Shreyas Sen and Archisman Ghosh

Circuit-Level Techniques for Side-Channel Attack Resilience

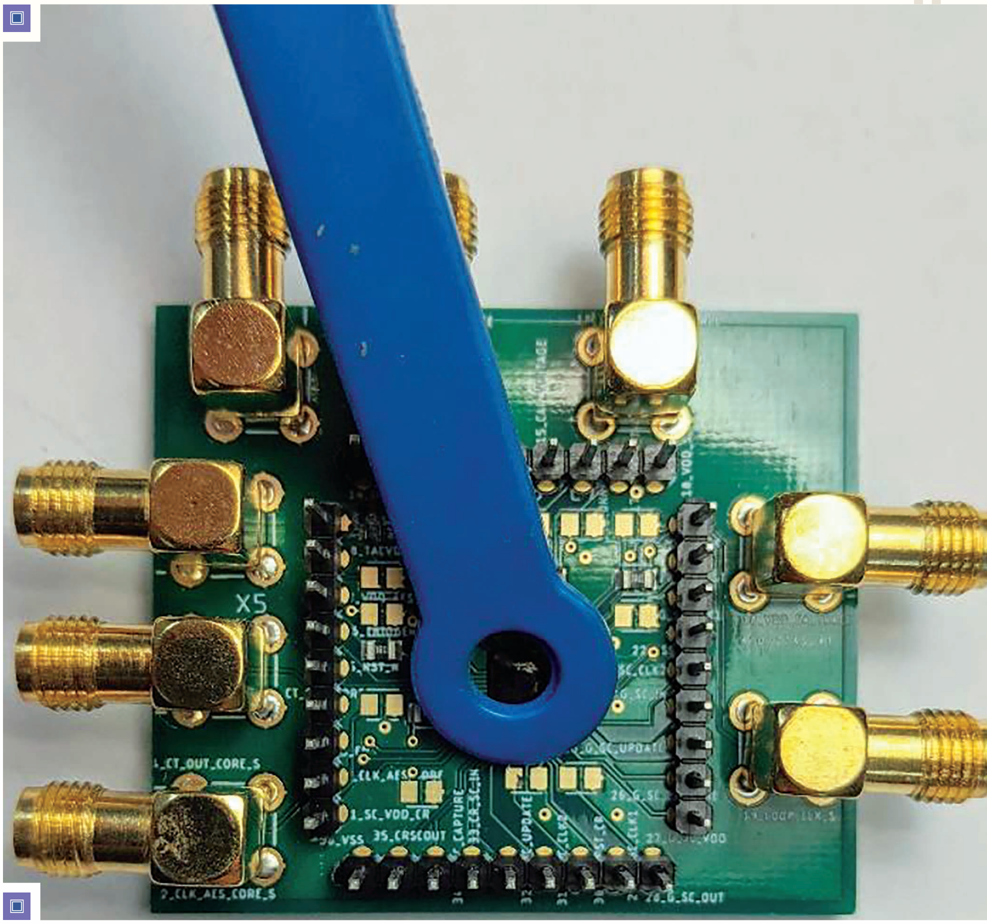
A tutorial

Cryptography protects sensitive data by using encryption that is impossible to break with modern computers in meaningful time through brute-force attacks. In contrast, side-channel attacks (SCAs), first developed a quarter century back [1], continue to pose a significant threat to the security of crypto systems in modern devices.

Introduction

Mathematically secure crypto algorithms, when implemented on hardware, inadvertently leak information through physical side-channel signatures, such as power, electromagnetics (EMs), light, acoustics, and so on. Exploiting these side channels drastically reduces the attacker's search space, illustrated by the diminishing protection of Advanced Encryption Standard (AES) 256 being

Digital Object Identifier 10.1109/MSSC.2024.3444740
Date of current version: 15 November 2024



proportional to 2^{256} encryptions by brute-force attacks compared to 2^{13} by SCAs, enabling real-time attacks. Additionally, the transition from AES-128 to AES-256 only doubles SCA protection, rather than the expected 2^{128} times increase seen in brute-force attack scenarios. This has led to many real-world examples of exploitation of vulnerabilities using SCAs, such as cloning of Google Titan 2FA keys [44], an Internet of Things worm using vulnerabilities in Philips Hue light bulbs [42], an EM SCA-based exploitation of iPhone 5 keys [43], among others. In the past two decades, many countermeasures against SCAs have been developed, first at the algorithm, architecture, and logic level and more recently, in the last decade, at the circuit level, providing generic low-overhead solutions. We start by defining a relevant taxonomy, followed by the genesis of power/EM SCAs [Figure 1(a)], leading to an overview of circuit-level techniques for SCA resilience [Figure 1(b)].

> **Side-channel attacks, first developed a quarter century back, continue to pose a significant threat to the security of crypto systems in modern devices.**

Taxonomy

A short taxonomy related to SCAs and their defense is presented below. For a detailed taxonomy on hardware security, please see [2] and [3]:

- *Cryptography*: A mathematical technique that constructs and analyzes protocols to prevent third parties from reading private information. It often relies on a trapdoor function that is easy to compute in one direction yet difficult to compute in the opposite direction (finding its inverse) without special (secret) information [4].
- *Symmetric key encryption*: Allows users to encrypt and decrypt with the same secret key. The most popular example is the AES [5]. Recently, Ascon [6] emerged as a lightweight crypto standard, and it is preferred in edge devices.
- *Asymmetric key encryption*: This is a technique of encryption by using a public key and decryption by using a secret key. Though ciphertext (CT) is available in the public domain, only the party with the secret key can use it. This is popular in communication channels, transport layer security, and so on. Rivest–Shamir–Adleman [7] is the most popular choice for asymmetric key encryption.
- *Postquantum crypto*: These crypto algorithms are mathematically resilient to future quantum computers, due to the absence of suitable quantum attack algorithms. Kyber, standardized by the National Institute of Standards and Technology in 2022, is the current postquantum crypto standard [8].
- *Crypto core*: This is a cryptographic algorithm implemented as a digital circuit in hardware to provide encryption/decryption.
- *Plaintext (PT)*: A sensitive payload to be encrypted.
- *CT*: An encrypted secure payload, CT can be reversed using the secret key to receive sensitive payload back.
- *Hardware security*: Explores hardware primitives useful for security, practical aspects and the possibility of deployment, and vulnerability due to hardware implementation as well as mitigation techniques (e.g., SCA and its countermeasure).
- *SCA/side-channel analysis*: A popular generic attack technique on different crypto cores. These attacks exploit vulnerabilities of the hardware implementation.
- *Attacks*: A technique of hacking secure crypto cores. *Attack* is a generic term; however, we use this term to convey "extracting the key from the practical implementation of crypto algorithms."
- *Vulnerabilities*: Sources of information leakage due to nonideal implementation of crypto cores.
- *Exploitation*: A technique for extracting a secret key (hence, secret PT) using vulnerabilities of crypto cores. The SCA is one of the exploitation techniques, which is discussed in more detail in the following sections.
- *Countermeasure*: A technique utilized along with crypto cores to reduce vulnerabilities. Countermeasures can be logical (often provably secure) or physical (circuit level), and they reduce information leakage at its source.
- *Masking*: A popular logical provably secure countermeasure [9], [10], [11], [12], [13]. It often incurs high overhead and is commonly used today when high security is required, at the cost of power, performance, and area (PPA) overhead.
- *Physical countermeasure*: This reduces the signal-to-noise ratio (SNR) of potential correlated information leakage. In this tutorial, we cover the following physical countermeasures:
  - *Power port*: This concerns countermeasures implemented at the power supply (V_{DD}). They are low overhead and crypto core independent in nature. We discuss the following three specific types of power port countermeasures.
    1) *LDO Regulators*: An important component of SoCs that are, in general, used for power delivery. We discuss how LDOs are being leveraged for SCA resilience.
    2) *Integrated voltage regulator*: Buck–boost converters are dc–dc converters used in the power delivery context and have been adapted as an SCA-resilient solution.
    3) *Switched capacitor converters*: A fundamental circuit technique used for computation in discrete-time mixed-signal systems. Switched capacitor-based converters are gaining increasing popularity for SCA resilience.

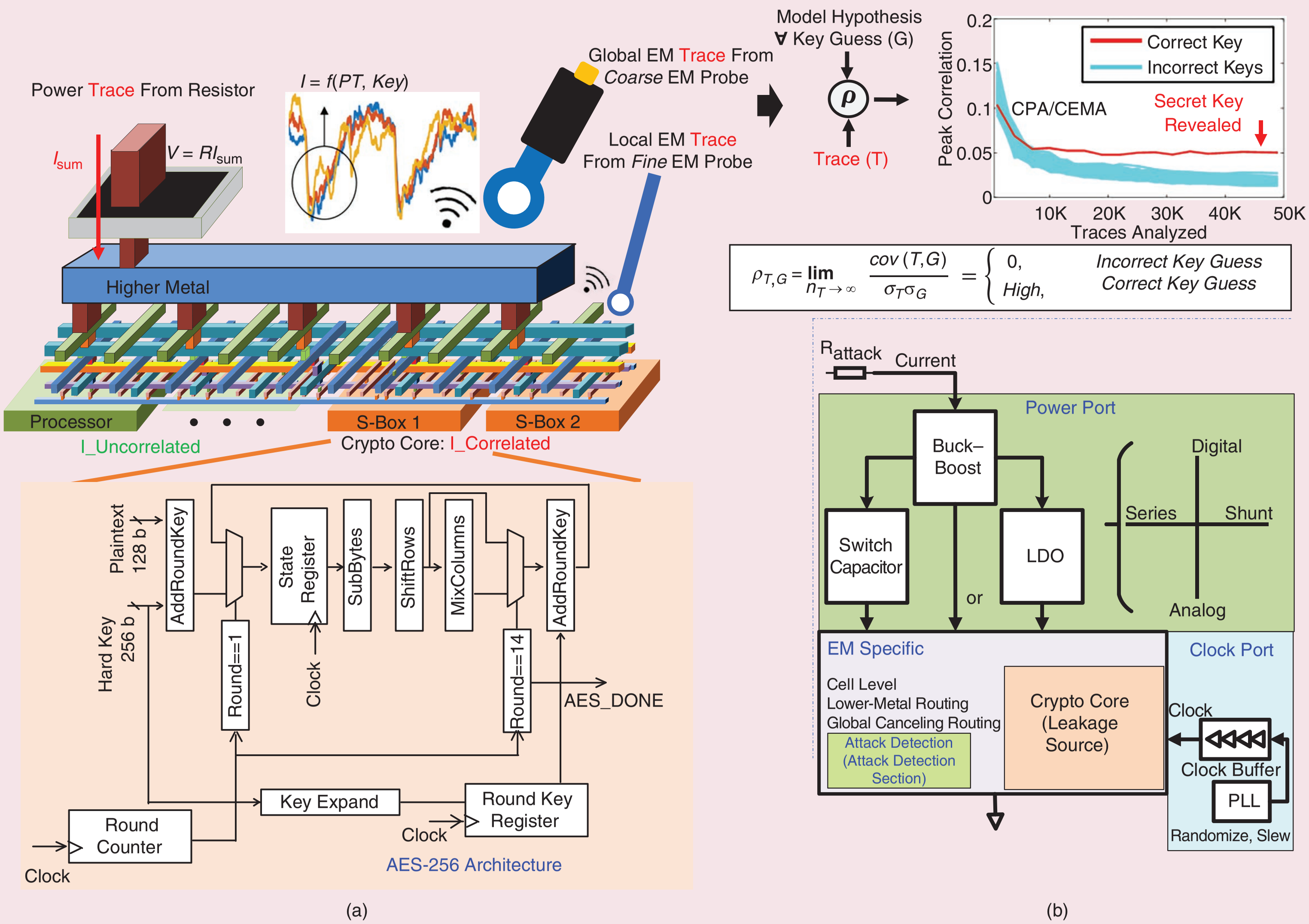


FIGURE 1: (a) The genesis of side-channel leakage, starting from an example crypto core (AES-256) generating correlated currents that flow first through lower and then higher metals leading to the power port, making local EM, global EM, and power SCAs possible, respectively. (b) The captured traces are correlated with a hypothesis, related to key guesses, to eventually extract the correct key overview of circuit-level countermeasures and the organization of the tutorial: power port, clock port, EM-specific countermeasures, and attack detectors. S-box: substitution box; CPA: correlational power attack; CEMA: cyber and EM activities.

- *Clock port*: This involves low-overhead crypto core-independent countermeasures at the clock port.
- *Clock slew/skew*: A technique where a nonideal (slanted) clock is introduced to SoCs [14]. A recent study shows clock slew as a potential technique for SCA mitigation. It is important to note that clock slew differs from clock skew, which introduces jitter. Effect of clock-skew in side channel countermeasure could be an interesting future study.
- *EM specific*: These countermeasures are specific to reducing EM leakages.
- *Attack detectors*: Since countermeasures increase PPA overhead, there is a growing trend toward including SCA detectors that turn on defenses only as needed.
- *Arithmetic techniques*: These are mathematical techniques, such as shuffling between instructions, to increase SCA immunity [15].
- *Minimum traces to disclosure (MTD):* A measure of SCA immunity. It shows the absolute number of traces/encryption required to reveal the secret key. A higher MTD implies higher security.
- *Relative MTD increase*: This is the ratio of protected MTD with respect to an unprotected counterpart. The MTD of unprotected crypto cores often varies based on the setup, measurement noise, crypto algorithms, and attack algorithms. Hence, we propose use of this metric for better comparison.
- *Test vector leakage analysis (TVLA)*: A measure of information leakage based on a statistical t-test [16]. A $|t|$-value of ≥ 4.5 shows a possibility of exploitation [16].
- *Threshold implementation (TI)*: A recently popular provably secure masking technique [9].
- *Signature*: We refer to the signature as sensitive data/information leakage. This includes power and EM traces that are correlated with a secret key.
- *Signature attenuation (AT)*: A physical countermeasure to attenuate the above-mentioned signature.
- *Noise injection*: Includes but is not restricted to thermal noise from the circuit, measurement noise, and so on. Anything uncorrelated to the key acts as noise for the purposes of SCA security. For example, other algorithmic operations can act as sources of noise. Intentional noise injection is a naive high-overhead technique for SCA resilience.

> **Mathematically secure crypto algorithms, when implemented on hardware, inadvertently leak information through physical side-channel signatures.**

SCA Leakage Fundamentals

All digital circuits implemented in silicon draw current based on their switching activity, which, in turn, is primarily related to the function of computing and its inputs. In the case of a crypto core, the inputs are PT and the secret key, making these switching currents correlated with the secret key. Hence, if the current can be observed through power or EM measurements, a power/EM side-channel leakage signature is created. The principal idea of the power/EM SCA is to statistically analyze these correlated signatures to trace back the secret key, as detailed in Figure 1(a). Consider AES-256 an example of a crypto core. The operations of multiple rounds, each including SubBytes, ShiftRows, and MixColumns, implement a one-way function and are the combinational logic along with the registers that store the data. The registers leak most at the clock edge, and the combination logic leaks in varying amounts throughout the cycle. The correlated leakage current passes through, first, lower metal layers and vias and then gets aggregated with other uncorrelated currents (e.g., from an adjacent processor core) and passes through higher layers of larger metals, vias, and bumps before coming out to the package and PCB to the power source. Power and EM (both global and local) measurements from these leakages are utilized to mount SCAs.

Power side-channel leakage occurs because digital gate switching involves charging and discharging MOS gate and interconnect capacitors, affecting the power supply and ground ports. Tracking current consumption through a small resistor in series with supply provides visibility of switching activity to attackers. EM side-channel leakage arises from these sharp transitions, following Maxwell's equations: accelerating or decelerating electrons emit EM fields, with faster rise/fall times resulting in higher EM leakage. The extent of EM leakage also depends on the size of the metal layers carrying the currents, with higher-level metal layers (e.g., >M6 in 65-nm CMOS) being significantly larger than lower layer (e.g., ≤M6). In ICs, current loops generate H-field components, while surfaces generate E-field components. Faraday cage shielding is often impractical due to necessary power and signal traversal openings. These leakages can be detected even from a distance using cheap H-probes. It is important to note that there are other circuit components that act as sources of noise as part of SoCs. Correlation attacks are extremely powerful, as these noises are averaged out. To circumvent this problem, an attacker can use micrometer-scale probes to detect sensitive data leakage from closer proximity and avoid the effect of noises caused by other circuits in SoCs. As this technique can detect sensitive EM leakages locally, we call this a *local EM SCA*, whereas other EM SCA techniques are referred to as *global EM SCAs* throughout the article. To reduce physical SCA leakages, countermeasures focus on reducing the signal or increasing the noise, leveraging an understanding of the physical aspects

Since countermeasures increase PPA overhead, there is a growing trend toward including SCA detectors that turn on defenses only as needed.

of these leaks for targeted protection strategies, as follows.

SCA Model

An SCA exploits current or EM emanation to trace back switching activity to, in turn, uncover a secret key. This switching activity provides additional visibility on mathematically secure crypto algorithms and opens a door for exploitation. Figure 1(a), top right, illustrates an SCA on a cryptographic DUT with input PT and output CT. The attacker, with physical access to the DUT, captures side-channel signatures (e.g., power or EM emissions) to uncover the secret key, as described previously. The attacker then correlates these real traces with hypothetical traces generated for all possible key guesses (e.g., 2^8 guesses for each byte in AES-256). In a correlational power attack (CPA)/correlational EM attack (CEMA), numerous traces for varying PTs are analyzed. As the number of traces increases, incorrect key guesses are ruled out, following the correlation equation shown, and the correct key guess stands out, leading to a successful attack on the key byte. This is then repeated for other key bytes. In summary, the underlying physics causes correlated secret information leakage, which attackers exploit through the power of statistics (e.g., correlation) over numerous traces. Moreover, the rise of machine learning-based SCA [17] has notably decreased attack times by shifting the workload to the training phase and enabling even single-trace attacks under certain conditions, expanding the attack surface. While numerous examples of SCAs exist, this article concentrates on recent circuit-level advancements providing resilience against such attacks over the past decade.

Countermeasures Overview

Resilience to SCAs has been explored at multiple layers of abstraction, including early exploration in the 2000s of countermeasures at the architectural (random dummy operation insertion and shuffling operations) and logical (e.g., [18] and [19]) layers, often leading to high PPA overheads. However, noting that physical SCA leakage is caused by accelerating and decelerating electrons, it can be efficiently mitigated by circuit-level countermeasures that address the issue at its root. These techniques, initiated in 2009 and gaining momentum since 2017, offer significant protection against SCAs. Although not provably secure like masking, circuit-level methods are often generic and provide high protection with minimal power and performance overhead. This makes attacks sufficiently challenging, redirecting practical attackers toward easier targets. Figure 1(b) provides an overview of various recently developed and emerging circuit-level countermeasures for SCAs, broken down into four key types:

1) *Power port*: switched capacitors, integrated voltage regulators (IVRs), and LDOs, including series LDOs and shunt LDOs
2) *Clock port*: clock randomization and clock slew
3) *EM specific*: cell level, local routing using lower metal, and global multipole canceling routing
4) *Attack detector*: for both power and EM SCAs.

The countermeasures as mentioned above need to be compared with one another. Security metrics are crucial for comparing countermeasures in SCAs. Unlike some other emerging hardware security subareas, the field of SCAs benefits from well-defined metrics like MTD and the t-test (TVLA). However, these metrics depend heavily on the measurement setup. For example, using a 100-mΩ versus a 10-Ω resistor in a power SCA can cause a 10K-fold change in MTD values. In EM SCAs, probe placement and dimensions (100-μm, 1-mm, and 10-mm diameters) significantly impact results. Measurement noise, averaging, and attacker expertise also affect MTD numbers. A practical solution is to report the relative MTD increase from unprotected to protected states on the same IC, using consistent setups and personnel. While standardizing SCA metrics across custom ICs remains challenging, this article uses the "relative MTD increase" to compare different designs [Figure 5(b)]. Each design offers valuable insights into SCA resilience at the circuit level. In the future, a unified evaluation framework could allow scalable comparisons and sharing of designs for validation by different groups. This article's goal is to focus on the underlying principles of these countermeasures, with the hope that a common framework will emerge for the community to evaluate and improve SCA countermeasures.

Power Port Countermeasures

We start with power port countermeasures. Since the correlated current is the source of power/EM side-channel leakage, most countermeasures proposed fall into this category.

Switched Capacitor Power Supply

Here, we discuss switched capacitor supply techniques to provide resilience against power SCAs. The crypto (e.g., AES) current is correlated and can be directly attacked via the power supply. The authors of [20] and [21] demonstrated the use of switched capacitors to decouple the power supply, achieving 10 million MTD. Figure 2(a) explains the operation. Phase 1 (P1) charges the capacitors (Cs); in P2, Cs is disconnected from V_{DD} and supplies the crypto logic, at the end of which an integrated value of the correlated information remains on Cs; and hence, in P3, Cs is discharged to a predefined fixed value to remove the residual information. Since discharging to zero wastes significant energy during every cycle, discharging to a fixed voltage was proposed, requiring additional analog circuit overhead. Since the stored charge on Cs supplies the AES, the voltage falls during P2, leading to a reduced-frequency operation and throughput reduction. A more advanced switched capacitor approach ([22], [23]) avoids resetting the capacitors. Instead, it uses two banks, charging and discharging, of multiple capacitors to create a time-varying transfer function (TVTF) between the correlated AES current and the power supply current, observable to the attacker. While multiphase switched capacitor power supplies with deterministic switching patterns are not very effective due to the same integrated residue, the TVTF randomly chooses capacitors from a charging bank to charge from V_{DD} and another randomly chosen capacitor from a discharging bank to discharge and supply the AES. This random mapping spreads the leakage information from one time instance to multiple random time instances, making the output appear significantly random, reducing correlation, and providing a 1,500× MTD improvement [24]. Additionally, using uneven capacitors adds distortion along with time variance, enhancing security to a 5,000× MTD increase. As with all SCA resilience techniques utilizing randomness, simple LFSRs are vulnerable; nested LFSRs may be usable, and true random number generators (TRNGs), especially with bias compensation, will provide the strongest protection. The work in [25] expanded switched capacitor SCA resilience from only the supply to both the supply and ground, creating a galvanically isolated AES engine with a 220× MTD increase while suffering from reduced throughput.

IVRs

The next power port countermeasures are IVRs, as shown in Figure 2(b). The authors of [26] and [27] first proposed that a buck regulator could be used for SCA resilience through inherent large signals transformations (switching frequency, duty cycle,

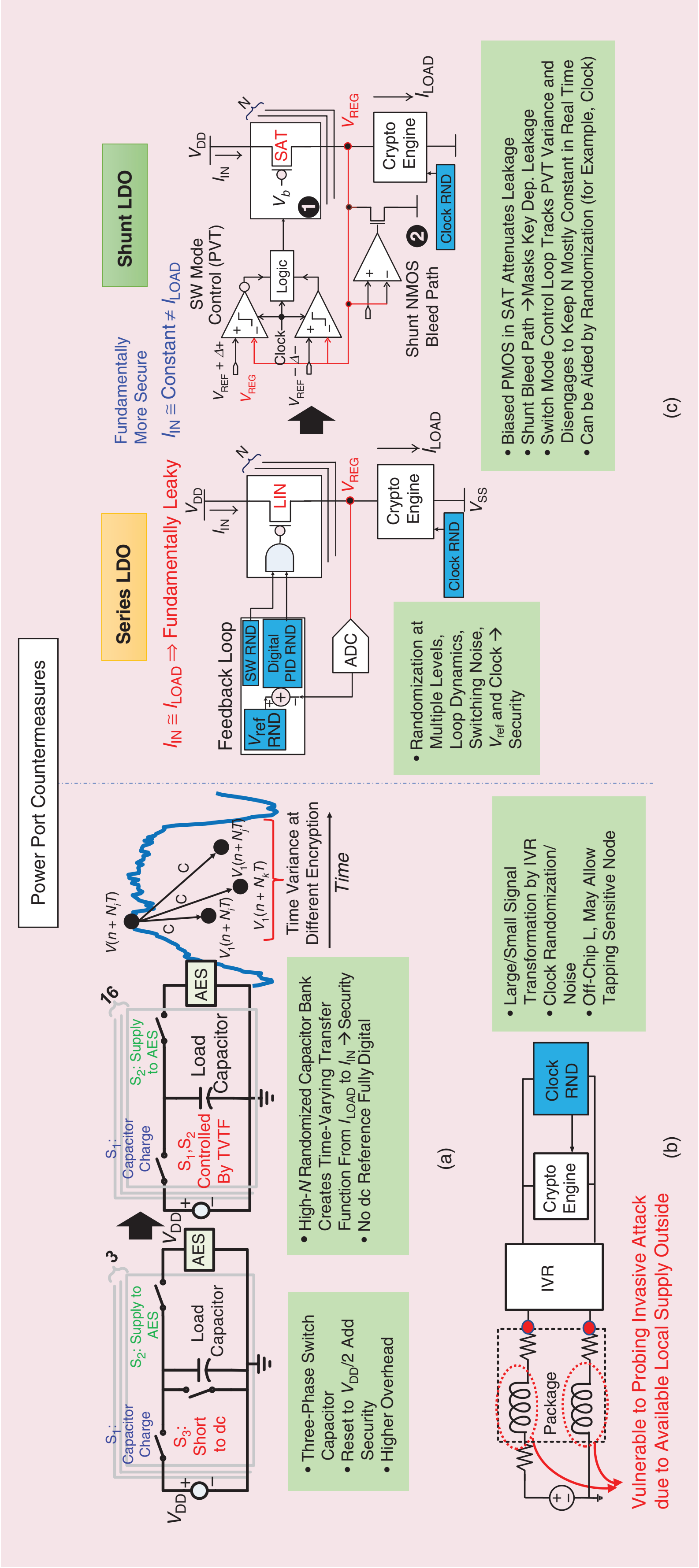

Power Port Countermeasures
V_{DD}
S_1: Capacitor Charge
S_3: Short to dc
S_2: Supply to AES
Load Capacitor
AES
3
16
S_1, S_2 Controlled By TVTF
$V(n+N_iT)$
C
$V_1(n+N_iT)$
$V_1(n+N_kT)$
$V_1(n+N_jT)$
Time Variance at Different Encryption
Time
• Three-Phase Switch Capacitor
• Reset to V_{DD}/2 Add Security
• Higher Overhead
• High-N Randomized Capacitor Bank Creates Time-Varying Transfer Function From I_{LOAD} to I_{IN} → Security
• No dc Reference Fully Digital
(a)
Package
IVR
Crypto Engine
Clock RND
Vulnerable to Probing Invasive Attack due to Available Local Supply Outside
• Large/Small Signal Transformation by IVR
• Clock Randomization/Noise
• Off-Chip L, May Allow Tapping Sensitive Node
(b)
Series LDO
$I_{IN} \cong I_{LOAD} \Rightarrow$ Fundamentally Leaky
Feedback Loop
Vref RND
SW RND
Digital PID RND
ADC
I_{IN}
V_{DD}
LIN
N
V_{REG}
Crypto Engine
Clock RND
I_{LOAD}
V_{SS}
• Randomization at Multiple Levels, Loop Dynamics, Switching Noise, V_{ref} and Clock → Security
Shunt LDO
Fundamentally More Secure
$I_{IN} \cong$ Constant $\neq I_{LOAD}$
SW Mode Control (PVT)
$V_{REF}+\Delta+$
V_{REG}
$V_{REF}-\Delta-$
Clock
Logic
V_b
SAT
1
2
Shunt NMOS Bleed Path
• Biased PMOS in SAT Attenuates Leakage
• Shunt Bleed Path → Masks Key Dep. Leakage
• Switch Mode Control Loop Tracks PVT Variance and Disengages to Keep N Mostly Constant in Real Time
• Can be Aided by Randomization (for Example, Clock)
(c)

FIGURE 2: The working principle of SCA countermeasures utilized at the power/V_{DD} port: (a) switched capacitor based, (b) IVR based, and (c) LDO based, including series LDO and shunt LDO, with the salient features highlighted for each. TVTF: time-varying transfer function; RND: randomization; SW: switch mode controller; dep: dependent.

and inductor/capacitor) and small signal transformations (pole-zero locations and loop delay) as well as intentionally introduced loop randomness, such as IVRs and AES clock misalignment. Fundamentally, the above techniques map the leakage to a different domain but do not reduce it significantly, as evidenced by an only 20× MTD improvement. Moreover, if, as in [27], the IVR inductor is outside, an attacker can just probe the IVR local supply node and mount an attack, removing any protection and making the IVR-based technique primarily effective only for emerging on-chip magnetic core elements, where the attack points are not exposed off chip. Follow-up work [28] combined an IVR buck with random frequency and voltage dithering to alter the power supply signature in time and amplitude. However, random clock misalignment proved ineffective since its location is visible in the power supply signature and can be factored into an attack. The work in [29] demonstrated a power injection attack breaking LFSR-based randomness in IVRs, leading to the proposal of the TRNG-based hysteresis controller loop for stronger security, which was later adopted in digital LDO-based countermeasures.

LDO Regulators

Similar to IVRs, modified digital LDOs can counteract power SCAs. Especially with the increasing use of micro-LDOs in modern SoCs, this becomes an attractive choice. We categorize LDO-based solutions into series LDO- and shunt LDO-based solutions and discuss the pros and cons of both in detail below:

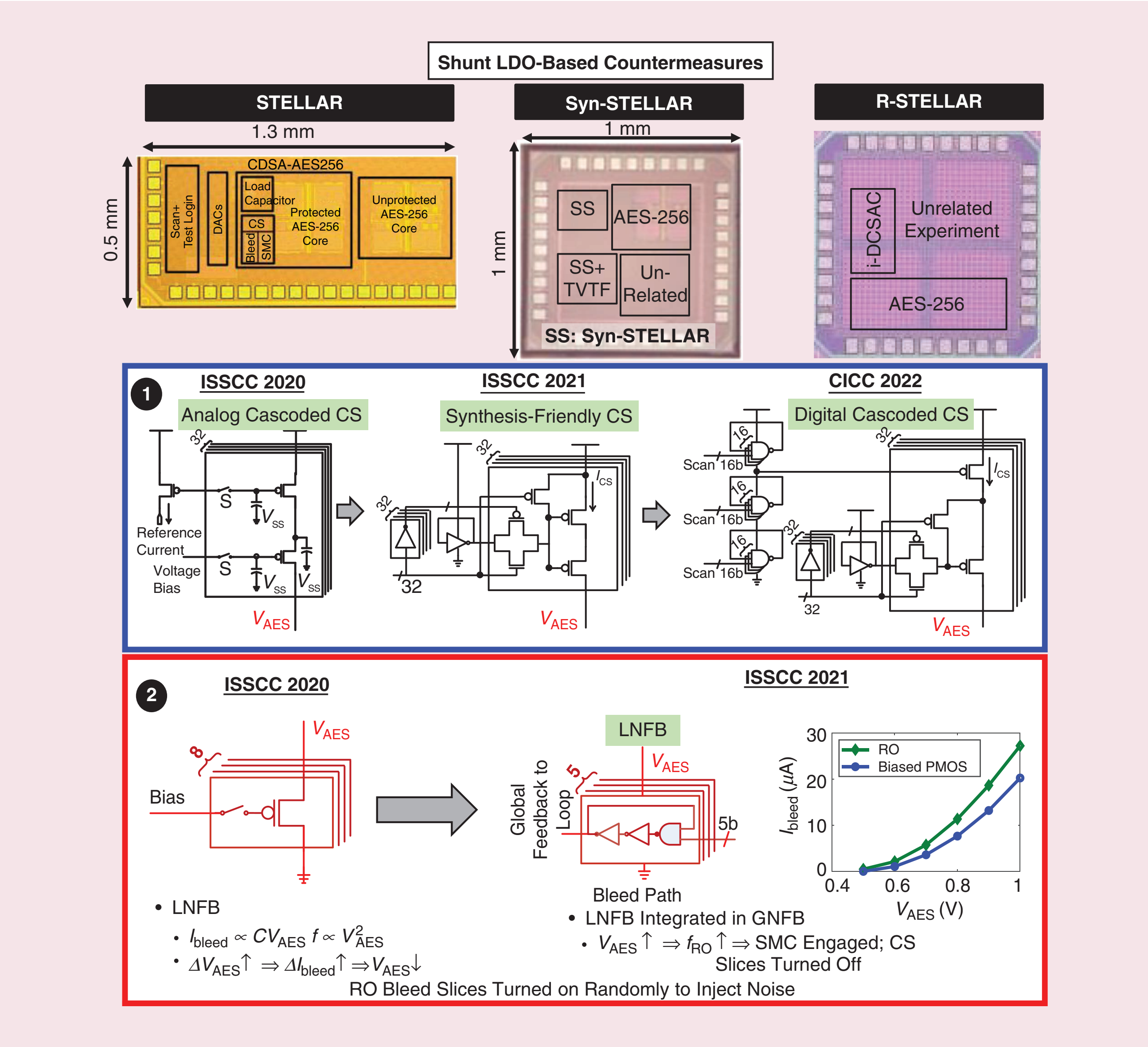
- *Series LDO-based countermeasures*: Figure 2(c), left, explains the operation of series LDOs, which is used for SCA resilience. The name arises from the fact that the regulating loop PMOS is in series with the digital load between the supply and ground. The regulated voltage is sensed, and the number of parallel PMOS slices, typically biased in the linear region as a switch in digital LDOs, are controlled dynamically to ensure that the current drawn from the supply equates to the varying current needed in the load, regulating V_{reg}. The work in [30] showed a ~3,500× MTD increase by using primarily multiple randomizations in the digital LDO loop, including random switching noise injection via power stage control, randomized reference voltage, and all-digital clock modulation. However, this design used the 2 nanofarad of the on-chip MIM capacitor, which may suffer from modulating the higher metal of the MIM cap, leading to additional EM SCA leakage and reducing the EM SCA MTD. An edge-chasing quantizer-based asynchronous digital low dropout regulator (DLDO) design was introduced [45], improving the MTD increase to 14,000×. Series LDO solutions rely on randomization to enhance SCA security. However, the primary goal of a series LDO [Figure 2(c)] is to make I_{supply} equal to I_{load}, which contradicts the SCA protection goal of making I_{supply} independent of I_{load}. The main security benefits come from randomized loops and noise injection techniques.
- *Shunt LDO-based countermeasures*: A shunt LDO, illustrated in Figure 2(c), right, on the other hand, utilizes a mostly fixed number of PMOS slices, biased in saturation, whereas regulation is provided by the shunt NMOS loop. Often, an additional top loop is used along with switched mode control to choose an optimum number of slices to counter PVT variation and then disengage, providing a current source-like behavior of the top PMOS and, hence, high output impedance. The authors of [31] and [32] first proposed that shunt LDOs might solve the above-mentioned fundamental contradiction by introducing an inline current source between the crypto load and the power supply, making I_{supply} mostly constant. Now the problem of supplying a varying load current from a constant source current is handled using on-chip LDO load capacitors supplying high-frequency components, and low-speed bleed path masking key-dependent dc current variations—local negative feedback (LNFB) in [22]—in conjunction with a global negative feedback (GNFB) loop, with switched mode digital control (SMC), change the average supplied current to be just above the average load current to counteract PVT and other variations. With carefully designed SMC, with an LSB size that is comparable to or more than what key-dependent current variations ensure, the GNFB is disengaged after adaptation, and key-dependent current variations do not show up in the supply, keeping I_{supply} mostly constant. Due to the finite route of current sources, the AT of the SCA signature is not infinite but can still be high (tens to hundreds), and the MTD improves by AT^2. This fundamentally new class of the physical signature AT countermeasure combined with lower-metal routing for reduced EM leakage [termed *Signature Attenuation Embedded Crypto With Low-Level Metal Routing* (*STELLAR*)] led to the first >1B MTD (a 125,000× increase) for both power and EM SCAs. Analog cascoded current sources (Figure 3) provide high output impedance and, hence, high AT, acting as a generic hard IP wrapper around any crypto core, enhancing SCA security. To address the need for scalable digital-friendly SCA solutions, synthesizable STELLAR [22], [23] employs a digital current source by using two stacked power gates biased by a self-biased inverter, at the expense of reduced AT yet achieving a >1.25B MTD by combining signature AT with a TVTF. In [33] and [46], improved AT with a digital-friendly current source was presented by separately biasing two power gates: the upper MOS, with a stacked tunable NAND gate (acting as a resistive divider), and the lower MOS, with a self-connected

inverter, mimicking analog cascoded current sources. Instead of an analog-biased PMOS bleed path as in [34], Syn-STELLAR introduced a synthesizable ring oscillator (RO) bleed as LNFB (Figure 3), utilizing the strong cubic dependence of an RO bleed current on the local crypto supply voltage. Moreover, the same RO count can be used as feedback to complete the GNFB loop, and the number of parallel RO slices can be randomly changed to introduce random noise, at the expense of varying loop gain. While not straightforward, a linear region attack on the signature AT countermeasure is possible by advanced attackers and could be thwarted by malicious voltage drop attack detection, as shown in [33]. Signature AT remains the strongest single-technique physical countermeasure in the published literature [Figure 5(b)].

Combining Countermeasures

An emerging trend in SCA resilience is digital circuit and arithmetic techniques applied directly on the crypto core. Unlike power and clock port countermeasures, these tend not to be generic but are easily implementable. These include the following:

1) *Arithmetic techniques [35], [36]*: By switching between heterogeneous substitution boxes (S-boxes) and randomizing the byte order, a time-variant data flow was created, yielding a 1,200× improvement, and the technique was later combined [15] with randomized nonlinear digital LDO to achieve protection of >1*B* CPA and CEMA MTD.
2) *Random additive masking [13]*: High overhead in SCA-resistant mode was accompanied by a fast



- LNFB
  - $I_{bleed} \propto CV_{AES}\, f \propto V^2_{AES}$
  - $\Delta V_{AES}\uparrow \Rightarrow \Delta I_{bleed}\uparrow \Rightarrow V_{AES}\downarrow$

- LNFB Integrated in GNFB
  - $V_{AES}\uparrow \Rightarrow f_{RO}\uparrow \Rightarrow$ SMC Engaged; CS Slices Turned Off

RO Bleed Slices Turned on Randomly to Inject Noise

FIGURE 3: The progressive evolution of the current source and shunt path for shunt LDO-based countermeasures. i-DCSAC: intelligent digital cascoded signature attenuation circuit; RO: ring oscillator; CDSA: current-domain signature attenuation; CS: current source.

Clock port countermeasures can be effectively combined with power port and arithmetic countermeasures for multiplicative benefits.

dual-core S-box to increase throughput when not in SCA mode. This required attack detection but achieved a 40,000× improvement.

3) *Multiplicative masking*: Multiplicative masking (MM) promises much lower overhead than additive masking but is vulnerable to zero-value attacks. The work in [12] used zero-value attack detectors in combinational MM to achieve a 34,000× improvement, reaching 850-M CPA and 1*B* CEMA MTD.

Clock Port Countermeasures

Digital circuits have two ports other than input and output: V_{DD} and clock. Countermeasures at the V_{DD} port are intuitive for power SCA, as described previously. Interestingly, the clock port also affects the SCA, as the distribution of the leaky points can be changed in the time domain, reducing the correlation or SNR of the measured leakage signal. There is a recent surge of clock port-based countermeasures, as discussed below.

Clock Randomization

Trace misalignment through clock randomization has been explored for some time now, which misaligns the power traces, making standard correlational attacks harder. However, clock randomization is often ineffective against postprocessing attacks like trace alignment and frequency domain analysis, as these techniques reduce the effect of misalignment.

Clock Slew

Recently, a clock slew technique introduced in [14] and [47] enhanced SCA resilience by exploiting digital circuits' inherent variability and noise as a function of clock slew. Figure 4(a) details the concept of how clock slew, introduced close to the clock port of the crypto core by using weak buffers (preferred due to their lower power requirements) or additional capacitive loading, helps achieve SCA resilience. Slew creates duty cycle distortion, as the clock may not have enough time for a full transition to the V_{DD} level. Notably, this is uneven, based on paths and different registers. Further, slew creates inconsistent latching times, as latching 1 and 0 are controlled by different buffered clock versions since the slew starts to reduce as it goes through more clock buffers, creating slew variability. These fundamental artifacts are aided by the Elmore delay effect and intradie process variation. Fundamentally, a small amount of slew does not significantly increase the probability of hold and setup time violation [as shown in Figure 4(b)] but can increase the uncorrelated variation [Figure 4(a), right]. Though the hold time increases, the Clk-Q delay increases too, and positive slack is always ensured for functional correctness.

Clock slew differs from clock skew, and the effect of clock skew on SCAs is yet to be explored. Clock slew countermeasures can be combined with clock randomization, reducing leaky frequency components and thwarting postprocessing attacks. Finally, clock port countermeasures can be effectively combined with power port and arithmetic countermeasures for multiplicative benefits.

EM-Specific Countermeasures

Most power SCA countermeasures also increase the global EM SCA resilience. However, local EM leakages picked up through fine-grain probes still may remain. This calls for EM-specific countermeasures:

- *Global cancellation*: To reduce EM side-channel leakage, multiple routing techniques have been explored. The work in [37] suggests routing in alternate directions which create *N*-pole magnetic dipole. This alternating routing strategy cancels near-field EM radiation in mm-cm distances, hence reduces meaningful leakage. The effect of different power grids has also been studied experimentally by [38] with eight different routing designs and showed benefits of 1.1–2.66× improvements, motivating further theoretical studies of the same.
- *Local lower-metal routing*: This avoids the routing of correlated current through higher-level metal layers. Routing the crypto core through lower-level metals and then passing the current through the signature AT block before passing the mostly constant current through field-canceling global routing promises the least EM SCA leakage.
- *Field-canceling standard cells*: Standard digital library cells are designed without consideration for their EM near-field leakage. It is possible to stack PMOS and NMOS transistors in a manner to cancel out fields and reduce EM leakage by 5×, as shown in [39].

Attack Detection

Both circuit-level and architectural countermeasures consume high overhead. The power overhead could be reduced by attack detection and and turning on the mitigation techniques only during an attack through event-driven duty cycling. This calls for the design of low-overhead power and EM attack detectors. Sense resistor and approaching probes introduces minimal change in observables such as instantaneous current or magnetic field. Hence, making attack detectors remains a hard problem and calls for further research.

Power Attack Detectors

Recently, a power attack detector [Figure 4(b), left] [40] was utilized via IR drop detection in the power supply line by forcing current pulses, leading to the need for stopping normal operation and higher overhead. Detectors that can detect power SCAs

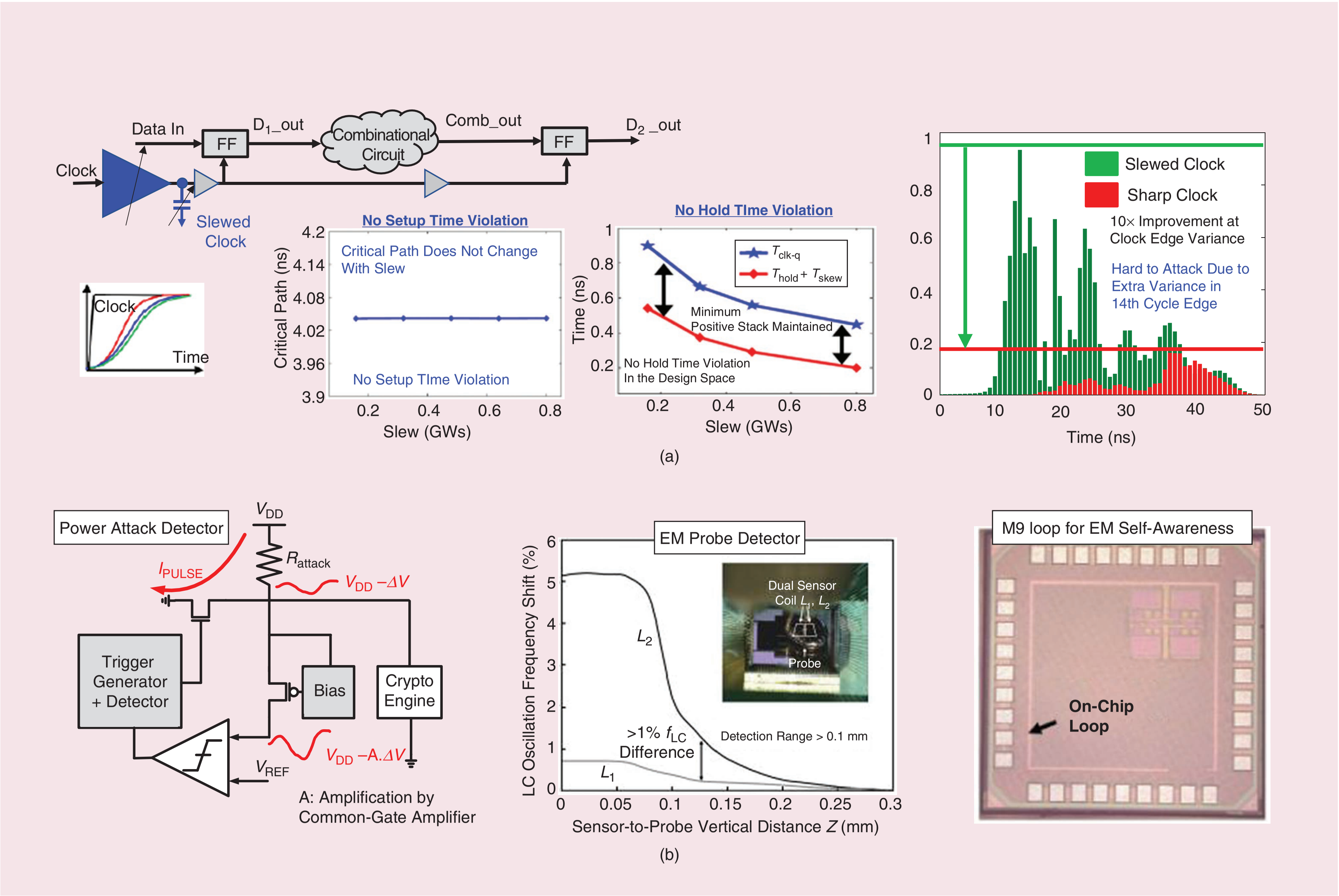


FIGURE 4: Different emerging techniques: (a) clock port-based techniques and (b) attack detectors, including power (left) and EM (middle and right).

while continuing encryption without significant additional current remain a desired solution.

EM Attack Detectors

One of the early EM detectors [Figure 4(b), middle] utilized the difference in mutual inductance of two on-chip loops with an approaching H-field probe, using oscillators and detecting a change in frequency successfully. Its efficacy might be limited to H-field probes and has been susceptible to spoofing by powering off the IC, bringing the attack probe close, and turning on the IC. To increase range and efficacy against all kinds of probes, capacitive sensor-based designs have been proposed that utilize the asymmetry of approaching probes to multiple on-chip structures. A simple on-chip loop included on the top metal layer [Figure 4(b), right] can serve multiple purposes, including detecting approaching probes, fault injection attacks, and providing EM self-awareness to the IC itself [41], [42]. Most of the attack detection techniques are still in the early stages. Further research is needed to establish effective detection and mitigation methods for commercially viable, low-overhead, and information-sensitive ICs.

Summary

The past decade has seen significant progress in circuit-level countermeasures for SCA resilience, which can be categorized into logical techniques (e.g., masking) and physical techniques that target the reduction of the SNR of the leakage signal, as shown in Figure 5(a). The security metric improves quadratically with the declining SNR, providing a strong motivation for circuit-level techniques that help attenuate the correlated current and EM signature (blue). While noise injection, by itself, can provide a similar benefit (gray), it comes either with compromised normal operation (e.g., randomization of the DLDO or IVR loop) or with a very high power cost (e.g., parallel current noise addition). Noise injection (e.g., randomization) in the attenuated signature leads to a multiplicative effect and provides the lowest overhead and highest-SCA-resilience countermeasures (green).

Figure 5(b) gives a comparative summary of the recent SCA resilience techniques discussed here. It is evident that logical countermeasures generally have a much higher overhead than physical countermeasures. The security community often prefers provable security measures for SCA. However, circuit-level techniques have low overhead and can be preferred from an industry point of view, especially in resource-constrained designs. Physical countermeasures typically do not provide guaranteed security; instead, they make an attack significantly harder, making it impractical. Since the security of a system is equal to its weakest link, the goal of physical countermeasures is to give protected crypto cores resilience that is orders of magnitude higher than that of the weakest link. Provable secure techniques (e.g., masking) have primarily focused on security quality and less on overhead. Research on low-overhead masking techniques should be explored to bridge the difference between the mathematics and circuit communities.

Future research calls for

1) more synthesizable physical countermeasures that utilize both signature AT and noise injection [the green area in Figure 5(a)] in optimized ways to increase resilience while reducing overhead (the top-left corner of Figure 5(b)]
2) significant reduction in the overhead of logical countermeasures
3) the combination of both low-overhead provably secure countermeasures with circuit-level countermeasures

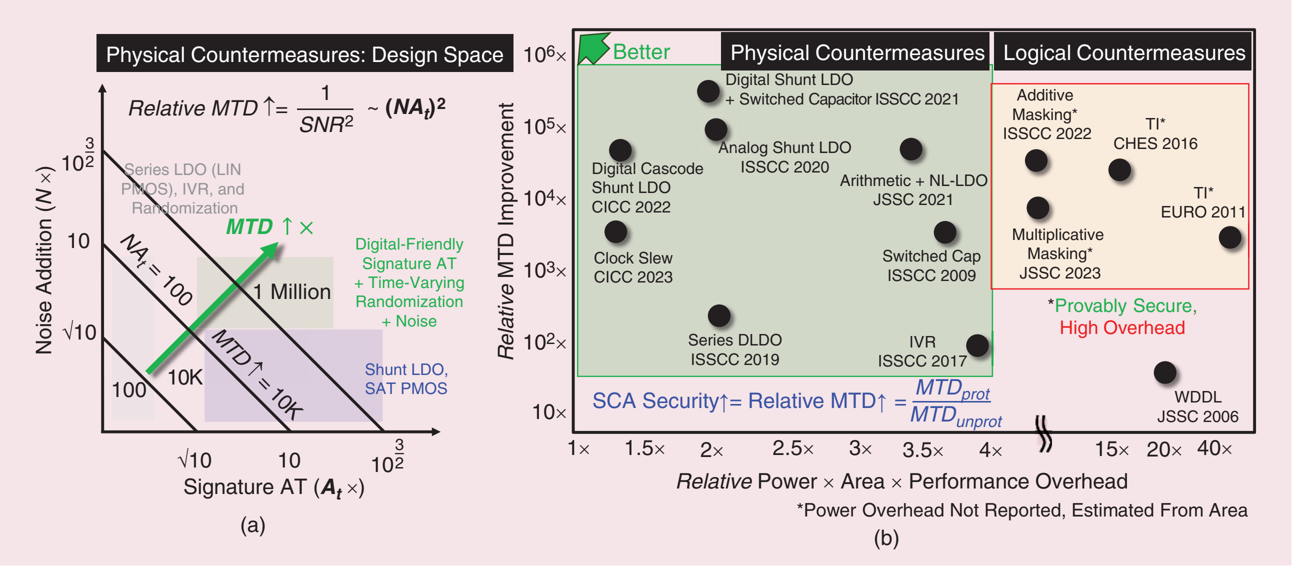


FIGURE 5: The SCA research landscape in the SCA community: (a) the design space of physical countermeasures as a function of the two key basis vectors and (b) a comparison of prominent techniques with respect to SCA resilience efficacy versus PPA overhead. ISSCC: International Solid-States Circuits Conference; CICC: IEEE Custom Integrated Circuits Conference; *JSSC: IEEE Journal of Solid-State Circuits;* IVR: integrated voltage regulator; CHES: Conference on Cryptographic Hardware and Embedded Systems; EURO: IEEE European Symposium on Security and Privacy.

4) SCA resilience against emerging attacks, such as fault injection-aided SCAs
5) SCA resilience against other modalities of leakage, such as photonic SCAs and thermal SCAs
6) low-overhead attack detectors for both power and EM attacks.

Finally, the field is still emerging, with significant research potential, but calls for a common framework for the evaluation of different designs and close collaboration with security communities, like the Conference on Cryptographic Hardware and Embedded Systems, IEEE International Symposium on Hardware Oriented Security and Trust, and IEEE Symposium on Security and Privacy. Finally, increased interaction between primary circuit designers and primary attackers will help improve the quality of countermeasures.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO, Lecture Notes in Computer Science*, M. Wiener, Ed., Berlin, Germany: Springer-Verlag, Aug. 1999, pp. 388–397.

[2] P. Prinetto et al., "Hardware security, vulnerabilities, and attacks: A comprehensive taxonomy," in *Proc. Italian Conf. Cybersecur.*, 2020, pp. 177–189.

[3] M. M. Ahmadi, F. Khalid, and M. Shafique, "Side-channel attacks on RISC-V processors: Current progress, challenges, and opportunities," 2021, *arXiv:2106.08877*.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman.* Cambridge, MA, USA: MIT Press, 2022, pp. 365–390.

[5] D. Joan and R. Vincent, "The design of Rijndael: AES-the advanced encryption standard," *Inf. Secur. Cryptogr.*, vol. 196, 2002.

[6] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "ASCON v1. 2: Lightweight authenticated encryption and hashing," *J. Cryptol.*, vol. 34, no. 3, pp. 1–42, 2021, doi: 10.1007/s00145-021-09398-9.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978, doi: 10.1145/359340.359342.

[8] J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Piscataway, NJ, USA: IEEE Press, 2018, pp. 353–367, doi: 10.1109/EuroSP.2018.00032.

[9] T. D. Cnudde, O. Reparaz, B. Bilgin, S. Nikova, V. Nikov, and V. Rijmen, "Masking AES with shares in hardware," in *Proc. Int. Conf. Cryptogr. Hardware Embedded Syst.*, Berlin, Germany: Springer-Verlag, 2016, pp. 194–212.

[10] L. De Meyer, O. Reparaz, and B. Bilgin, "Multiplicative masking for AES in hardware," *IACR Trans. Cryptographic Hardware Embedded Syst.*, vol. 2018, no. 3, pp. 431–468, 2018, doi: 10.46586/tches.v2018.i3.431-468.

[11] B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen, "Higher-order threshold implementations," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2014, pp. 326–343.

[12] R. Kumar et al., "A 7-Gbps SCA-resistant multiplicative-masked AES engine in intel 4 CMOS," *IEEE J. Solid-State Circuits*, vol. 58, no. 4, pp. 1106–1116, Apr. 2023, doi: 10.1109/JSSC.2022.3230372.

[13] R. Kumar et al., "An 8.3-to-18Gbps reconfigurable SCA-resistant/dual-core/blind-bulk AES engine in Intel 4 CMOS," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Piscataway, NJ, USA: IEEE Press, 2022, pp. 1–3, doi: 10.1109/ISSCC42614.2022.9731739.

[14] A. Ghosh, M. A. Rahman, D. Das, S. Ghosh, and S. Sen, "Power and EM SCA resilience in 65nm AES-256 exploiting clock-slew dependent variability in CMOS digital circuits," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Piscataway, NJ, USA: IEEE Press, 2023, pp. 1–2, doi: 10.1109/CICC57935.2023.10121240.

[15] R. Kumar et al., "A SCA-resistant AES engine in 14nm CMOS with time/frequency-domain leakage suppression using non-linear digital LDO cascaded with arithmetic countermeasures," in *Proc. IEEE Symp. VLSI Circuits*, Piscataway, NJ, USA: IEEE Press, 2020, pp. 1–2, doi: 10.1109/VLSICircuits18222.2020.9162988.

[16] T. Schneider and A. Moradi, "Leakage assessment methodology: Extended version," *J. Cryptographic Eng.*, vol. 6, no. 2, pp. 85–99, 2016, doi: 10.1007/s13389-016-0120-y.

[17] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, and S. Sen, "X-DeepSCA: Cross-device deep learning side channel attack," in *Proc. 56th ACM/IEEE Design Automat. Conf. (DAC)*, Jun. 2019, pp. 1–6.

[18] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. 28th Eur. Solid-State Circuits Conf.*, Florence, Italy, Sep. 2002, pp. 403–406.

[19] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18um CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006, doi: 10.1109/JSSC.2006.870913.

[20] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *Proc. IEEE Int. Solid-State Circuits Conf. - Dig. Tech. Papers*, Feb. 2009, pp. 64–65,65a, doi: 10.1109/ISSCC.2009.4977309.

[21] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010, doi: 10.1109/JSSC.2009.2034081.

[22] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "36.2 an EM/power SCA-resilient AES-256 with synthesizable signature attenuation using digital-friendly current source and RO-bleed-based integrated local feedback and global switched-mode control," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Piscataway, NJ, USA: IEEE Press, 2021, pp. 499–501, doi: 10.1109/ISSCC42613.2021.9365978.

[23] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-STELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2021, doi: 10.1109/JSSC.2021.3113335.

[24] A. Ghosh, D. Das, and S. Sen, "Physical time-varying transfer function as generic low-overhead power-SCA countermeasure," *IEEE Open J. Circuits Syst.*, vol. 4, pp. 228–240, 2023, doi: 10.1109/OJCAS.2023.3302254.

[25] M. Wang et al., "Galvanically isolated, power and electromagnetic side-channel attack resilient secure AES core with integrated charge pump based power management," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Piscataway, NJ, USA: IEEE Press, 2021, pp. 1–2, doi: 10.1109/CICC51472.2021.9431524.

[26] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, USA, Feb. 2017, pp. 142–143, doi: 10.1109/ISSCC.2017.7870301.

[27] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018, doi: 10.1109/JSSC.2018.2822691.

[28] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," *IEEE J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, Feb. 2019, doi: 10.1109/JSSC.2018.2875112.

[29] W.-H. Yang et al., "An enhanced-security buck DC-DC converter with true-random-number-based pseudo hysteresis controller for internet-of-everything (IOE) devices," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Piscataway, NJ, USA: IEEE Press, 2018, pp. 126–128.

[30] A. Singh et al., "25.3 A 128b AES engine with higher resistance to power and electromagnetic side-channel attacks enabled by a security-aware integrated all-digital low-dropout regulator," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Feb. 2019, pp. 404–406, doi: 10.1109/ISSCC.2019.8662344.

[31] D. Das et al., "27.3 EM and power SCA-resilient AES-256 in 65nm CMOS through >350× current-domain signature attenuation," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Piscataway, NJ, USA: IEEE Press, 2020, pp. 424–426, doi: 10.1109/ISSCC19947.2020.9062997.

[32] D. Das et al., "EM and power SCA-resilient AES-256 through> 350× current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021, doi: 10.1109/JSSC.2020.3032975.

[33] A. Ghosh, D.-H. Seo, D. Das, S. Ghosh, and S. Sen, "A digital cascoded signature attenuation countermeasure with intelligent malicious voltage drop attack detector for EM/power SCA resilient parallel AES-256," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Piscataway, NJ, USA: IEEE Press, 2022, pp. 01–02, doi: 10.1109/CICC53496.2022.9772853.

[34] 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 *Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20, doi: 10.1109/HST.2019.8740839.

[35] R. Kumar et al., "A 4900×m2 839Mbps side-channel attack resistant AES-128 in

14nm CMOS with heterogeneous sboxes, linear masked mixcolumns and dual-rail key addition," in *Proc. Symp. VLSI Circuits*, Piscataway, NJ, USA: IEEE Press, 2019, pp. C234–C235, doi: 10.23919/VLSIC.2019.8778041.

[36] R. Kumar et al., "A 4900-μ m^2 839-mb/s side-channel attack-resistant AES-128 in 14-nm CMOS with heterogeneous Sboxes, linear masked MixColumns, and dual-rail key addition," *IEEE J. Solid-State Circuits*, vol. 55, no. 4, pp. 945–955, Apr. 2020, doi: 10.1109/JSSC.2019.2960482.

[37] M. Nath, D. Das, and S. Sen, "A multipole approach toward on-chip metal routing for reduced EM side-channel leakage," *IEEE Microw. Wireless Compon. Lett.*, vol. 31, no. 6, pp. 685–688, Jun. 2021, doi: 10.1109/LMWC.2021.3062809.

[38] M. Wang et al., "Physical design strategies for mitigating fine-grained electromagnetic side-channel attacks," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Piscataway, NJ, USA: IEEE Press, 2021, pp. 1–2, doi: 10.1109/CICC51472.2021.9431438.

[39] D. Das et al., "EM SCA white-box analysis-based reduced leakage cell design and Presilicon evaluation," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 11, pp. 4927–4938, Nov. 2022, doi: 10.1109/TCAD.2022.3144369.

[40] S. J. Kim, D. Kim, A. Sharma, and M. Seok, "EQZ-LDO: A near-zero EDP overhead, > 10m-attack-resilient, secure digital LDO featuring attack-detection and detection-driven protection for a correlation-power-analysis-resilient IoT device," in *Proc. Symp. VLSI Circuits*, Piscataway, NJ, USA: IEEE Press, 2021, pp. 1–2, doi: 10.23919/VLSICircuits52068.2021.9492345.

[41] A. Ghosh, M. Nath, D. Das, S. Ghosh, and S. Sen, "Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection," *IEEE Microw. Wireless Compon. Lett.*, vol. 32, no. 6, pp. 784–787, Jun. 2022, doi: 10.1109/LMWC.2022.3161001.

[42] E. Ronen, A. Shamir, A. -O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, 2017, pp. 195–212, doi: 10.1109/SP.2017.14.

[43] O. Lisovets, D. Knichel, T. Moos, and A. Moradi, "Let's take it offline: Boosting brute-force attacks on iPhone's user authentication through SCA," in *IACR Trans. Cryptographic Hardware Embedded Syst.*, 2021, pp. 496–519.

[44] T. Roche, V. Lomné, C. Mutschler, and L. Imbert, "A side journey to titan," in *Proc. 30th USENIX Security Symp. (USENIX Security)*, 2021, pp. 231–248.

[45] Y. He and K. Yang, "25.3 A 65nm edge-chasing quantizer-based digital LDO featuring 4.58ps-FoM and side-channel-attack resistance," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2021, pp. 384–386.

[46] A. Ghosh, D. H. Seo, D. Das, S. Ghosh, and S. Sen, "R-STELLAR: A resilient synthesizable signature attenuation SCA protection on AES-256 with built-in attack-on-countermeasure detection," 2024, *arXiv:2408*.12021.

[47] A. Ghosh, A. Rahman, D. Das, S. Ghosh, and S. Sen, "Exploiting clock-slew dependent variability in CMOS digital circuits towards power and EM SCA resilience," Cryptology ePrint Archive, 2024, Paper 2024/1019.

About the Authors

Shreyas Sen (shreyas@purdue.edu) is an Elmore Associate Professor of electrical and computer engineering and biomedical engineering at Purdue University, West Lafayette, IN 47906 USA. His research interests include mixed-signal circuits/systems and electromagnetics for the Internet of Bodies and hardware security. He has authored/coauthored three book chapters and over 200 journal and conference papers, and he has 25 patents granted/pending. He serves as the director of the Center for Internet of Bodies, Purdue University. He is the inventor of Electro–Quasistatic Human Body Communication, or body-as-a-wire technology, for which he was named an MIT Technology Review top 10 worldwide Indian inventor under 35 in 2018 and a winner of the Georgia Tech 40 Under 40 Award in 2022. To commercialize this invention, he founded Ixana and serves as the chairman and chief technology officer, leading the company to awards such as the 2024 CES Innovation Award, EE Times Silicon 100, and 2023 Indiana Startup of the Year Mira Award. His work has been covered by 250+ news outlets worldwide, and he has been invited to appear on TEDxIndianapolis, NASDAQ TradeTalks at the 2023 Consumer Electronics Show, the CNBC TV18 *Young Turks* program, Lakeshore Public Radio, and the CyberWire podcast. He is a recipient of the 2020 National Science Foundation (NSF) CAREER Award, 2016 Air Force Office of Scientific Research Young Investigator Award, 2017 NSF Directorate for Computer and Information Science and Engineering Computer and Information Science and Engineering Research Initiation Initiative Award, Intel Outstanding Researcher Award, 2017 Google Faculty Research Award, 2021 Purdue College of Engineering Early Career Research Award, 2012 Intel Labs Quality Award for industry-wide impact on USB-C, 2010 Intel Ph.D. Fellowship, 2008 IEEE Microwave Fellowship, 2007 Gigascale System Research Center Margarida Jacome Best Research Award, and nine best paper awards, including at the 2019 and 2021 IEEE Custom Integrated Circuits Conference (CICC) and the 2017–2020 IEEE International Symposium on Hardware Oriented Security and Trust. His work was chosen as one of the top 10 papers in the hardware security field (TopPicks 2019). He serves/has served as an associate editor for *IEEE Solid-State Circuits Letters*, *Scientific Reports*, *Frontiers in Electronics*, and *IEEE Design & Test*. He is an executive committee member of IEEE Central Indiana Section and a technical program committee member of the International Solid-State Circuits Conference, CICC, Design Automation Conference, ACM Conference on Computer and Communications Security, IEEE Microwave Theory and Technology Society International Microwave Symposium, Design Automation and Test in Europe conference, ACM/IEEE International Symposium on Low Power Electronics and Design, International Conference on Computer-Aided Design, and International VLSI Design & Embedded Systems conference. He is a Senior Member of IEEE.

Archisman Ghosh (ghosh69@purdue.edu) received his B.E. degree in electronics and telecommunication engineering from Jadavpur University, India, in 2017. He is pursuing his Ph.D. degree at Purdue University, West Lafeyette, IN 47906 USA, where he was a recipient of the Meissner Fellowship in electrical and computer engineering (2019–2020) as an incoming graduate student and is a Bilsland Dissertation fellow. His research interests include digital system-on-chip design and hardware security. Prior to his Ph.D., he worked at Samsung Semiconductor India Research for two years, and he has interned with Intel Labs. He was the recipient of the 2022 IEEE Solid-State Circuits Society Predoctoral Achievement Award. He is a Student Member of IEEE.