2021 IEEE International Symposium on Smart Electronic Systems (iSES) | 978-1-7281-8753-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/iSES52644.2021.00053

Unified Countermeasures against Physical Attacks in Internet of Things - A survey

Jaya Dofe, Aaron Nguyen, Andy Nguyen
Department of Computer Engineering
California State University, Fullerton, CA, USA
jdofe@fullerton.edu

***Abstract*—The Internet of Things (IoT) impacts how we interact with the world around us for good. While IoT benefits are undeniable, it is a double-edged sword. The security aspect is the major concern in the IoT realm, especially side-channel attacks since there are abundant channels due to physical effects. IoT devices have been widely used in many fields of production and social living, such as healthcare, energy and industrial automation and military application, to name a few. Much research focuses on software, network, and cloud security; however, hardware security in these devices has been overlooked. The low-power, heterogeneous and resource-constrained nature of IoT devices makes incorporating security features extremely challenging. Conventional security measures, such as encryption, are infeasible for deployment under such constraints.**

This survey paper discusses the existing countermeasures for isolated side-channel attacks (SCA) and then dives into unified countermeasures that benefit IoT devices to address the area footprint and power constraints. Further, to defeat the IoT system from the advanced SCA, we proposed to use 3D integration as an IoT platform. 3D technology provides various advantages such as heterogeneous integration, split manufacturing, disparate technologies for IoT like MEMS sensors, etc., making 3D integration the best choice for IoT platforms.

***Index Terms*—Internet of Things (IoT), Physical Attacks, Side-channel Attacks, 3D ICs, Secure IoT.**

I. 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, industry, hospitals, cities, farms, etc. These connected objects—the Internet of Things (IoT)- bring 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 threats at various levels. IoT devices allocate their resources like energy and computation for the functionality, and incorporating security becomes very challenging [1]. With the short time-to-market and fierce competition among companies, security has become an afterthought [2] and has not been prioritized as a crucial metric. The security aspect is the biggest concern in the IoT realm. 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. How can we secure the IoT technology where they touch the broader internet?

IoT can become more secure through cryptography for communication between the physical and cyber world. Research shows that many IoT infected devices have little to no security protections [3]. Several IoT devices have embedded cryptographic cores for authentication and information processing. However, a prominent attack method—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 [4], [5]. Current IoT studies show that adversaries can easily acquire side-channel information, which is hard to detect because leakages are inevitable [6]. Side channels in IoT systems may arise from timing information, sensor data, or traffic rates between devices prevalent in our everyday lives.

The current state of Internet of Things (IoT) devices, for short, is challenging traditional security protocols. Many IoT designs prioritize keeping their devices small in size, battery, and computation power, making traditional security methods unsuitable. This is causing a tug of war currently between having good security on your device or having a good performance at a low price. This fray in security is causing IoT devices to be vulnerable to side-channel attacks. There are many published research that discussed IoT security and challenges facing IoT devices [7]–[9]. 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 [10], [11] for IoT applications. However, there is

978-1-7281-8753-2/21/$31.00 ©2021 IEEE
DOI 10.1109/iSES52644.2021.00053

a lack of surveys that mainly discuss the side-channel attacks and respective countermeasures in the IoT domain.

To the best of our knowledge, this is the first survey that addresses unified countermeasures for side-channel attacks, specifically for IoT devices. As the existing countermeasures for the SCA 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 for building the IoT devices as it offers a natural defence against SCA attacks, heterogeneity, small form factor, and reduced power dissipation.

The rest of this paper is organized as follows. Section II presents an overview of side-channel attacks. Sections III discusses generic countermeasures for the selected side channel attacks. In section IV, the defense methods specific to IoT against SCA are introduced. The unified approaches unique to the SCA attacks are discussed in section V. Section VI provides the details of 3D integration to design secure IoT devices. Finally, section VII, concludes the paper.

II. 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 attack in which 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 behaviour of the device, 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 needed access to the physical device. However, in the IoT, these attacks can be made remotely.

Side-channel analysis (SCA) attacks [4], [5], [12] 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 [13]. 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 [14] 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 [15] 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 by using faulty outputs. The work [16] 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.

Various studies indicate that IoT devices' distributed and remote nature provides the adversaries with the time and physical access to manipulate any remote node.

III. 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 [17], [18] is to cover up a correlation between the power traces and the intermediate values. Hiding deceit the 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 [18].

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 [19]. Recently, authors Das et al. used white-box modeling [15] to develop a low-overhead generic circuit-level countermeasure against electromagnetic side-channel attacks. Electromagnetic Equalizer is proposed in [20], 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 behaviour is never data-dependent. The sequence of cache accesses or branches does not depend on either the key or the plaintext. Paper [21] 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 [22]. One beneficial way to make time attacks challenging is to desynchronize the execution of sensitive parts by 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 [23]. Survey paper [24] presented countermeasures against fault injection attacks, including algorithmic changes, sensors and shields, and fault detection or correction techniques.

IV. 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 [4]–[6]. 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 [5] 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 [25] 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 [26] 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.

V. Unified Countermeasures for IoT

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

The paper [27] propose 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.

An embedded trusted platform module is proposed in [28] 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 Figure 1 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.

Recently, authors Das et al. used white-box modeling [15] 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 Figure 2. This approach utilizes the local lower-metal layers to route the

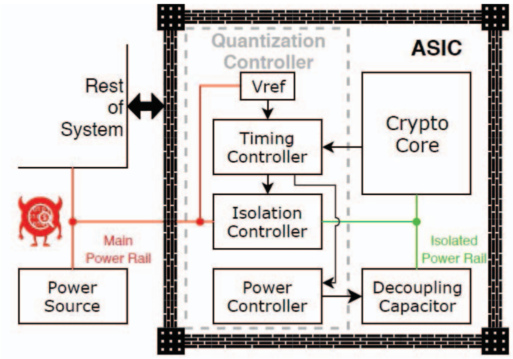

Fig. 1: Secure Processor using Quantization Controller [28].

crypto core with a signature suppression circuit, reducing the leakage reaching the top metal layer.

In paper [29], 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 Micro-controller units to carry out parallel byte-sliced encryption. As depicted in Figure 3, the same data byte D1 is cloned four times and encrypted using a fake key (K_F) twice and true key (K_T) twice. This arrangement will generate the correlated algorithmic noise to protect against SCA as both computations operate parallel on the 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 [30], [31], 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.

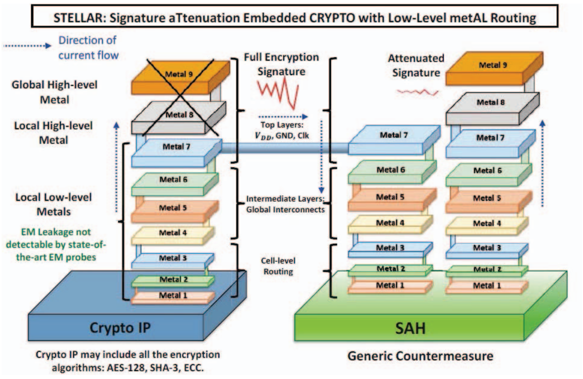
STELLAR: Signature aTtenuation Embedded CRYPTO with Low-Level metAL Routing
Direction of current flow
Global High-level Metal
Local High-level Metal
Local Low-level Metals
EM Leakage not detectable by state-of-the-art EM probes
Full Encryption Signature
Top Layers: V_{DD}, GND, Clk
Intermediate Layers: Global Interconnects
Cell-level Routing
Attenuated Signature
Metal 9
Metal 8
Metal 7
Metal 6
Metal 5
Metal 4
Metal 3
Metal 2
Metal 1
Crypto IP
SAH
Crypto IP may include all the encryption algorithms: AES-128, SHA-3, ECC.
Generic Countermeasure

Fig. 2: Stellar Technique for Side-channel Protection [15].

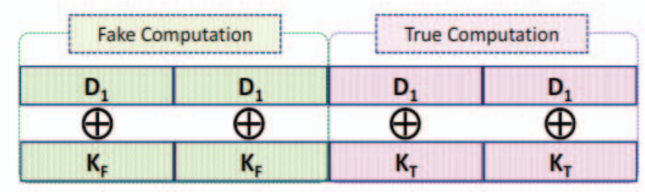

Fig. 3: Combined SCA and FA Countermeasure [29].

An on-chip waveform measurement (OCM) technique is exploited in [32] that protect 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.

VI. 3D Integration as a Secure platform for IoT Devices

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 security. Security measures implemented in traditional computers, such as cryptography, present a challenge from this context when applied in 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 [33]. 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.

Three-dimensional (3D) integration [34] 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. 3D integrated circuits (3D ICs) include several heterogeneous layers in a stacked architecture in the chip layout and provide a promising paradigm for secure, heterogeneous 3D integration suitable for IoT devices. 3D technology provides various advantages such as heterogeneous integration [35], split manufacturing [36], [37], disparate technologies for IoT like MEMS sensors [38], etc.

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 4.

1. Separate security plane using 3D stack: Sherwood et al. [39] 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.

2. Shielding side-channels with 3D stacking: In this approach, authors utilize intrinsic characteristics of 3D chip and dynamic shielding to hide the security-related activities on the chip [40]. They propose to use micro-controller unit to produce complementary activity patterns dynamically thwarting side-channel information leakage.

3. Intrinsic power distribution network (PDN) noise to defeat SCA in 3D ICs: In this work, the authors demonstrate 3D PDN introduce noise to the power profile of 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 [41], [42].

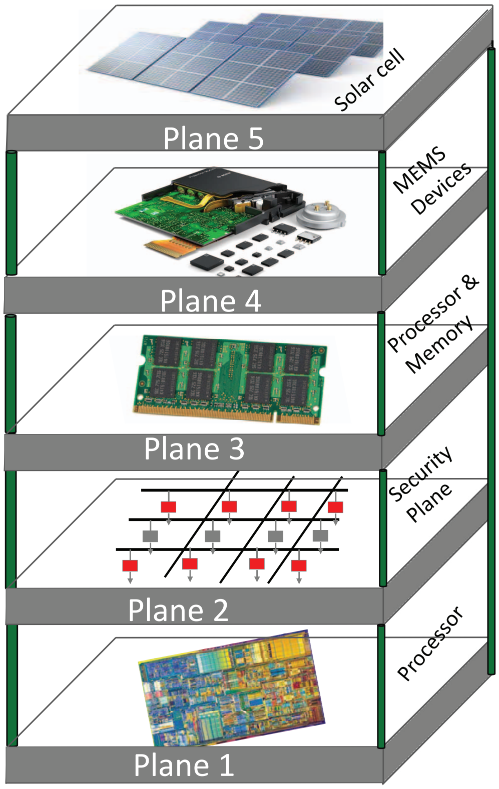

Fig. 4: 3D Structures for IoT Devices.

4. Energy harvesting using solar cell: Many IoT devices will be battery operated or self-powered. 3D integration provides an opportunity to use alternate forms of energy like solar, electromagnetic, thermal, etc., because of its heterogeneous nature.

VII. Conclusion

The Internet of Things (IoT) impacts the way we interact with the world around us for good. While IoT benefits are undeniable, it is a double-edged sword. The security aspect is the major concern in the IoT realm, especially side-channel attacks since there are abundant channels due to physical effects. IoT devices have been widely used in many fields of production and social living, such as healthcare, energy and industrial automation and military application, to name a few. Much research is focused on software, network, and cloud security, and hardware security in these devices has been overlooked. The low-power, heterogeneous and resource-constrained nature of IoT devices makes incorporating security features extremely challenging. Conventional security measures, such as encryption, are infeasible for deployment under such constraints.

This survey paper discussed the existing countermeasures for individual side-channel attacks (SCA) and unified countermeasures that will benefit IoT devices because of area footprint and power constraints. Further, to defeat the IoT system from the advanced SCA, we proposed to use 3D integration as an IoT platform. 3D technology provides various advantages such as heterogeneous integration, split manufacturing, disparate technologies for IoT like MEMS sensors, etc., making 3D integration the best choice for IoT platforms.

References

[1] S. Ray, Y. Jin, and A. Raychowdhury, "The Changing Computing Paradigm With Internet of Things: A Tutorial Introduction," *IEEE Design Test*, vol. 33, no. 2, pp. 76–96, 2016.

[2] D. Bastos, M. Shackleton, and F. El-Moussa, "Internet of Things: A survey of technologies and security risks in smart home and city environments," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pp. 1–7, 2018.

[3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[4] 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.

[5] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "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)*, pp. 62–67, 2017.

[6] W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 1–8, 2016.

[7] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[8] A. Al-Omary, A. Al Janaby, H. Alsabbagh, and H. Al-Rizzo, "Survey of Hardware-based Security support for IoT/CPS Systems," 10 2018.

[9] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of things," *Computer Networks*, vol. 57, p. 2266–2279, 07 2013.

[10] S. Sallam and B. D. Beheshti, "A Survey on Lightweight Cryptographic Algorithms," in *TENCON 2018 - 2018 IEEE Region 10 Conference*, pp. 1784–1789, 2018.

[11] A. Al-ahdal and N. Deshmukh, "A Systematic Technical Survey Of Lightweight Cryptography On Iot Environment," *International Journal of Scientific & Technology Research*, 05 2020.

[12] D. Das and S. Sen, "Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach," *Cryptography*, vol. 4, no. 4, 2020.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*, (Berlin, Heidelberg), pp. 388–397, pringer Berlin Heidelberg, 1999.

[14] P. C. Kocher, "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.

[15] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "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.

[16] M. Tunstall, D. Mukhopadhyay, and S. Subidh Ali, "Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault.," pp. 224–233, 01 2011.

[17] A. Fritzke, "Obfuscating Against Side-Channel Power Analysis Using Hiding Techniques for AES," 01 2012.

[18] S. Mangard, E. Oswald, and T. Popp, "Power analysis attacks - revealing the secrets of smart cards," 2007.

[19] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "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.

[20] C. Wang, Y. Cai, H. Wang, and Q. Zhou, "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.

[21] D. Jayasinghe, R. Ragel, and D. Elkaduwe, "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.

[22] Q. Ge, Y. Yarom, D. Cock, and G. Heiser, "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware," *Journal of Cryptographic Engineering*, vol. 8, pp. 1–27, 04 2018.

[23] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard," *IEEE Transactions on Computers*, vol. 59, no. 5, pp. 608–622, 2010.

[24] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[25] W. Yu and S. Köse, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2934–2944, 2017.

[26] K. Yang, J. Park, M. Tehranipoor, and S. Bhunia, "Robust Timing Attack Countermeasure on Virtual Hardware," in *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 148–153, 2018.

[27] S. Patranabis, D. Roy, A. Chakraborty, N. Nagar, A. Singh, D. Mukhopadhyay, and S. Ghosh, "Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications," *Journal of Hardware and Systems Security*, vol. 3, 06 2019.

[28] M. Moukarzel, T. Eisenbarth, and B. Sunar, "Leech: A side-channel evaluation platform for IoT," in *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 25–28, 2017.

[29] E. Aerabi, A. Papadimitriou, and D. Hely, "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.

[30] Q. Yu, Z. Zhang, and J. Dofe, *Proactive Defense Against Security Threats on IoT Hardware*, ch. 18, pp. 407–433. John Wiley & Sons, Ltd, 2020.

[31] J. Dofe, H. Pahlevanzadeh, and Q. Yu, "A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack," *J. Electron. Test.*, vol. 32, no. 5, pp. 611–624, 2016.

[32] M. Nagata, "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.

[33] M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[34] J.-Q. Lu, "3-D Hyperintegration and Packaging Technologies for Micro-Nano Systems," *Proceedings of the IEEE*, vol. 97, no. 1, pp. 18–30, 2009.

[35] J. Dofe, P. Gu, D. Stow, Q. Yu, E. Kursun, and Y. Xie, "Security Threats and Countermeasures in Three-Dimensional Integrated Circuits," pp. 321–326, 05 2017.

[36] Y. Xie, C. Bao, Y. Liu, and A. Srivastava, "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.

[37] J. Dofe, Q. Yu, H. Wang, and E. Salman, "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.

[38] Z. Wang, "3-D Integration and Through-Silicon Vias in MEMS and Microsensors," *Microelectromechanical Systems, Journal of*, vol. 24, pp. 1211–1244, 10 2015.

[39] J. Valamehr, T. Huffmire, C. Irvine, R. Kastner, C. Koc, T. Levin, and T. Sherwood, "A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors," vol. 6805, pp. 364–382, 11 2012.

[40] 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.

[41] J. Dofe and Q. Yu, "Exploiting PDN Noise to Thwart Correlation Power Analysis Attacks in 3D ICs," in *2018 ACM/IEEE International Workshop on System Level Interconnect Prediction (SLIP)*, pp. 1–6, 2018.

[42] Z. Zhang, J. Dofe, and Q. Yu, "Improving power analysis attack resistance using intrinsic noise in 3D ICs," *Integration*, vol. 73, pp. 30–42, 2020.