SN Computer Science (2023) 4:36
https://doi.org/10.1007/s42979-022-01443-z

SURVEY ARTICLE

Internet of Things World: A New Security Perspective

Jaya Dofe[1] · Kriti Rai Saini[1]

Received: 29 April 2022 / Accepted: 2 October 2022 / Published online: 1 November 2022

Abstract
The Internet of Things (IoT) is changing and transforming how we interact with the physical world. IoT devices have had widespread applications in many fields of production and social living, such as healthcare, energy and industrial automation, and military application, to name a few. While we can't deny the benefits of IoT, like convenience, accessibility, and efficiency, it is a double-edged sword. The security aspect remains a significant concern in the IoT realm, especially physical attacks since there are abundant channels due to physical effects. Much research focuses on software, network, and cloud security; however, hardware security in these devices has been overlooked. Considering this motivation, in this survey, first, we provide the recent advancement in the physical attack defense techniques and extend the literature to summarize the unified countermeasures that benefit IoT devices to address the footprint and power constraints. We also discuss some open problems that need attention. Further, to defeat the IoT system from advanced hardware attacks, we proposed to use 3D integration as a key enabling IoT platform. 3D technology provides various advantages, such as heterogeneous integration, split manufacturing, and disparate technologies like MEMS sensors, making 3D integration the best choice for IoT platforms.

Keywords Hardware security · Internet of things security · Physical attacks · Side-channel attacks · 3D integrated circuits

Introduction

The internet is going through a new stage in which billions of smart objects, "things" that sense and interact with the physical world, are connected in homes, industries, hospitals, cities, farms, etc. These connected objects-the Internet of Things (IoT), are bringing about a paradigm shift in services, infrastructure, and consumer industries. It brings extraordinary possibilities for improvements in various domains like smart cities and grids, healthcare, wearable devices, robotic systems, and numerous other systems. IoT is gradually becoming an integral part of personal as well as professional lives for betterment. IoT brings improvements in connectivity, efficiency, convenience, conversations, and much more. While IoT benefits are undeniable, it is a double-edged sword. An IoT ecosystem is constantly subjected to changes and security threats at various levels—device, data transmission, and data storage within the systems and its applications.

IoT environment is a paradigm that works together, is aware, intelligent, and has a specific purpose. With the increased commercialization of this environment, society is growing more connected with the IoT infrastructure—making it more susceptible to various vulnerabilities. Security vulnerabilities in the IoT domain have intensified potential threats and attacks that can potentially compromise critical infrastructures and national security, causing physical and financial losses.

McAfee's quarterly threat report exposed 176 new cyber-threats every minute [1]. Mirai-botnet-based recent DDoS attack on low-cost IoT devices infected over 2.5 million devices within just four months [1]. FDA found St Jude Medical's implantable cardiac devices have vulnerabilities [2] and recalled 465,000 Pacemakers. In [3], the authors demonstrated an attack using popular Philips Hue smart lamps that can impact the IoT infrastructure on a mass scale. Side channel attacks on devices like smart card and mobile phones are rising

This article is part of the topical collection "Smart and Connected Electronic Systems" guest edited by Amlan Ganguly, Selcuk Kose, Amit M. Joshi and Vineet Sahula.

✉ Jaya Dofe
jdofe@fullerton.edu

Kriti Rai Saini
kritirais@csu.fullerton.edu

[1] Electrical and Computer Engineering, California State University, Fullerton, 800 N State College Blvd, Fullerton, CA 92831, USA

[4, 5]. Another prominent example affecting billions of IoT devices is the Bluetooth low-energy communication protocol could potentially expose user data [6]. This protocol is used in many wearable and industrial IoT devices.

This scale of the impact is potentially expected to grow extensively with the increasing volume of IoT devices (29 billion in 2022). Traditionally, IoT devices allocate resources like energy and computation for the functionality, and incorporating security becomes very challenging [7]. With the short time-to-market and fierce competition among companies, security has become an afterthought [8] and has not been prioritized as a crucial metric. The security aspect is the primary concern in the IoT realm for deployment. Unlike in the traditional internet, where threats affect the digital world, attacks on IoT would directly impact the physical world. IoT's future will rely on the ability to secure hard-to-secure, resource-sparse devices effectively. As IoT solutions are becoming prevalent in day-to-day life, attackers have found new opportunities to exploit the lack of built-in security.

This work addresses unified countermeasures for side-channel attacks, specifically for IoT devices. As the existing countermeasures for the physical attacks in IoT are limited to the applications, algorithms, platforms, and hardware specifics, there is a need to rethink the trusted environment to incorporate the security against these attacks. With this motivation, we propose to utilize 3D integration [9] for building the IoT devices as it offers a natural defence against physical attacks, heterogeneity, small form factor, and reduced power dissipation.

To the best of our knowledge, this is the first survey that addresses unified countermeasures in IoT and also describe the 3D integration features that can benefits to design reliable and secure IoT devices. The rest of this paper is organized as follows. "Preliminaries" briefly introduces security concerns in IoT, Three-dimensional (3D) integrated circuits in context to IoT, and hardware attacks. "Generic Countermeasures Against Side-Channel Attacks" discusses generic countermeasures for the selected side-channel attacks. In "Resilience Against Physical Attacks in IoT" , the defense methods specific to IoT against SCA are introduced. The unified approaches unique to the SCA attacks are discussed in "Unified Countermeasures for IoT". "3D Integration as an Key Enabling Technology for IoT Devices" provides the different aspects of utilizing 3D integration for IoT systems and approaches to designing secure IoT devices using 3D ICs. Finally, "Conclusion", concludes the paper.

Preliminaries

This section provides basic knowledge about the security concerns in the IoT realm and existing hardware attacks that can threaten the IoT infrastructure. It also provides background knowledge for the reader associated with 3D integrated circuits to understand section 6 effectively.

Security Concerns in IoT

As argued by many researchers, IoT will be the main component of the next era in computing. The network of smart devices-internet-enabled embedded systems is not limited to sensors and actuators but is a wide complex system from home appliances to smart cities and hospitals. The current state of IoT devices, for short, is challenging traditional security protocols. Many IoT designs prioritize keeping devices small in size, battery, and computation power, making traditional security methods unsuitable. It is currently causing a tug of war between having good security on your device or having a good performance at a low price. This fray in security affects IoT devices to be vulnerable to side-channel attacks. There are many published research that discussed IoT security and challenges facing IoT devices [10–12]. Most of the survey papers focus on secure IoT infrastructure creation and implementation, authentication, trust management, and attack in different IoT layers. Also, the survey related to the lightweight cryptographic algorithms is presented in [13, 14] for IoT applications. However, there is a lack of surveys that mainly discuss the side-channel attacks and respective countermeasures in the IoT domain.

The very nature of IoT devices means data are constantly being transmitted, processed, and collected in the cloud. Research shows many IoT infected devices have little to no security protections [15]. IoT can become more secure through cryptography for communication between the physical and cyber worlds. Some IoT devices have embedded cryptographic cores for authentication and information processing. However, a prominent attack method-physical side-channel attack (SCA), that breaks an encryption system's security by exploiting the information leaked from the physical devices is a rising threat in IoT [16, 17]. Current IoT studies show that adversaries can easily acquire side-channel information, which is hard to detect because leakages are inevitable [18]. Side channels in IoT systems may arise from timing information, sensor data, or traffic rates between devices prevalent in our everyday lives. Further, having easy network connectivity as an intrinsic feature, these IoT devices have become lucrative targets for attackers.

Hardware Attacks

The emerging hardware threats arise because of globalized IC supply chain. There are multiple stages within the supply chain that can be manipulated by potential adversary in certain ways to perform the attacks. These diverse hardware attacks can be broadly classified in the following categories.

IP Piracy

Intellectual property (IP) piracy is the illegal or unlicensed usage of IPs. The semiconductor industry increasingly relies on a hardware IP based design flow, where reusable, pre-verified hardware modules are integrated to create a complex system of intended functionality. An attacker can steal valuable hardware IPs in the form of register-transfer-level (RTL) representations ('soft IP"), gate-level designs directly implementable in hardware ("firm IP"), or GDSII design database ("hard IP"), and sell those IPs as genuine ones. Hardware IP reusing in Systems-on-chip (SoCs) design is a prevalent practice in the silicon industry as it reduces design time and cost dramatically. The IP piracy attack can occur at various stages in the IC supply chain [24]. The potential IP piracy attackers could be designers, third-party IP (3PIP) vendors, and SoC integrators at the design, synthesis, and verification stages. In the fabrication stage, an untrusted foundry may overbuild the IP cores and sell them under a different brand name to make a profit. Hardware IPs obtained from untrusted third-party vendors can have various security and integrity issues. An adversary inside an IP design house can deliberately insert a malicious circuit or design modification to compromise system security. Various design and algorithmic level robust hardware-based security primitives are proposed in [26] to protect the modern semiconductor supply chain.

Reverse Engineering

The process of identifying an IC's structure, design, and functionality is known as reverse engineering. Different types of reverse engineering include product teardowns, system-level analysis, process analysis, and circuit extraction. One can use reverse engineering to (1) determine the device technology, (2) extract the gate-level netlist, and (3) infer chip functionality. Several techniques and tools have been developed to facilitate reverse engineering. Traditionally, it has been a legal method for teaching, assessing, and evaluating mask work processes under the US Semiconductor Chip Protection Act. Reverse engineering, on the other hand, is a two-edged sword. Reverse engineering techniques could be used to pirate ICs. Reverse engineering attacks can be carried out at many levels of abstraction in the supply chain, depending on the attacker's goals [25].

Counterfeiting

A counterfeit semiconductor component is an illegal forgery or imitation of the original component. Counterfeiting is often performed by one of the many entities in the semiconductor supply chain, including new product vendors or secondary (recycled) IC vendors. In recent years, because of technological advances in 3D packaging, fake ICs are hard to distinguish from real ones. Counterfeit ICs are a serious threat to the IC supply chain. Computers, telecommunications, automotive electronics, and military systems are all affected by counterfeiting attacks. As counterfeiters get more sophisticated, counterfeit chips are becoming more difficult to detect.

Hardware Trojans

One of the most insidious methods of attacking a circuit is maliciously modifying its hardware. In simple words, a hardware Trojan (HT) is created by discreetly inserting hidden functionality into a Hardware Design. This insertion can occur at any stage in a production path and could have devastating effects on the final design [25]. Such Trojans can have a variety of functionality, ranging from denial-of-service that gives designs a controllable kill switch to hidden data leaks that can leak sensitive information. HTs are a direct threat to already vulnerable IoT. Unlike software Trojans, HTs cannot be removed simply by a firmware update, so they are very harmful and challenging to remove. Consequently, HT detection is a vital step to guarantee the chips used in IoT are authentic-meaning they only do what they intend to do, nothing less, nothing more. The simple structure of HT is shown in Fig. 1.

Side Channel Attacks

In the hardware security domain, one of the most prominent and influential tools in the hands of adversaries is a physical attack. Physical attacks are the type of attacks where the attacker has access to the targeted device. These attacks can help the adversary to intrude into the IoT. Physical attacks can be classified into two major categories—invasive vs. non-invasive and active vs. passive. Invasive attacks require tampering with the device under attack, while non-invasive don't. If the adversary actively influences the device's behavior, then it is an active attack, or they passively observe leaking information. With mobile devices, the scope of side-channel attacks changed dramatically. Early on, attackers

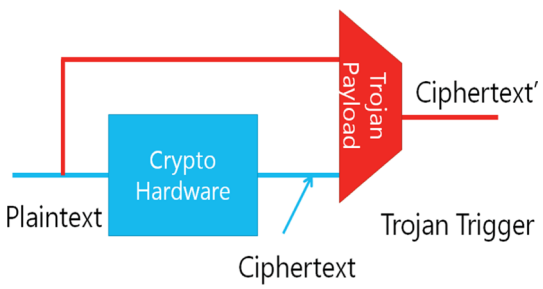

Fig. 1 Simple example of hardware Trojan

needed access to the physical device. However, in the IoT, these attacks can be made remotely.

Side-channel analysis (SCA) attacks [16, 17, 27] aim to retrieve the secret key in cryptosystems by analyzing physical parameters like power, delay, or electromagnetic emission of the IC which runs security-critical applications.

Power Analysis Attacks Kocher et al. introduced power analysis attacks that exploit implementation of cryptographic algorithm [28]. Power-based SCA attacks are extensively studied that exploit the correlation between the power consumption of the cryptosystem and the hypothetical crypto key to retrieve the secret key applied. There are three common power analysis attacks: simple, differential, and correlation power analysis.

Timing Attacks This attack was also invented by Kocher [29] in 1996. It exploits the data-dependent execution time to reveal secret information. Cryptosystems take slightly different execution times to process different inputs because systems use conditional branches in the algorithm and performance optimization.

Electromagnetic Side-channel Attacks Electromagnetic side-channel attack [30] is also an important information source and is available when any system operates. This attack is non-invasive and does not need device tampering to measure the side-channel leakage. Electromagnetic SCA is becoming popular in the IoT paradigm because of the easy availability of EM probes to conduct the attack. This attack is more prominent in IoT as adversaries do not need physical access to devices compared to power SCA.

Fault Attacks A fault attack is an attack on a physical, electronic device (e.g., smartcard, HSM, USB token) which consists of stressing the device by an external mean (e.g., voltage, light) to generate errors in such a way that these errors lead to a security failure of the system. Fault attacks can be performed by an adversary to either force the device to bypass security mechanisms or to extract secret information using faulty outputs. The work [31] shows that a fault attack can break the advanced encryption standard (AES) implementation with only a pair of fault-free and faulty ciphertexts. One of the most common ways of performing the fault attack is by manipulating the external clock or power inputs or using electromagnetic disturbances. This type of attack is easy to perform as it needs a motivated attacker with mid-level expertise and low-cost equipment. Thus, these fault injection techniques should be considered as a severe threat to IoT systems.

Thermal Side-channel Attacks This type of side-channel attack is typically non-invasive. The temperature traces are collected from the device under attack to extract the secret information. Thermal attacks are not the most common because of the noise associated with the measurement. However, in the context of IoT devices, its distributive and remote nature provides easy access to capture thermal leakage on any node. Aljuffri et al. propose a thermal attack by maneuvering correlation power analysis and deep learning side-channel attack to perform a thermal attack [32]. This work proved that thermal side-channel attacks are possible, and IoT devices need to be safeguarded against them.

3D Integrated Circuits

For the last fifty years, Moore's Law lies at the heart of high rates of technological change observed in the computer, communication, and software industries. It has accurately predicted the doubling of device density within Integrated Circuits (ICs). However, as conventional channel length scaling continues beyond the 10nm technology node, power and performance gains of scaling are becoming incommensurate. The semiconductor industry is exploring More-than-Moore technologies to overcome the disparity [19].

One such more-than-Moore technology is three-dimensional (3D) integration. 3D integration and similar forms of die-level integration provide novel design methodologies to increase transistor density, reduce interconnect distances, and integrate additional system components. In 3D ICs, active devices are placed in multiple planes (or tiers) of semiconductor dies and are interconnected vertically. 3D integration also facilitates combining multiple different process technologies within a single heterogeneous IC (Fig. 2).

3D SiP Using Wire Bonding

In system-in-package (SiP) technology, multiple pre-fabricated dies are encapsulated within the same package. Multiple stacked tiers in a package are connected using wire bonding [20]. Wire bonds are placed around the perimeter of each die to achieve die-to-die connections and die-to-package connections. This technology is used in the IoT domain for

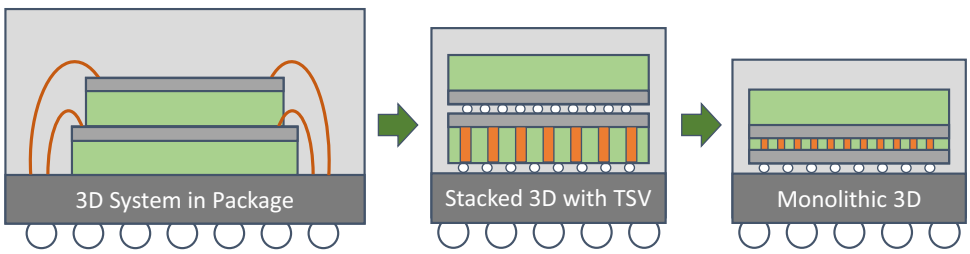

Fig. 2 3D integration approaches

sensing applications, where multiple heterogeneous silicon tiers are stacked, and integrated [21].

Through Silicon Vias

3D integration through silicon via (TSV) technology has become a promising solution for realizing high-density packages and high-speed integrated circuits [22]. In TSV-based 3D ICs, the communication between multiple tiers (planes) is achieved by high-density TSVs. TSV technology is the heart and most important key enabling technology of 3D integration. TSVs can be fabricated in several ways, including via-first (before Front End Of Line (FEOL) processing), via-middle (after FEOL processing, but before BEOL processing), or via-last (after BEOL processing).

Monolithic 3D ICs

Monolithic 3D ICs are fabricated using sequential fabrication that begin with a base wafer and then additional layers of crystallized silicon, metalized layers and active as well as passive circuitry are added. The layers are interconnected using fine-pitched Monolithic Inter-tier Vias (MIVs) [23]. It enables ultra fine-grained vertical integration since the MIVs are fabricated using a similar process as the regular local metal vias. There are primarily three design styles for M3D ICs: block-level, gate-level, and transistor-level

Generic Countermeasures Against Side-Channel Attacks

For power-based side-channel attacks, the main objective of countermeasure is to make the power consumption of a device as independent as possible to the intermediate values of a cryptographic algorithm. The general countermeasures for AES include either hiding or masking the data. The goal of hiding [33, 34] is to cover up a correlation between the power traces and the intermediate values. Hiding deceit power traces by randomizing power consumption in a device or flattening the power consumption to make all operations look similar. For the masking technique, the goal is to conceal data by adding/multiplying random numbers to the intermediate values in the encryption process to ward off potential attackers [34]. The challenge becomes implementing the countermeasures without reducing the speed, increasing the power consumption, or increasing the area of the cryptographic algorithm beyond reasonable limits.

Some of the countermeasures proposed against electromagnetic SCA include signal strength reduction techniques like shielding or signal information reduction using noise insertion [35]. Recently, Das et al. used white-box modeling [30] to develop a low-overhead generic circuit-level countermeasure against electromagnetic side-channel attacks. Electromagnetic Equalizer is proposed in [36], where on-chip power grid impedance is adjusted to flatten the current waveform.

A common approach to protecting the cryptographic core from timing attacks is to ensure that its behavior is never data-dependent. The sequence of cache accesses or branches does not depend on either the key or the plaintext. Paper [37] proposed to perform rescheduling of instructions so that each encryption round will consume constant time independent of the cache hits and misses. Another way is to induce noise in all events to prevent exploitation of timing information [38]. One beneficial way to make time attacks challenging is to desynchronize the execution of sensitive parts using random waits, dummy instructions, jitter on clocks, etc., as much as possible. The most cost-effective approach against FA attacks is modifying the cryptographic device's design to detect injected faults. Traditional fault detection methods for cryptosystems exploit information redundancy, spatial redundancy, or time redundancy to detect faults [39]. Survey paper [40] presented countermeasures against fault injection attacks, including algorithmic changes, sensors and shields, and fault detection or correction techniques.

Resilience Against Physical Attacks in IoT

Side-channel information may arise from timing information, sensor data, or data traffic prevalent in everyday lives. Current IoT studies show that adversaries can easily acquire side-channel information, which is hard to detect because leakages are inevitable hence tackling these attacks is of utmost importance [16–18]. The IoT devices are intended to be small and convenient, and traditional, sophisticated security protocol implementations are unacceptable as used in the existing literature. The traditional countermeasures against power attacks reduce the signal to noise ratio, which may be expensive to implement for IoT lightweight applications. The attenuated signature AES is proposed in [17] to resist power-analysis attacks with reduced overhead. This approach implements AES in a signature attenuating hardware, making the variations in AES current highly suppressed. A false key-based AES engine that utilized wave dynamic differential logic (WDDL) is presented in [41] as a countermeasure against CPA attacks. The false round keys generated by the constant intermediate value added to the original round keys are added to the original round keys to disguise the correlation between the dynamic power consumption profile and the actual key. As the area and power overhead of the proposed technique is negligible compared to the unprotected AES, this method fits IoT devices. Kai Yang et al. presented a flexible FPGA virtualization approach [42]

to prevent the FPGA-based system from timing attacks. This method's masking and architectural diversity make it challenging to obtain the required information to carry the successful timing attacks.

In recent years, the adiabatic logic circuit [43] has evolved as a promising solution to design cryptographic circuits for IoT applications because of their energy efficiency and resilience to power-based side-channel attacks. In work [43, 44], authors proposed to use novel single-rail Clocked CMOS Adiabatic Logic (CCAL) to design PRESENT-80 S-box. The study further explored the resistance of the CCAL logic against CPA. Power-based side-channel instruction-level monitoring [45]—side-channel disassembler that tracks the target device's control flow and enforces decoupled monitoring. Chakraborty et al. developed a hardware-software framework called hardware-aware software timing-attack evaluation to detect the timing side-channel vulnerabilities and malware [45, 46] in runtime. Bai et al. introduced a low-cost external monitoring circuit board to detect anomalous behavior in IoT systems to monitor power, and electromagnetic traces [47]. A comprehensive defense and attack analysis of electromagnetic side-channel attack is presented in [48]. Paper [49] presents a very extensive overview of the approach to developing SoC level security measurement and estimation in IoT applications regarding Power Side-Channel Analysis. In the paper [50], the authors demonstrate the AM signal obtained from the capacitance value in real-time can leak to the outside world in the form of EM radiations. They proposed the technique to alter the accessible capacitance in a single-phase SC dc-dc converter to hinder the side channel. Dynamic IR drop solver ANSYS RedHawk is used in [51] to detect the root cause of EM leakage before manufacturing to minimize the leakage after chip fabrication. Power side-channel leakage assessment framework is presented in [52] that performs a fast, automated, and technology-independent pre-silicon evaluation at the RTL level.

The literature presented above is summarized in Table 1 and is representative of the defense approaches for three primary physical attacks-power, timing, and electromagnetic analysis discussed above. It covers a variety of methods, from standalone devices to comprehensive frameworks for SoC-level system security, and details about the simulation, hardware platform, and security metrics. However, the open questions that the research community is still struggling with are - how does one define the security of the chip and system as a whole? Are there any unified metrics that the community can use? Also, how do we deal with emerging threats inevitable in IoT? Can artificial intelligence be a friend in designing security methods against physical attacks? What is the best way forward?

Unified Countermeasures for IoT

As mentioned earlier, IoT devices are a constrained power budget, so it is imperative to design unified countermeasures that can address multiple attacks simultaneously.

An embedded trusted platform module is proposed in [53] to address a variety of side-channel attacks, including power, timing, fault, and power-glitching attacks. This work makes use of a quantized controller as shown in Fig. 3, that sits between a security-critical core and the rest of the system. A controller uses integrated decoupling capacitors to create uniform power and timing footprints. The inherent implementation of the controller allows control where the computer processor receives its power. During security-critical processes, it can switch the processor's power source from the main power rail to the controller's internal storage capacitors, invisible to attackers. This allows the power traces to become unreadable with the proper implementation. A core design is to leverage on-demand isolation to allow side-channel protection from a software-level decision, making the method effective in real-time changes to accommodate IoT design.

The paper [54] proposes strategies that could be used for the design specific targets, specifically for lightweight IoT applications. The first method is to use a maximum distance separable linear layer to incorporate diffusion and fault space transformation that helps to protect against classical cryptanalysis and differential fault attacks. The second strategy exploits modified transparency order metrics to select from different S-box implementations that guide the adequate refresh rate for the mask to defeat the differential power attacks with the same resistance. Cipher-dependent nibble-wise shuffling was proposed in their third method to enhance the side-channel resistance.

Recently, Das et al. used white-box modeling [30] to develop a low-overhead generic circuit-level countermeasure called STELLAR - Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing against electromagnetic and power side-channel attacks shown in Fig. 4. This approach utilizes the local lower-metal layers to route the crypto core with a signature suppression circuit, reducing the leakage reaching the top metal layer.

In the paper [55], the authors proposed a concurrent software approach to resist the side-channel and fault attacks. This countermeasure is generic and applicable to any byte-size cipher. It utilizes larger data path of 32-bit or 64-bit Microcontroller units to carry out parallel byte-sliced encryption. As depicted in Fig. 5, the same data byte D1 is cloned four times and encrypted using a fake key (K_F) twice and a true key (K_T) twice. This arrangement will generate the correlated algorithmic noise to protect against SCA as both computations operate parallel on the

Table 1 Categories of countermeasures against physical attacks in IoT with details of algorithm, security metric, hardware used and method description

Attack type	Reference paper	Algorithm used	Security analysis metric	Hardware used/simulation	Method details
Correlational power analysis	[17] - 2017	AES	Minimum Traces to Disclosure	Simulation	Use of attenuated signature hardware to suppress current variation
Correlational power analysis	[41] - 2017	AES	Test vector leakage assessment p (TVLA)	130 nm CMOS technology p node simulated in Cadence	False key-based AES engine that p utilized wave dynamic differential logic
Timing analysis	[42] - 2018	RSA	t-test timing leakage assessment	FPGA	Flexible FPGA virtualization approach
Power analysis	[45] - 2019	ATMega 328P instructions	Dissect accuracy	AVR microcontroller	Side-channel disassembler for real time IoT
Power analysis	[43] - 2021	PRESENT-80 S-box	Normalized energy deviation normalized standard deviation	Simulation	Single-rail clocked CMOS Diabatic logic circuit to design PRESENT-80 Sbox
EM side-channel analysis	[50] - 2021	AES	TVLA	Cadence and Scilab simulation	Modify the capacitance value of AM signal to deter the attacker
EM side-channel analysis	[48] - 2022	AES	Success rate and machine learning modeling success rate	FPGA and Arduino	A comprehensive defense and attack analysis
Power Analysis	[49] - 2022	AES	JS divergence	Simulation	Approach to developing SoC level security measurement and estimation
EM side-channel analysis	[51] - 2022	AES	Partial guessing entropy	ANSYS RedHawk and Custom Chips 40 nm CMOS	Use of Dynamic IR drop solver ANSYS RedHawk to detect the leakages before manufacturing
Timing analysis	[45, 46]-2019, 2022	RSA	Maximum timing difference	BOOM Architecture	Hardware-aware software timing-attack evaluation to detect the timing side-channel vulnerabilities
Power analysis	[52] - 2022	AES and PRESENT	TVLA	FPGA	Leakage assessment framework at register transfer level

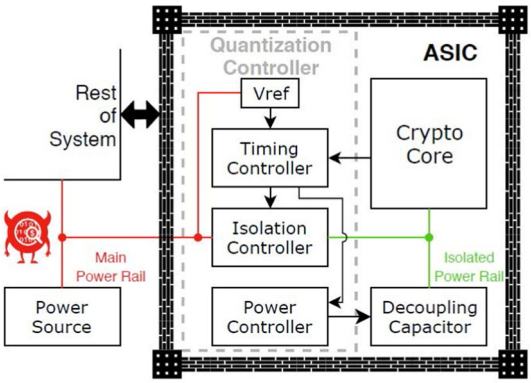

Fig. 3 Secure processor using quantization controller [53]

same data but using two different keys. The same approach helps detect the fault injection attack because of duplicated results from both the fake and correct key computation to detect any anomalies.

In study [56, 57], authors proposed to integrate a dynamic masking technique with an error control code-based error deflection mechanism to thwart power analysis and fault attacks simultaneously. This method generates the masking vector from the intermediate state register in runtime, which changes over time. This arrangement fails the power model modification according to a guessed masking vector.

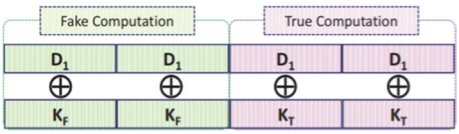

Fig. 5 Combined SCA and FA countermeasure [55]

An on-chip waveform measurement (OCM) technique is exploited in [58] that protects against physical side-channel attacks. The on-chip latch comparator resonator senses the proximate antennas using magnetic coupling. The OCM captures the voltage substrate waveforms when a laser hits the substrate detecting the fault attacks. When OCM detects the antenna or laser presence, the cryptographic chip forces are immediately halted or transitioned to a dummy state. A framework–hardware aware software timing-attack evaluation is presented in [46] to detect the timing side-channel vulnerabilities and malware in runtime. We summarized these papers in Table 2.

Unified countermeasures benefit the IoT systems' security considering the constraints. However, while designing the combined security approaches, one should analyze their impact on other attacks as they are not always orthogonal.

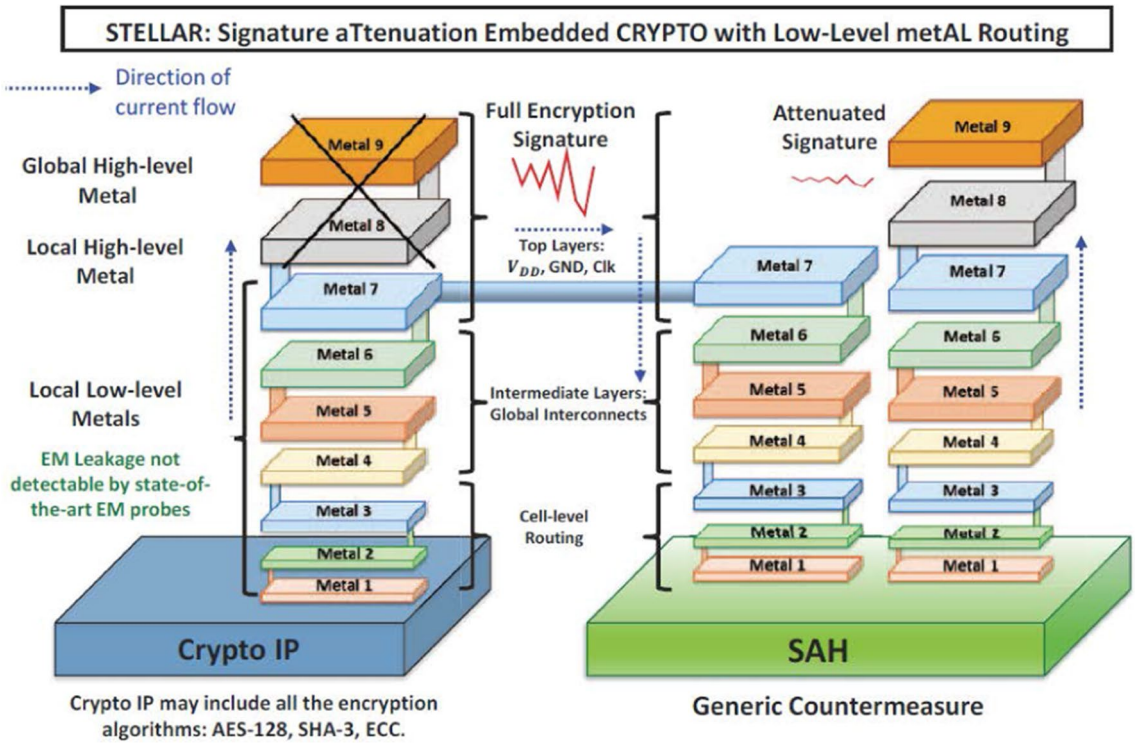

Fig. 4 Stellar technique for side-channel protection [30]

Table 2 Unified countermeasures against physical attacks in IoT

Reference paper	Attack type	Details
[53] - 2017	Power, timing, fault, and power-glitching attacks	Embedded trusted platform - quantized controller in between security core and rest of the system
[54] - 2019	Classical and biased fault attacks and power analysis attacks	Target independent strategies
[30] - 2019	Electromagnetic and power side-channel attacks	Generic circuit-level countermeasure -use of local metal to route crypto
[55] - 2019	Side-channel and fault attacks	Parallel byte-sliced encryption using fake and correct keys
[56] - 2020	Power analysis and fault attacks	Dynamic masking technique with an error control code-based error deflection
[58] - 2019	Electromagnetic and power side-channel attacks	Use of on-chip latch comparator resonator
[46] - 2022	Timing and malware attacks	Hardware-software framework

3D Integration as an Key Enabling Technology for IoT Devices

3D integration is an emerging technology to ensure the growth in transistor density and performance expected for future ICs. 3D integration has attracted significant attention to developing diverse computing platforms such as high-performance processors, low power systems-on-chip (SoCs), and portable devices during the past two decades. However, 3D integration is not used in IoT devices yet much.

3D Heterogeneous Integration—More than Moore Technology

3D ICs include several tiers that are stacked together in the chip layout and provide a promising paradigm for IoT devices. 3D heterogeneous integration has great potential to design more complex systems such as IoT. 3D technology provides various advantages such as heterogeneous integration [59], split manufacturing [60, 61], disparate technologies for IoT like MEMS sensors [62], etc.

3D Integration for Reliability

Electrostatic discharge (ESD) failure in the nanometer regime is considered the most devastating reliability concern. In research work [63], Wang et al. designed a non-traditional above IC nano crossbar array for ESD protection using 3D heterogeneous integration. The nano crossbar ESD device is built into the back-end of CMOS, i.e., above-IC. Hence, this approach does not utilize any silicon area indeed reduces Si die area traditionally consumed by Si solutions for ESD protection. The same research also designed a novel vertical magnetic-cored inductor with an integrated stacked-via magnetic core made of nano particle powder for RF ICs.

Split Manufacturing

Split manufacturing protects IC design companies against piracy of their intellectual property (IP) by third-party manufacturing facilities [64]. Leading fabless semiconductor companies such as AMD and research agencies such as Intelligence Advanced Research Projects Agency have proposed split manufacturing. In split manufacturing, a design house (with a low-end, in-house, trusted foundry) fabricates the Front End Of Line (FEOL) layers (transistors and lower metal layers) in advanced technology nodes at an untrusted high-end foundry [65]. 3D integration has been successful in splitting 2D IP modules within 3D ICs [66] without thinking security aspect.

Energy Harvesting Using Solar Cell

Many IoT devices will be battery operated or self-powered. Energy harvesting is one technique that shows the potential to improve energy efficiency in IoT devices. Solar cells are the common option for providing a source of power to these devices. 3D integration provides an opportunity to use alternate forms of energy like solar, electromagnetic, thermal, etc., because of its heterogeneous nature.

Wireless 3D ICs

The idea of 3D integration to construct highly-integrated heterogeneous IoT chips has not yet been realized. The primary reason is the cost of manufacturing and limited EDA support for designing 3D chips. Fletcher explored a low-cost alternative to replace the bulky TSVs using wireless vertical links [67]. With the proposed approach, existing 2D fabrication processes can be used as it is and for all technologies. In wireless 3D ICs, the data is communicated to different tiers via an electromagnetic coupling instead of physical channels as in TSV-based 3D ICs. The authors utilized a low-energy Inductive coupling link (ICL) transceiver for data and power transmission using spike-latency encoding

to reduce the energy consumption of existing ICL ideal for IoT devices (Fig. 6).

Security Perspective

The fact that security is not the main functionality of an IoT device means that even a lesser portion of its computing power is available for the security. Security measures implemented in traditional computers, such as cryptography, present a challenge in this context when applied to IoT devices. Further, due to the heterogeneity of devices, the power budget may not be enough to implement sophisticated security features. Many studies showed that side-channels in IoT devices are easy to obtain and hard to defend against; hence, addressing the side-channel leakage is crucial. Although various threats challenge IoT security, the root of trust starts from the hardware [68]. Without trusted and authenticated IoT devices, high-level approaches cannot stop these attacks. As many IoT devices are small in size, low in computation capabilities, and powered by low capacity batteries, we need to rethink the trusted environment for IoT.

3D integration provides the following benefits for their application in the IoT paradigm. The overview of the 3D structure for IoT devices is shown in 6.

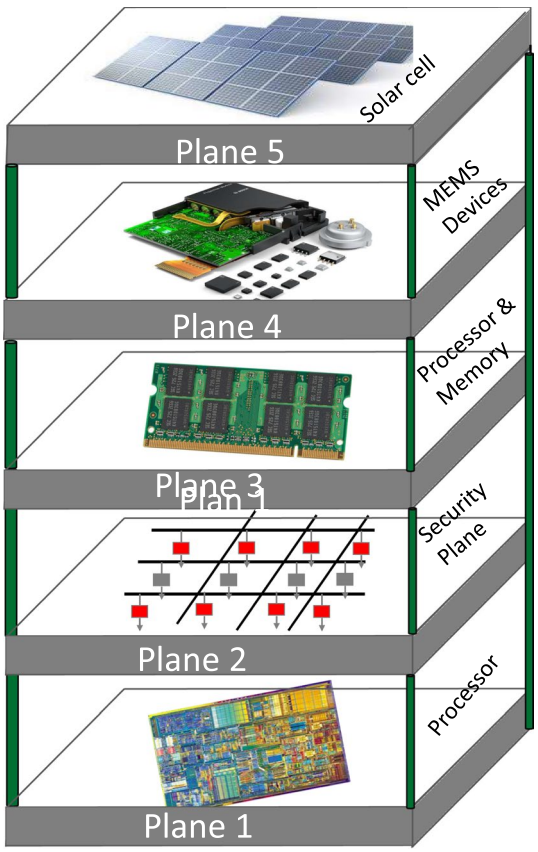

Fig. 6 3D structure for IoT devices

Separate Security Plane Using 3D Stack

Sherwood et al. [69] introduce a novel architecture using a separate control plane, stacked using 3D integration, that provides security mechanisms to protect the design from explicit and implicit channels of information leakage. 3D will provide much higher integration, bringing multiple CPUs, memory blocks and cryptographic engines together. Hence the side channel information will become noisy, making the attacks very challenging. If the control (security) plane is placed in the middle stack of 3D IC for fault prevention, it will be unlikely to inject reliable faults to carry out successful fault attacks.

Shielding Side-Channels with 3D Stacking

In this approach, the authors utilize intrinsic characteristics of the 3D chip and dynamic shielding to hide the security-related activities on the chip [70]. They propose to use a micro-controller unit to produce complementary activity patterns dynamically thwarting side-channel information leakage. This method work with on-chip power budget and thermal management to minimize the power overhead by controlling activities in each layer. When the functional unit is active and utilizes more power, the noise generator will also increase the power counteracting the impact.

Intrinsic Power Distribution Network (PDN) Noise to Defeat SCA in 3D ICs

In this work, the authors demonstrate that 3D PDN introduces noise to the power profile of the crypto unit that depends on the load switching activities, PDN topology, and crypto module deployment in the 3D chip. Using real 3D PDNs and through-silicon-vias (TSVs) models, they performed quantitative experimentation to exploit intrinsic noise to defeat the side-channel attacks [72, 73]. The overview of the method is shown in Fig. 7. The crypto unit is divided into multiple sub-units (e.g., four). Each sub-unit is driven by a local supply voltage V DDi (i = 1, 2, 3, 4). We utilize a crossbar to connect the local VDD pins with the PDN nodes close to four power TSVs. Due to the non-uniform switching activities in every 3D plane, each TSV passes a unique voltage from other 3D planes to the plane carrying the crypto unit. The effect of parasitic resistance and capacitance (RC) of the metal wire between the power grid and the local VDD pin further increases the variance of the four VDDs for the crypto unit.

Camouflaging in Monolithic 3D ICs

Yan et al. [71] proposed a logic camouflaging for 3D ICs, more specifically for monolithic 3D ICs, to enable

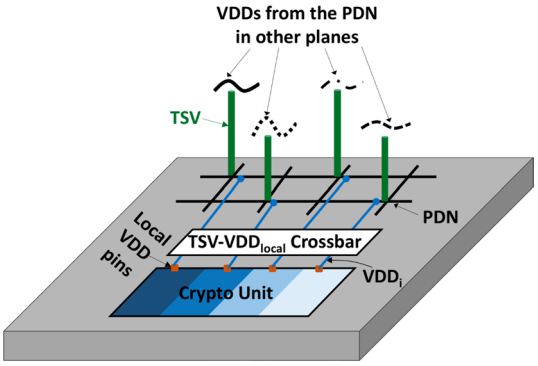

Fig. 7 Countermeasure against CPA attacks in 3D ICs

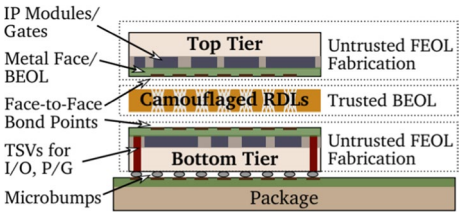

Fig. 8 3D split manufacturing with Camouflaging [74]

ultra-high density device integration. In work, standard cell libraries are created and characterized to analyze the performance of monolithic 3D ICs. Further, the authors used these libraries to design a camouflaged lightweight block cipher–SIMON and several academic benchmarks. This method is notable because it helps thwart reverse-engineering attacks with low overhead compared to classical 2D-centric camouflaging. For example, in the camouflaged 2D SIMON implementation, area, wirelength increased by 21.1%, 11.3%, and 7.4%, respectively, compared to the conventional 2D implementation. In contrast, in camouflaged monolithic 3D, the area, wirelength, and power are reduced by 37.7%, 15.7%, and 22% compared to 2D design.

Integration of Split Manufacturing and Camouflaging into 3D CAD Flow

The idea of combining the split manufacturing with camouflaging for security-driven 3D CAD flow is described in article [74]. Their scheme for 3D integration is focused on face-to-face 3D ICs and utilizes TSVs for external connections and additional metal redistribution layers (RDLs) for internal connections. These additional obfuscated layers (camouflaged RDLs) as shown in Fig. 8 protect against reverse engineering attacks thwarting IP piracy at untrusted foundries.

Conclusion

The emerging technological space is growing with the Internet of Things (IoT). IoT is revolutionizing our lives by bringing the physical and digital worlds together. While creating exceptional benefits like convenience, accessibility, and efficiency, IoT is also causing significant concerns in the security realm. Security vulnerabilities in the IoT domain are threatening critical infrastructures and national security.

Many IoT designs prioritize keeping their devices small in size, battery, and computation power, making traditional security methods unsuitable. We must rethink the trusted environment for IoT devices that provides lightweight solutions and enhanced security. This paper highlights the countermeasures for single and then explores unified defense methods for physical attacks in IoT applications. Further, we explore the potential of 3D integration as a key enabling technology for IoT devices. It provides various advantages, such as heterogeneous integration, split manufacturing, and disparate technologies for IoT like MEMS sensors, making 3D integration the best choice for IoT platforms.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. "Mcafee labs threats report." https://www.mcafee.com/April2017ThreatsReport, April 2017.
2. Arghire I. St. jude medical recalls 465,000 pacemakers over security vulnerabilities. https://www.securityweek.com/st-jude-medical-recalls-465000-pacemakers-over-security-vulnerabilities, 2017.
3. Ronen E, Shamir A, Weingarten A.-O, O'Flynn C. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In 2017 IEEE Symposium on Security and Privacy (SP),2017; pp. 195–212.
4. Kim T. W, Kim T. H, Hong S. Breaking Korea Tansit Card with Side-Channel Analysis Attack-Unauthorized recharging-, 2017.
5. Genkin D, Pachmanov, L, Pipman, I, Tromer E, Yarom Y, ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, (New York, NY, USA), p. 1626-1638, Association for Computing Machinery, 2016.
6. Antonioli D, Tippenhauer N. O, Rasmussen K. B, Payer M. Blurtooth: exploiting cross-transport key derivation in bluetooth classic and bluetooth low energy. Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022.
7. Ray S, Jin Y, Raychowdhury A. The changing computing paradigm with internet of things: a tutorial introduction. IEEE Design Test. 2016;33(2):76–96.
8. Bastos D, Shackleton M, El-Moussa F. Internet of things: a survey of technologies and security risks in smart home and city environments. Living Internet Things: Cybersecur IoT. 2018;2018:1–7.

9. Lu J-Q. 3-D hyperintegration and packaging technologies for micro-nano systems. Proc IEEE. 2009;97(1):18–30.
10. Sicari S, Rizzardi A, Grieco L, Coen-Porisini A. Security, privacy and trust in internet of things: the road ahead. Comput Netw. 2015;76:146–64.
11. Al-Omary A, Al Janaby A, Alsabbagh H, Al-Rizzo H. Survey of Hardware-based Security support for IoT/CPS Systems, 10 2018.
12. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of things. Comput Netw. 2013;57(07):266–2279.
13. Sallam, S, Beheshti BD. A Survey on Lightweight Cryptographic Algorithms. In TENCON 2018 - 2018 IEEE Region 10 Conference, 2018;1784–1789.
14. Al-ahdal, A, Deshmukh N. A Systematic Technical Survey Of Lightweight Cryptography On Iot Environment. International Journal of Scientific & Technology Research, 2020;05.
15. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. IEEE Internet Things J. 2019;6(5):8182–201.
16. Workshop Report by Guru Prasadh Venkataramani and Patrick Schaumont. NSF Workshop on side and covert channels in computing systems." https://www2.seas.gwu.edu/~guruv/workshop-report.pdf, 2019. Online; accessed 5 January 2021.
17. Das D, Maity S, Nasir S. B, Ghosh S, Raychowdhury A, Sen S. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017;62–67.
18. Stout W. M. S, Urias V. E. Challenges to securing the Internet of Things. In 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 2016;1–8.
19. Wang R, Qin F, Chen S, An T, Yu H. The characterization of tsv cu protrusion under thermal cycling. In 2015 16th International Conference on Electronic Packaging Technology (ICEPT),2015;888–890.
20. Carson F, Lee H. T, Yee J. H, Punzalan J, Fontanilla E. Die to die copper wire bonding enabling low cost 3d packaging. In 2011 IEEE 61st Electronic Components and Technology Conference (ECTC), 2011;1502–1507.
21. Jeong S, Foo Z, Lee Y, Sim J-Y, Blaauw D, Sylvester D. A fully-integrated 71 nw cmos temperature sensor for low power wireless sensor nodes. IEEE J Solid-State Circuits. 2014;49(8):1682–93.
22. Hu J, Wang L, Jin L, JiangNan HZ. Electrical modeling and characterization of through silicon vias (tsv). In 2012 International Conference on Microwave and Millimeter Wave Technology (ICMMT). 2012;2:1–4.
23. Dofe J, Yan C, Kontak S, Salman E, Yu Q. Transistor-level camouflaged logic locking method for monolithic 3d ic security. In 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), 2016;1–6.
24. Roy J. A, Koushanfar F, Markov I. L. Epic: Ending piracy of integrated circuits. In 2008 Design, Automation and Test in Europe, pp. 1069–1074, 2008.
25. Rostami M, Koushanfar F, Rajendran J, Karri R. Hardware security: Threat models and metrics. In 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 819–823, 2013.
26. Rahman M. T, Hardware-based Security Primitives and Their Applications to Supply Chain Integrity. PhD thesis, University of Florida, 2017.
27. Das D, Sen S. Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach. Cryptography, 2020;4(4).
28. Kocher P, Jaffe J, Jun B. Differential Power Analysis. In Advances in Cryptology — CRYPTO' 99, (Berlin, Heidelberg), pp. 388–397, pringer Berlin Heidelberg, 1999.
29. Kocher P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Advances in Cryptology — CRYPTO '96, (Berlin, Heidelberg), pp. 104–113, Springer Berlin Heidelberg, 1996.
30. Das D, Nath M, Chatterjee B, Ghosh S, Sen S. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 11–20, 2019.
31. Tunstall M, Mukhopadhyay D, Subidh Ali S. Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault.. 2011;01:224–233.
32. Aljuffri A, Zwalua M, Reinbrecht CRW, Hamdioui S, Taouil M. Applying thermal side-channel attacks on asymmetric cryptography. IEEE Trans Very Large Scale Integr VLSI Syst. 2021;29(11):1930–42.
33. Fritzke A. Obfuscating Against Side-Channel Power Analysis Using Hiding Techniques for AES. 01 2012.
34. Mangard S, Oswald E, Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards. 1st ed. Incorporated: Springer Publishing Company; 2010.
35. Agrawal D, Archambeault B, Rao J. R, Rohatgi P. The EM Side-Channel(s). In Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers, vol. 2523 of Lecture Notes in Computer Science, pp. 29–45, Springer, 2002.
36. Wang C, Cai Y, Wang H, Zhou Q. Electromagnetic Equalizer: An Active Countermeasure Against EM Side-channel Attack. In 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 1–8, 2018.
37. Jayasinghe D, Ragel R, Elkaduwe D. Constant time encryption as a countermeasure against remote cache timing attacks. In 2012 IEEE 6th International Conference on Information and Automation for Sustainability, pp. 129–134, 2012.
38. Ge Q, Yarom Y, Cock D, Heiser G. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. J Cryptogr Eng. 2018;8(04):1–27.
39. Mozaffari-Kermani M, Reyhani-Masoleh A. Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard. IEEE Trans Comput. 2010;59(5):608–22.
40. Barenghi A, Breveglieri L, Koren I, Naccache D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. Proc IEEE. 2012;100(11):3056–76.
41. Yu W, Köse S. A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks. IEEE Trans Circuits Syst I Regul Pap. 2017;64(11):2934–44.
42. Yang K, Park J, Tehranipoor M, Bhunia S. Robust Timing Attack Countermeasure on Virtual Hardware. In 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 148–153, 2018.
43. Kahleifeh Z, Thapliyal H. EE-ACML: Energy-Efficient Adiabatic CMOS/MTJ Logic for CPA-Resistant IoT Devices. Sensors, 2021;21(22).
44. Degada A, Thapliyal H. Single-Rail Adiabatic Logic for Energy-Efficient and CPA-Resistant Cryptographic Circuit in Low-Frequency Medical Devices. IEEE Open Journal of Nanotechnology. 2022;3:1–14.
45. Park J, Rahman F, Vassilev A, Forte D, Tehranipoor M. Leveraging Side-Channel Information for Disassembly and Security. J. Emerg. Technol. Comput. Syst., vol. 16, dec 2019.
46. Chakraborty P, Cruz J, Posada C, Ray S, Bhunia S. HASTE: Software Security Analysis for Timing Attacks on Clear Hardware Assumption. IEEE Embed Syst Lett. 2022;14(2):71–4.
47. Bai Y, Stern A, Park J, Tehranipoor M, Forte D. RASCv2: Enabling Remote Access to Side-Channels for Mission Critical and IoT Systems. ACM Trans. Des. Autom. Electron. Syst., vol. 27, jun 2022.

48. He J, Guo X, Tehranipoor M, Vassilev A, Jin Y. EM Side Channels in Hardware Security: Attacks and Defenses. IEEE Design & Test. 2022;39(2):100–11.
49. Ahmed B, Bepary M. K, Pundir N, Borza M, Raikhman O, Garg A, Donchin D, Cron A, Abdel-moneum M. A, Farahmandi F, Rahman F, Tehranipoor M. Quantifiable Assurance: From IPs to Platforms. 2022.
50. Jevtic R, Ylitolva M, Calonge C, Ojanen M, Santti T, Koskinen L. EM Side-Channel Countermeasure for Switched-Capacitor DC-DC Converters Based on Amplitude Modulation. IEEE Transactions on Very Large Scale Integration Systems. 2021;29(6):1061–72.
51. Poggi D, Ordas T, Sarafianos A, Maurine P. Checking robustness against em side-channel attacks prior to manufacturing. IEEE Trans Comput Aided Des Integr Circuits Syst. 2022;41(5):1264–75.
52. Pundir N, Park J, Farahmandi F, Tehranipoor M. Power Side-Channel Leakage Assessment Framework at Register-Transfer Level. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, pp. 1–12, 2022.
53. Moukarzel M, Eisenbarth T, Sunar B. Leech: A side-channel evaluation platform for IoT. In 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 25–28, 2017.
54. Patranabis S, Roy D, Chakraborty A, Nagar N, Singh A, Mukhopadhyay D, Ghosh S. Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications. Journal of Hardware and Systems Security. 2019;3:06.
55. Aerabi E, Papadimitriou A, Hely D. On a Side Channel and Fault Attack Concurrent Countermeasure Methodology for MCU-based Byte-sliced Cipher Implementations. In 2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 103–108, 2019.
56. Yu Q, Zhang Z, Dofe J, Proactive Defense Against Security Threats on IoT Hardware, ch. 18, pp. 407–433. John Wiley & Sons, Ltd, 2020.
57. Dofe J, Pahlevanzadeh H, Yu Q. A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack. J Electron Test. 2016;32(5):611–24.
58. Nagata M. On-Chip Protection of Cryptographic ICs Against Physical Side Channel Attacks: Invited Paper. In 2019 IEEE 13th International Conference on ASIC (ASICON), pp. 1–4, 2019.
59. Dofe J, Gu P, Stow D, Yu Q, Kursun E, Xie Y. Security Threats and Countermeasures in Three-Dimensional Integrated Circuits. 2017:05:321–326.
60. Xie Y, Bao C, Liu Y, Srivastava A. 2.5D/3D Integration Technologies for Circuit Obfuscation. In 2016 17th International Workshop on Microprocessor and SOC Test and Verification (MTV), pp. 39–44, 2016.
61. Dofe J, Yu Q, Wang H, Salman E. Hardware security threats and potential countermeasures in emerging 3d ics. In Proceedings of the 26th Edition on Great Lakes Symposium on VLSI, GLSVLSI '16, (New York, NY, USA), p. 69-74, Association for Computing Machinery, 2016.
62. Wang Z. 3-D Integration and Through-Silicon Vias in MEMS and Microsensors. Microelectromechanical Systems, Journal of. 2015;24(10):1211–44.
63. Wang A, Chen Q, Li C, Lu F, Wang C, Zhang F, Wang X. S, Ng J, Xie Y.-H, Ma R, Wang L, Lin L. More-than-moore: 3d heterogeneous integration into cmos technologies. In 2017 IEEE 12th International Conference on Nano/Micro Engineered and Molecular Systems (NEMS), 2017;1–4.
64. McCants C. Trusted integrated chips (tic)." https://www.iarpa.gov/index.php/research-programs/tic, 2011. Intelligence Advanced Research Projects Activity (IARPA).
65. Rajendran J. J, Sinanoglu O, Karri R. Is split manufacturing secure?. In Proceedings of the Conference on Design, Automation and Test in Europe, DATE '13, (San Jose, CA, USA), p. 1259-1264, EDA Consortium, 2013.
66. Jung M, Song T, Wan Y, Peng Y, Lim S. K. On enhancing power benefits in 3d ics: Block folding and bonding styles perspective. In 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1–6, 2014.
67. Fletcher BJ, Das S, Mak T. Design and Optimization of Inductive-Coupling Links for 3-D-ICs. IEEE Trans Very Large Scale Integr VLSI Syst. 2019;27(3):711–23.
68. Rostami M, Koushanfar F, Karri R. A Primer on Hardware Security: Models, Methods, and Metrics. Proc IEEE. 2014;102(8):1283–95.
69. Valamehr J, Huffmire T, Irvine C, Kastner R, Koc C, Levin T, Sherwood T. A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors. 2012;6805(11):364–382.
70. P. Gu, S. Li, D. Stow, R. Barnes, L. Liu, Y. Xie, and E. Kursun. Leveraging 3D technologies for hardware security: Opportunities and challenges. In 2016 International Great Lakes Symposium on VLSI (GLSVLSI), pp. 347–352, 2016.
71. Yan C, Dofe J, Kontak S, Yu Q, Salman E. Hardware-efficient logic camouflaging for monolithic 3-d ics. IEEE Trans Circuits Syst II Express Briefs. 2018;65(6):799–803.
72. Dofe J, Yu Q. Exploiting PDN Noise to Thwart Correlation Power Analysis Attacks in 3D ICs. In 2018 ACM/IEEE International Workshop on System Level Interconnect Prediction (SLIP), 2018;1–6.
73. Zhang Z, Dofe J, Yu Q. Improving power analysis attack resistance using intrinsic noise in 3D ICs. Integration. 2020;73:30–42.
74. Knechtel J, Patnaik S, Sinanoglu O. 3d integration: Another dimension toward hardware security. In 2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 147–150, 2019.