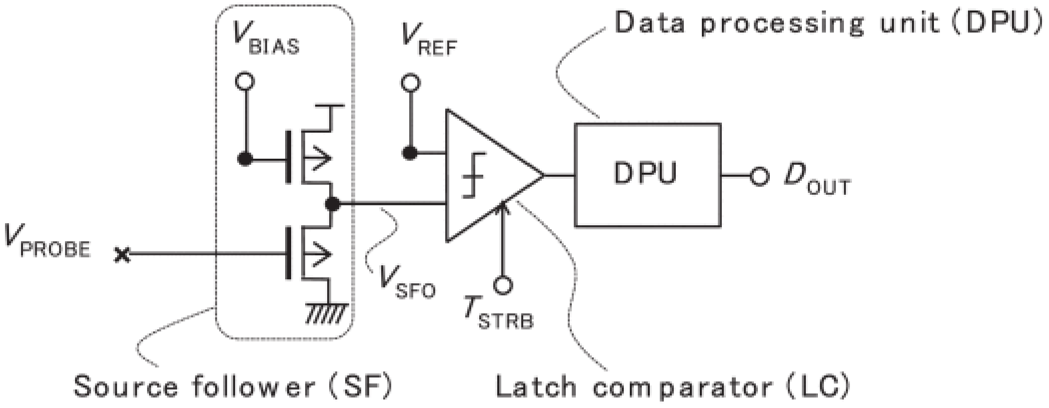
6.1.1 Analysis of Existing Chip-Level Security Solutions

The first stage of the study focused on the identification of chip-level security solutions already in the market. In this analysis, efforts were made to consider current techniques, appreciate existing potentials, and explore shortcomings.

7. Existing Protection methods:

7.1. On-Chip Characterization

The unparalleled technique in detecting SC leakages and adversarial activities in crypto circuits is presented through OCM in Figure below. The method of measurement involves the variation of local voltage at selected points of core VDD and VSS wirings and VSUB taps, while the measured values are independent of any coupled noises by the global PDN. To solve problems of power and substrate noise and further enable EMC, an OCM has been developed. Recently it has been extended toward advanced hardware security applications. (Nagata et al., 2021)



Fiqure 6: Circuit schematic of OCM (Nagata et al., 2021)

This is achieved by performing the measurement of the target voltage at the input of the

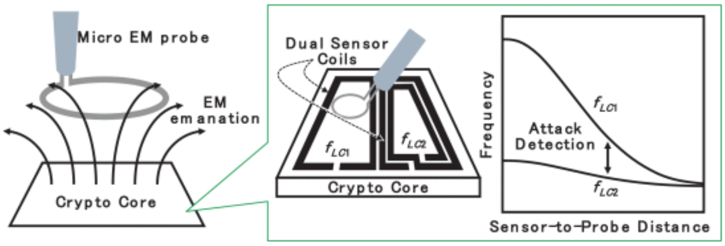
OCM, VPROBE, with the aid of an SF; the voltage is then converted into a digital code: the SF output voltage VSFO is compared to a stepped reference voltage VREF using an LC at given timings TSTRB. This comparison, performed at each given timing, provides a digital code corresponding to the closest approach between VSFO and VREF. This process repeats iteratively across the chip for successive timings, with extremely fine resolutions: voltage steps (ΔVREF) are 100 µV, and timing steps (ΔTSTRB) are 100 ps. This will capture and analyze the waveforms in real time for possible SC leakages from cryptographic operations. The successive approximation register analog-to-digital converter is being used, which enables execution of several thousands of clock cycles while digitizing in using public-key cryptography like ECDSA running at 50 MHz (Nagata et al., 2021)

7.2. Attack detection through Electromagnetic wave:

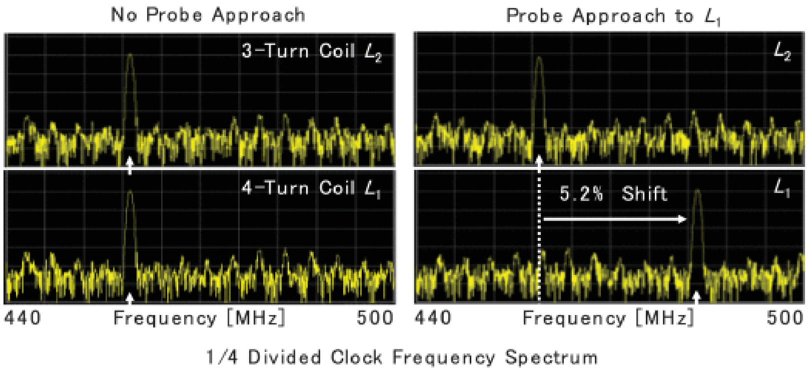
Indeed, electromagnetic power can be directly coupled with the vulnerable nodes of an IC chip either via cables or by irradiing the top side of a packaged chip. The idea has been exploited in active fault injection attacks to disrupt intentionally the execution of cryptographic primitives. Unlike other invasive techniques, such as voltage surges or clock glitches, which can be easily countered by using power converters and PLLs, respectively, in general EM attacks are more efficient and low-cost, and in most scenarios, no high-end test equipment is needed. (Nagata et al., 2021)

In passive attacks, a miniaturized micro antenna µEM probe is scanned over the IC chip to seek locations that indicate the highest EM side-channel leakage, such as in the case of LEMA. Removing the resin protective layers covering the chip in question greatly improves the resolution of such scans.

The EM power can be coupled directly onto the vulnerable nodes of an IC chip via cables or by irradiing the top side of a packaged chip. This technique becomes quite customary for active fault injection, with the purpose of hampering cryptographic operation executions. As voltage surges or clock glitches that can easily be counteracted using power converters and PLLs, respectively, attacks through EM are more feasible in terms of investment cost and effectiveness, mostly without the need for high-end equipment. (Nagata et al., 2021) The so-called µEM probe-a miniaturized micro antenna-is scanned over the chip to identify those locations that have the highest EM side-channel leakage, in passive attacks like local electromagnetic SC attacks-namely, LEMA. Removing protective resin layers that cover the chip increases the resolution of such scans drastically. (Nagata et al., 2021)



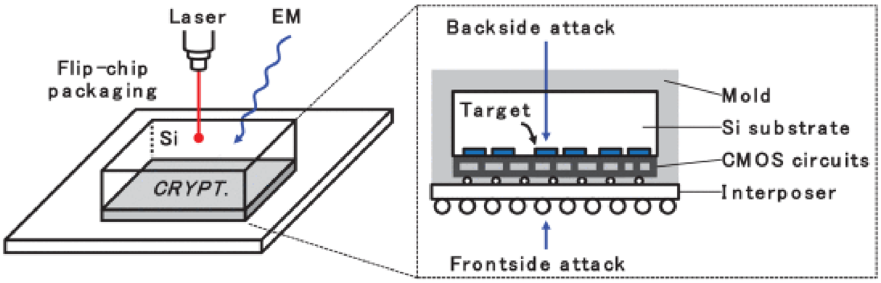
Fiqure 7: Sensing principle of LEMA (Nagata et al., 2021)



Fiqure 8: Electromagnetic wave detection demonstration. (Nagata et al., 2021)

7.3. Packaging method to secure IC

The backside of a flip-chip packaged IC chip is directly exposed to a potential attack on the Si substrate as shown in Fig. 15. Antennas can inject EM waves from the resin coating or plastic molding of a chip, but detachment of these increases the vulnerability of chips. Furthermore, optical observation can trace photon emissions out of active transistors, or laser irradiation induces body currents that can generate faults in a chip. These types of attacks typically require decapsulation of the chip, thinning, or even partial removal of the Si substrate. The attackers may employ FIB machinery for high-level reverse engineering Photo-current sensors can also detect incoming light in case the package has been opened with the intent of performing this class of attack. (Nagata et al., 2021)

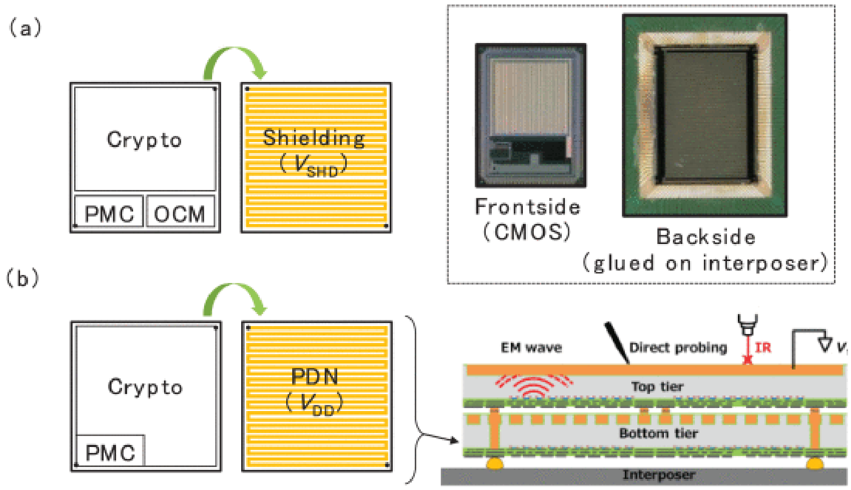


Fiqure 9: Attack surface of an Si backside. (Nagata et al., 2021)

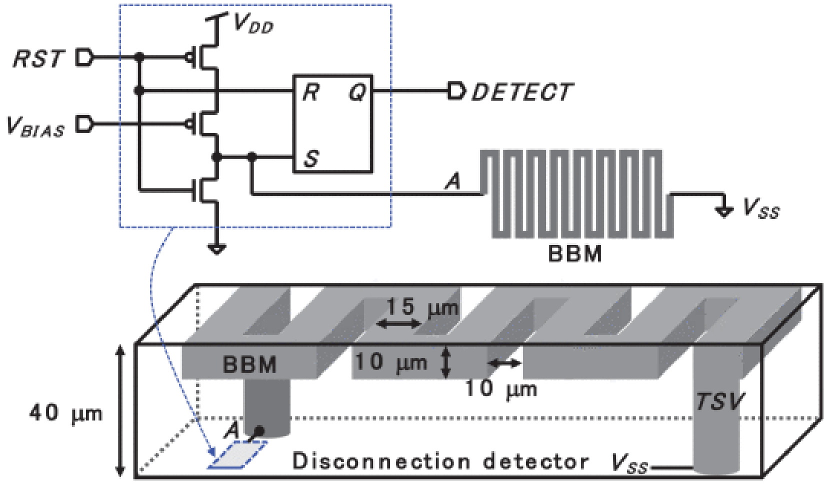
Growth has the challenge of bringing in more resilience against multi-model and combinatorial physical attacks. Advancement in semiconductor packaging technologies needs performance improvement, size reduction, and lowering of the profile of mass-produced IC chips. Resilient packaging combined with detection circuitry could, on the other hand, achieve manifold increases in protection for crypto-circuits against invasive and non-invasive active and passive Side-Channel (SC) attacks. Secure packaging methods are defined as. (Nagata et al., 2021)

Various schemes have been proposed to enhance the power delivery capability within the IC chips based on a technology called backside buried metal (BBM) [85]. It is also used for secure packaging. The BBM wiring was made of copper with width and depth of 15 and 10 □m, respectively. It was placed at the backside of a 40 □m thick silicon (Si) substrate and was connected to the frontside CMOS circuits using TSVs. (Nagata et al., 2021)

Monolithic architectures to thwart attacks for a single chip and a 3D chip stack respectively. In such architecture, front-end CMOS circuits, which contain crypto circuits, voltage regulators and OCM circuits can prevent and detect the attack. Note that, in case of using flip-chip package, BBM wiring is exposed to the outside. This meander shape will provide an EM shielding, screen out lasers and work as a disconnection detector in case of an attempt of laser cutting is made. This is preferable overusing one metal plate to cover the whole backside area. This will secure the entire public-key crypto circuit.

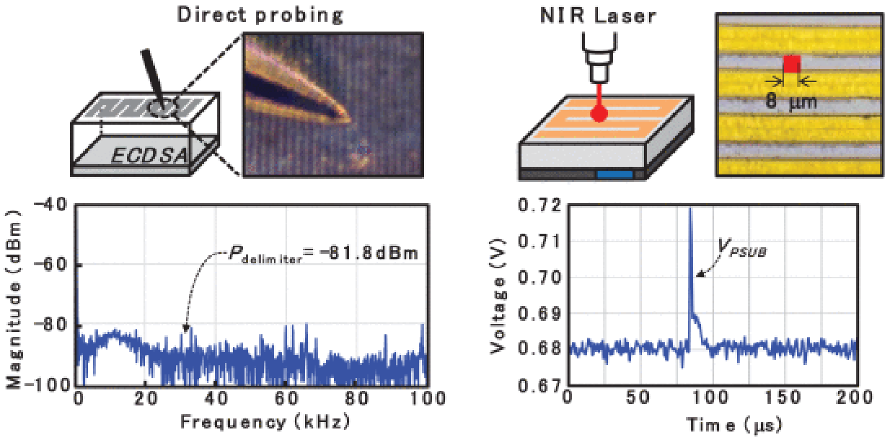


Fiqure 10: Attack protection Structure, a represents single chip, b represents Chip stack in 3D (Nagata et al., 2021)



Fiqure 11: Disconnection detection using BBM (Nagata et al., 2021)

It presents the test results of attack protection and die photographs of BBM chip. Voltage probing test which is directly done on backside Si substrate exhibits the suppression of Pdelimiter for more than 25 dB in comparison to the regular IC chip without BBM. It can focus on the gap between the BBM stripes, with 10 µm set in our experimental fabrication process; however, the resultant voltage variation on the frontside of an IC chip can be captured and recognized by the OCM. The BBM meander conceals the circuit components from laser irradiations, and further detects the unexpected disconnection due to the adversarial trial of the metal removal by a laser cutter. (Nagata et al., 2021)



Fiqure 12: Passive on left side, active on right side, demonstrates BBM protection. (Nagata et al., 2021)

BBM IC chips are in stacked 3-D packaging. The bottom chip carries crypto circuits with its own designated power converters and supported PDNs by BBM stripes over the full backside area. While the frontside is facing down to a plastic interposer and assembling on a PCB, the backside is facing up and gets occluded by the top tier die. The top chip has a similar architecture to that in the single die with only one important difference, it does not embed cryptographic functions. The proposed architecture suppresses SC leakages both vertically-by the shielding effect of the BBM-and horizontally-by the BBM distributed decoupling capacitors across the PDNs. While the second one locally flattens the variation of power currents among logical switching gates and thus suppresses the power current dependence on sequences of arithmetic computation in, for example, EC-based public-key crypto algorithms. (Nagata et al., 2021).

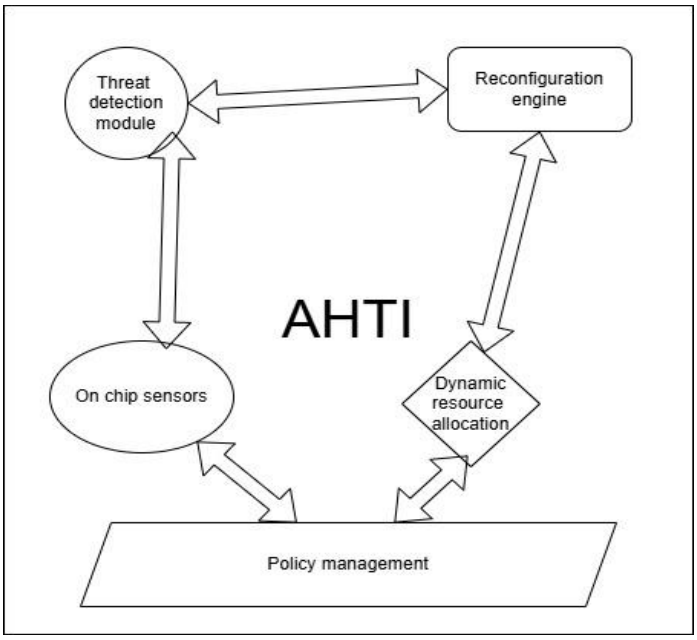
Reference	Description	Attacks	Advantages	Disadvantages
(Dione et al., 2023)	This study examines hardware security problems for IoT in the age of quantum computing and covers NIST's post-quantum cryptography standards. It emphasizes the need of safeguarding hardware from side-channel assaults (SCAs)	Side-channel vulnerability, and quantum-era risks	Provides insights on post-quantum cryptography and emphasizes the necessity for SCA protection.	Focus on theoretical issues rather than actual implementations.
(Canavese et al., 2024)	Proposes an IoT Proxy to improve security for resource-constrained IoT devices by externalizing security tasks via a network gateway that includes Virtual Network Security tasks. (VNST)	Network-based attacks, unauthorized access	scalable, reduces computational overhead on IoT devices, security enhances through ML techniques	May require significant network infrastructure changes
(Khan et al., 2024b)	Trusted Hardware-based Scalable Secure Architecture for IoT systems.	Key exposure, data tampering	Scalable and modular, supports dynamic key rolling to enhance security	Relies on additional hardware components (TPM)

Reference	Description	Attacks	Advantages	Disadvantages
National Institute of Standards and Technology (NIST). (n.d.).	This demonstrates the use of Manufacturer Usage Description to secure home IoT devices by restricting network communications to only what is necessary for device functionality.	Network-based threats such as DDoS attacks	Enhances device resilience to network attacks, automates network configuration based on MUD specifications	Requires manufacturer support and network infrastructure compatibility
(Sidhu et al., 2019)	Discusses hardware Trojans (HT) in IoT devices and presents countermeasures such as Proof Carrying Hardware (PCH) and Hardware Security Modules (HSMs).	Hardware Trojans, IP piracy	Provides detailed taxonomy of HTs, suggests robust detection and prevention methods like PCH and HSMs	Implementation can be complex and costly

Table 1: Some of the published methods of protecting chip-level cybersecurity.

8. Proposed Model (AHTI):

AHTI: AHTI stands for Adaptive Hardware-Level Threat Isolation and defines a new security framework embedding real-time threat detection and isolation mechanisms right into chip architectures. Such an approach is crucial in trying to handle hardware-level vulnerabilities that software solutions hardly can mitigate.



Fiqure 13: AHTI overall architecture.

AHTI is implemented in a modular, scalable architecture to fit within a nanometre-sized chip for mobile devices or computers.

8.1. Module 1: Threat Detection Module TDM

Overview

TDM is an architecture that continuously monitors the chip's physical parameters using distributed sensors. This would identify vulnerabilities, which might signal a security compromise caused by side-channel attacks or fault injections.

Sensors are on-chip parts.

1. High-Accuracy Remote and Local Temperature Sensors.

2. Voltage Monitors: These are implemented utilizing comparator-based designs to detect changes in voltage, such as voltage dips.

3. Current Sensors: A differential amplifier-based sensor for detecting power consumption.

4. Performance Counters: count cycles, cache misses, amongst others.

Abnormal Detection Engine

It simply uses statistical models and machine learning techniques to discover deviations from typical behaviour.

Detailed Architecture

On-Chip Sensors

1. Temperature Sensors

Type: High Precision Remote and Local Temperature Sensor is used to measure temperature changes utilizing an onboard thermal transistor or diode.

Interface: Two-wire SMBus, pin-programmable addresses.

2. Voltage monitors.

Type: Comparators and Evaluation

Purpose: To find sags in the supply voltage with respect to a reference.

$$V_{out}\{1\ if\ V_{in} > V_{ref}$$

$$V_{out}\{0\ if\ V_{in} < Vref$$

3. Current Sensors:

Type: differential amplifier-based function, which can be computed based on measurement of the voltage drop across the sensing resistor.

Equation:

$$I = \frac{V}{R_S}$$

4. Performance counters.

Observe the anomaly in several CPU signals such as cycles or cache misses.

Anomaly Detection Engine:

- Z-score. Normalization:

Normalizes sensor readings in a scale to make the analysis uniform. Sensor Readings are referred to as X, mean as μ and, standard deviation as σ.

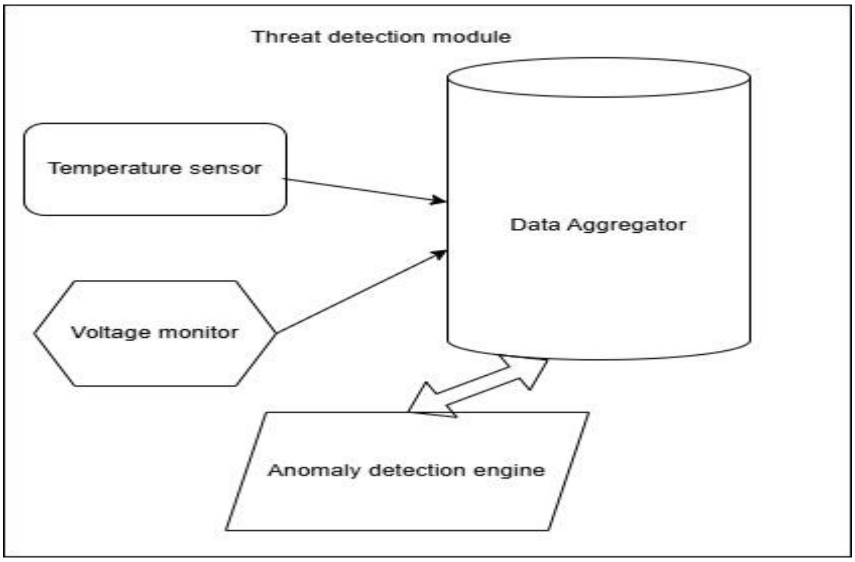
$$Z = \frac{X}{\sigma} - \frac{\mu}{\sigma}$$

Anomaly Score Calculation:

S=w1·Ztemp+w2·Zvoltage+w3·ZcurrentS=w1·Ztemp+w2·Zvoltage+w3·Zcurrent Weights (w1, w2, w3w1, w2, w3) are assigned based on parameter importance.

Working Conditions:

Operating temperature: -40°C to +125°C Power consumption: Less than 1mW/sensor



Fiqure 14: TDM architecture

8.2. Module2: Reconfiguration Engine

Thus, it does dynamic readjustments of chip configurations to mitigate such threats without compromising functionality.

Components:

Configuration Manager: Stores predefined, secure configurations.

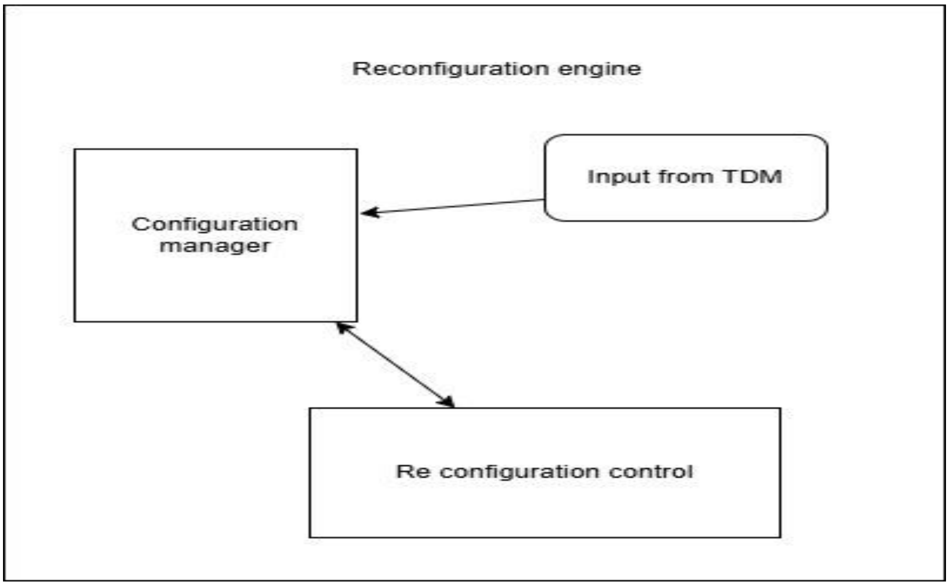
Re-Config. Controller: Applies configurations according to the threat input provided by TDM.

Mitigation Process:

1.Threat Ingestion: Processes threat feeds from TDM.

2. Configuration Changes: To stabilise the system, it adjusts the clock frequency or powers down non-critical components.

3. Sandbox Execution: Isolates the compromised component to prevent additional harm.



Fiqure 15: RE architecture.

8.3. Module 3: Dynamic reallocation

In the case of isolation, DRA improves resource consumption by delegating work from attacked components to unaffected ones.

Components:

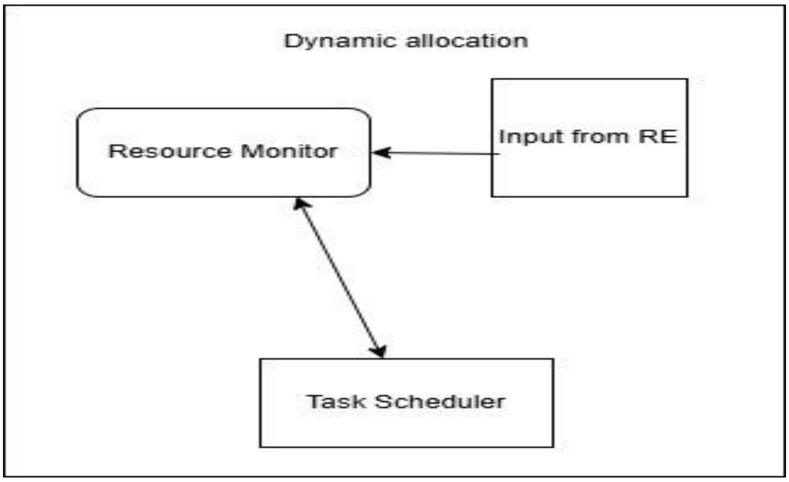
Resource Monitor: Tracks resource use across the chip.

The Task Scheduler conducts tasks from secure zones in isolated regions.

Resource Management Process:

Resource Monitoring: Continuously checks resource usage across all components.

Task Migration: It migrates isolated components from insecure to safe areas using a low disturbance task scheduler.



Fiqure 16: Dynamic allocation architecture

8.4. Module 4: Policy.

It performs the function of implementing security regulations across modules and directing their responses.

Components:

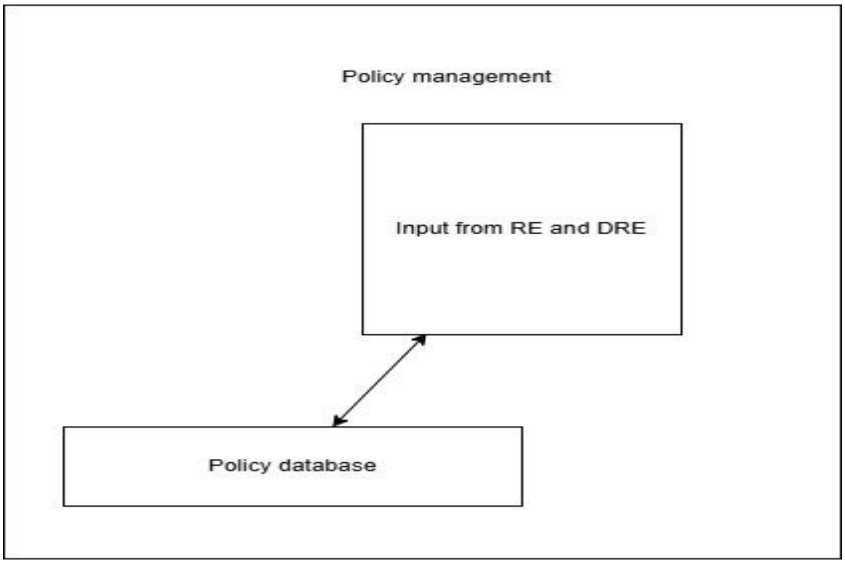
The Policy Database stores specified security policies.

Policy Enforcer: Ensures that rules are followed for threat response.

Policy Enforcement:

Policy Retrieval: Retrieves appropriate policies from the database based on the risks detected.

Policy Execution: Enables policy implementation by organizing actions in the TDM, RE, and DRA modules.



Fiqure 17: Policy architecture.

8.5. Future Directions of Improvement

There are some basic points at which further development of AHTI, in particular its effectiveness and flexibility, is needed:

AI and ML

AI-driven threat detection can enhance AHTI's ability to identify complex patterns and predict potential threats before they occur.

Scalability to IoT and Edge Devices:

As IoT devices proliferate, AHTI can be adapted to secure these endpoints by integrating lightweight security modules that operate efficiently in resource-constrained environments

8.6. Advanced Isolation Techniques:

The introduction of more advanced isolation mechanisms, including ARM Trust Zone or Intel SGX, has the potential to significantly enhance the capacity of AHTI to safeguard sensitive information by establishing a secure enclave for its operations.

8.7. Example Use Cases of Module Functionality:

1. TDM: Threat Detection Module

Example: TDM can be performed using hardware-assisted security sensors that detect in real-time anomalies in the environment where the critical infrastructure is situated. Such a simple example refers to a Hardware Security Token-HST-acting like a trusted sensor by observing an attempt of access and ascertaining the integrity of data.

2. RE (Reconfiguration Engine):

Example: The RE can dynamically change system settings in cloud data centers to prevent a detected threat. Similarly, Google Cloud's hardware-based Titanium architecture can isolate a hijacked component in such a way that service integrity remains intact (Google Cloud 2024).

3. DRA Dynamic Resource Allocation

Example: DRA has changed resources distribution in a multi-core processing environment to achieve sustained performance through a process of isolation. On the Adaptive Secure Multicore architecture, how resource demand management is done for efficiency in hardware utilization and allowing security

4. Unit for Policy Management:

The adoption of security policies for the enterprise networks is quite evident at PMU. Therefore, the inclusion of ASCA will boost the strength as it involves continuous reviews for the purpose of achieving perfection in the mechanisms of control.

8.8. Development: From Prototype to Physical Model

AHTI moved from being a prototype to a real model in appearance.

Prototype development:

Preliminary testing and validation on FPGA platforms using the modules developed at AHTI.

Provide the basic features: implement algorithms of threat detection and protocols of reconfiguration in programmable hardware.

Simulation and Analysis:

Use comprehensive simulations to assess the performance metrics of Detection Accuracy, Latency, and Power Consumption.

Test the integrations of the AI models that have further improved anomaly detection.

Tangible Configuration

Either develop Application-Specific Integrated Circuit designs or integrate AHTI into existing system-on-chip architectures suitable for deployment in commercial product environments.

Carrying out collaborative work with semiconductor manufacturers on compatibility in the nanometer-sized processing technologies.

Practical Implementation:

Deploy AHTI in data center, IoT networks, or industrial control system environments.

Performance monitoring and taking feedback to iteratively improve.

9. Challenges and Limitations

The transition to chip-level security increases numerous technical, operational, and economic issues that must be considered and solved to make new chips more secure. This section discussesvarious concerns that are; integration issues in the chip production; the dilemma of achieving both high performance and performance with higher security; and the possibility of the costs of security measures increasing.

9.1. Integration Challenges in Chip Manufacturing

The biggest challenges arising from incorporating security features into chips is in the manufacturing levels where issues to do with precision measurement, scalability and reliability certain significant levels of terminologies.

9.2. Design Complexity

The design engineers have more challenging coding when the chip contains dedicated security featuresadded to the design. Security functionalities must meet several factors including power efficiency, thermal management and layout when adopted by engineers. Such intricacy increases design risk and may also lengthen design time and improve the probability of design failure. For example, it is challenging to integrate cryptographic modules or on-chip sensors into the chip design without degrading performance when compared with unintegrated designs because significant effortmust be devoted to ensuring that interactions with primary computational tasks do not hinder these other features

9.3. Manufacturing Process Variability

The use of chips entails formation procedures that are complex and with narrow margins. Changes to process stability that may be caused by the introduction of new security mechanisms include tamper-detection circuits or secure boot modules. Changes in the manufacturing process or in the characteristics of etching, for example, can reduce the reliability of protection elements, whichcan lead to additional quality control needs

9.4. Supply Chain Vulnerabilities

This factor tends to make the manufacturing of semiconductors a global issue hence expose it to the dangers of a supply chain attack. The essence of security techniques can be rendered ineffective due to fabrication, assembly, or transportation of the system. For instance, presumably unintended and uncontrolled parties could inject hardware Trojans within the chips at uncontrolled stages of the supplychain thereby negating the desired security gains

9.5. Testing and Verification Challenges

To make as certain of these features of security it is necessary to intensively test and check. It has beenfound that conventional approaches are not effective enough for the verification of sophisticated security solutions. However, extensive testing leads to overall increased development time and costswhich can be a challenge to the time-to-market strategy

9.6. Balancing Performance with Enhanced Security

Perhaps the main problem of chip-level cybersecurity is to work at high speed and at the same time toensure protection against threats.

9.7. Resource Overheads

Security features that include cryptographic engines or other forms of machine learning-based anomaly detectors demand the underlying hardware's things like power and core cycles and even space. Frequently they can have negative effects on the performance of the whole system, mainly in the case of IoT devices or embedded systems

9.8. Latency Issues

The security measures may cause delays in core operation processes. For instance, it may be evident with the use of hardware encryption modules because the rates of data transmission slow down the encryption and decryption process. Likewise, real-time threat detection systems incorporating AI algorithms may find themselves outpaced and slowed down by high-speed data in performance- sensitive applications (Khan et al., 2021).

9.9. Compatibility with Legacy Systems

Current day security solutions frequently must interface with legacy systems which weren’t developed with these features in mind. Achieving compatibility and at the same time having the best optimized performance can sometimes pose a complicacy. If attempting to integrate security aspectsinto older chip designs, then normally there will be certain losses in terms of performance and capabilities

9.10. Trade-offs in Security and Usability

There continues to be a tension between security and convenience. Introducing strict security measures including regular authentication measures, access control measures restrict the use thus affecting the normal functioning of the system. On the other hand, focusing on the usability aspect might decrease the strength and effectiveness of security features which in turn disastrous for systemsas will exposed to several attacks

9.11. Potential Cost Implications

A third limitation has to do with the financial cost of implementing and implementing chip-level cybersecurity solutions at the chip level.

9.11.1 Increased Research and Development Costs

The development of secure chips usually entails a huge amount of expenditure in the research and development (R&D) costs. Engineering practice requires a search for new approaches, the creation ofprototypes of ideas and high experimentation. These measures add expenses at the early phases of development and prolong cycles, a burden that greatly affects small to medium enterprises

9.11.2. Higher Manufacturing Costs

We can find that integrating advanced security features will require the application of premium materials, extra fabrication processes, and specific manufacturing tools. For example, design and implementation of certain chips that may include post-quantum cryptographic modules or secure memory partitions may demand high / lithography complexities, thereby increasing the total cost of units produced.

9.11.3. Maintenance and Lifecycle Costs

Ensuring security throughout a chip’s lifecycle adds to the total cost of ownership. Measures such as secure firmware updates, runtime monitoring, and end-of-life disposal protocols require ongoing investment. Additionally, organizations must allocate resources for training personnel to manage andoperate secure systems effectively

9.12. Addressing Challenges and Limitations

Despite these challenges, several strategies can mitigate their impact and facilitate the adoption of chip-level cybersecurity measures.

9.12.1. Standardization and Collaboration

Setting up industrywide standards and encouraging stakeholder collaboration can reduce the complexity and cost of integration. Meanwhile, standards like those provided by the Trusted Computing Group give a widely accepted foundation for implementing secure hardware features. The collaborative efforts of manufacturers, academia, and governments in such initiatives will jointly reduce resources and accelerate innovation.

9.12.2. Innovative Design Automation

Advances in EDA toolsets have finally made integration possible with a small performance overhead. Automated design flows that incorporate security considerations from the very beginning could decrease complexity and boost efficiency.

9.12.3. Economic Incentives

The government and organizations may also promote the use of the chip by providing a subsidy, tax deduction, or grants for R&D activities. In return, incentivization will help cover the higher cost linked with secure chip production, enabling wider market applications.

9.12.4. Consumer Awareness Campaigns

Educate consumers and businesses about insecure hardware risks and the long-term benefits of investing in secure chips to raise demand for these technologies. Also, highlight case studies that used the technology to drive value from such a design. Chip-level cybersecurity will no longer be a nicety but become indispensable as the modern computing world must be assured from the evolution of threats. Nevertheless, there are challenges associated with this. Besides the integration complexities at chip fabrication, there is a trade-off that must be made in performance for increased security-which has big cost implications. By embracing state-of-the-art measures and working cooperatively, such limitations can be surmounted, and a road could be cleared for a more secure future of technology.

10. Conclusion

Chip-level cybersecurity speaks volumes on the sea change in computing systems. The key themes that were deduced in this research were on the need for hardware implementation since the software solution growth is on the anvil and growth in chip architecture with greater complexity. It also suggested a framework-AHTI, or Adaptive Hardware-Level Threat Isolation-which could inculcate chip architectures with the mechanism for threat detection and isolation in real time.

Key results of discussed study are:

- This would prove that on-chip characterization is effective in detecting side-channel leakages and adversarial activities in cryptographic circuits.
- Its capability in the field of electromagnetic wave vulnerabilities detection
- Discussion on the security aspect through packaging techniques like BBM, which keeps the chip safe from many attacks of physical nature.

These novel developments in chip-level security create a premise for other new advances in cybersecurity. Embedding of security in hardware will make diverse systems robust enough to cope with various kinds of emerging threats.

Chip-level security is one such necessary thing that assumes greater intricacy in cyberspace threats with time. Further research in future directions should be oriented toward refining such techniques, studying new hardware-software co-design methods, and offering mechanisms for advanced threat detection and isolation. Innovation on this front would surely promise leaps in security for computing systems in this digitally interconnected world, turning out to be the most vulnerable.

11. References

- Canavese, D., Mannella, L., Regano, L., & Basile, C. (2024). Security at the edge for resource-limited IoT devices. *Sensors, 24*(2), 590. https://doi.org/10.3390/s24020590

- CVE. (n.d.). Common vulnerabilities and exposures. Retrieved from https://cve.mitre.org/

- Dione, D., Seck, B., Diop, I., Cayrel, P., Faye, D., & Gueye, I. (2023). Hardware security for IoT in the quantum era: Survey and challenges. *Journal of Information Security, 14*(4), 227–249. https://doi.org/10.4236/jis.2023.144014

- Google | Documentation | Google Cloud. Retrieved from https://cloud.google.com/docs/security/titanium-hardware-security-architecture
- Khan, M., Hatami, M., Zhao, W., & Chen, Y. (2024b). A novel trusted hardware-based scalable security framework for IoT edge devices. *Discover Internet of Things, 4*(1). https://doi.org/10.1007/s43926-024-00056-7

- M. Reimann, Lennart , et al. "Integrity of Hardware Supply Chains | HiPEAC Vision." *Hipeac.net*, 2021. Retrieved from, https://vision.hipeac.net/cybersecurity--integrity-of-hardware-supply-chains.html
- Nagata, M., Miki, T., & Miura, N. (2022). Physical Attack Protection Techniques for IC Chip Level Hardware Security. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 30(1), 1-14. https://doi.org/10.1109/TVLSI.2021.3073946

- Sidhu, S., Mohd, B. J., & Hayajneh, T. (2019). Hardware security in IoT devices with emphasis on hardware Trojans. *Journal of Sensor and Actuator Networks, 8*(3), 42. https://doi.org/10.3390/jsan8030042

- Supply Chain Risk in leading-edge integrated circuits. (n.d.-b). https://www.ida.org/-/media/feature/publications/s/su/supply-chain-risk-in-leading-edge-integrated-circuits/d-21590.ashx
- Tomlinson, Andrew, et al. "Drivers and Barriers for Secure Hardware Adoption across Ecosystem Stakeholders." *Journal of Cybersecurity*, vol. 8, no. 1, 1 Jan. 2022,

https://doi.org/10.1093/cybsec/tyac009.

- Varshika, M L, et al. “Hardware-Software Co-Design for On-Chip Learning in AI Systems.” *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, 16 Jan. 2023, https://doi.org/10.1145/3566097.3568359
- Xi, Wei, et al. “Cyber Security Protection of Power System Equipment Based on Chip-Level Trusted Computing.” *Frontiers in Energy Research*, vol. 10, 4 July 2022, https://doi.org/10.3389/fenrg.2022.842938.
- Ye, Mengmei, et al. “TZSlicer: Security-Aware Dynamic Program Slicing for Hardware Isolation.” *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 1 Apr. 2018, pp. 17–24. https://doi.org/10.1109/HST.2018.8383886.
- Yuan, Jie, et al. “A Survey of Side-Channel Attacks and Mitigation for Processor Interconnects.” *Applied Sciences*, vol. 14, no. 15, 31 July 2024, pp. 6699–6699, https://doi.org/10.3390/app14156699.