

Screaming Channel: Recent Advances in Far Field EM Side-Channel Attacks based on Radio Coupling

Huanyu Wang^{1,2}, Pei Cao¹, Chi Zhang^{1,*}, Dawu Gu^{1,*}

1. Shanghai Jiao Tong University, Shanghai, China.

2. Hunan University of Science and Technology, Xiangtan, China.

*. Correspondence: Chi Zhang (zcsjtu@sjtu.edu.cn) and Dawu Gu (dwgu@sjtu.edu.cn).

Abstract—The Internet of Things (IoT) is revolutionizing society by enabling anytime, anywhere connectivity, but its widespread deployment also makes IoT devices attractive targets for malicious activities. Over the past decade, radio-coupling based Far-field EM Side-Channel Attacks (FEM-SCAs), also known as screaming channel attacks, have emerged as a new threat to these wireless IoT edges. Unlike conventional power or near-field EM side-channel attacks, FEM-SCAs exploit the unintended coupling between digital computation and the Radio Frequency (RF) transmission chain, allowing sensitive information to be captured through radiated radio signals at long distances. Since the first screaming-channel demonstration, this field has progressed rapidly: attacks have become more efficient, DL-enabled methods have been developed, and recent studies have begun to examine more realistic wireless-protocol settings. Despite existing practical cases of remote FEM-SCA attacks, the literature remains fragmented. To systematically understand this security threat and to aid future countermeasure design, this paper presents the first systematic survey of existing screaming channel attack methodologies and case studies. We organize studies into a hierarchical framework covering leakage discovery and understanding, enhanced attack capability, attack targets and variants, and public data collections. Through a fine-grained cross-paper analysis, we compare representative works in terms of target implementation, attack distance, analysis method, profiling requirement, acquisition environment, and other factors. Building on this end-to-end review, we provide a focused discussion that distills FEM-SCA research into one central trade-off, three major limitations, and three future research roadmaps. Taken together, this survey offers a structured framework for understanding a rapidly developing far-field side-channel attack class, and provides practical guidance for evaluating its real-world threat boundaries.

Index Terms—Side-channel attack, screaming channel, far-field EM radiation, radio frequency, deep learning.

I. INTRODUCTION: FROM DIGITAL LEAKAGE TO RADIO

“He made my heart beat like radio. It used to go dum dum dadadada dum...”

SIDE-CHANNEL ATTACKS (SCAs) have become an increasingly prominent threat to the security of modern computing systems, particularly with the rapid expansion of embedded edge device deployment. The very silicon hearts of electronic devices, from sensors to controllers, may disclose sensitive information through physical leakage. During the processing of sensitive executions, the material nature of these embedded systems becomes a vulnerability, producing invisible data traces through power fluctuations, electromagnetic (EM) emissions, computational timing variations, and

others. By exploiting these non-prime, unintentional physical leakage generated during the execution of embedded systems, the adversaries can eventually recover the secret data. These are called SCAs. During the past two decades, various side channels have been investigated in various malicious activities. These include compromising cryptographic implementations [1]–[3], reverse neural networks’ architecture [4]–[6], stealing intellectual property [7], monitoring user-browser information [8], [9], predicting random number generators [10], tracking the code execution [11], [12], and private user identities [13]–[16], and attack the file systems [17].

Traditional SCAs are typically divided according to the leakage source they exploit: power analysis observes data-dependent power consumption [18]; timing analysis measures execution-time variations caused by secret-dependent operations [19]; near-field EM analysis captures localized electromagnetic radiation from switching circuits [20]; optical analysis detects voltage-induced optical changes in silicon [21]; and acoustic analysis extracts information from sound or vibration produced by electronic components [22]. Although these side channels have been highly effective in laboratory and evaluation settings, their threat model is usually constrained by the measurement interface. Power attacks often require physical contact with the chip, near-field EM attacks require probes placed close to the board, and optical attacks may require visibility of the die or package-level access. Therefore, conventional SCAs are generally constrained by the need for physical proximity, which may limit their practicality in scenarios where the attacker cannot obtain physical access to the victim device.

In 2018, a new type of side channel has been discovered, called **Far-field EM Side-Channel Attacks** (FEM-SCAs), also known as **Screaming Channel** attacks, introduced by Camurati et al. at the 2018 CCS conference [23]. This is considered a growing threat as the side-channel attack can be conducted remotely, without physical proximity to the target device. In the novel FEM-SCAs, by exploring the coupling effect between EM emissions from the CPU core and radio carrier signals on mixed-signal chips, adversaries are feasible to eliminate the requirement of the access to the victim device, which makes the attack increasingly convert (as shown in Fig. 1). Considering that the core components of widely deployed IoT edge devices are predominantly mixed-signal chips, the security threats posed by FEM-SCAs might be broader than expected. This method of attack capitalizes on

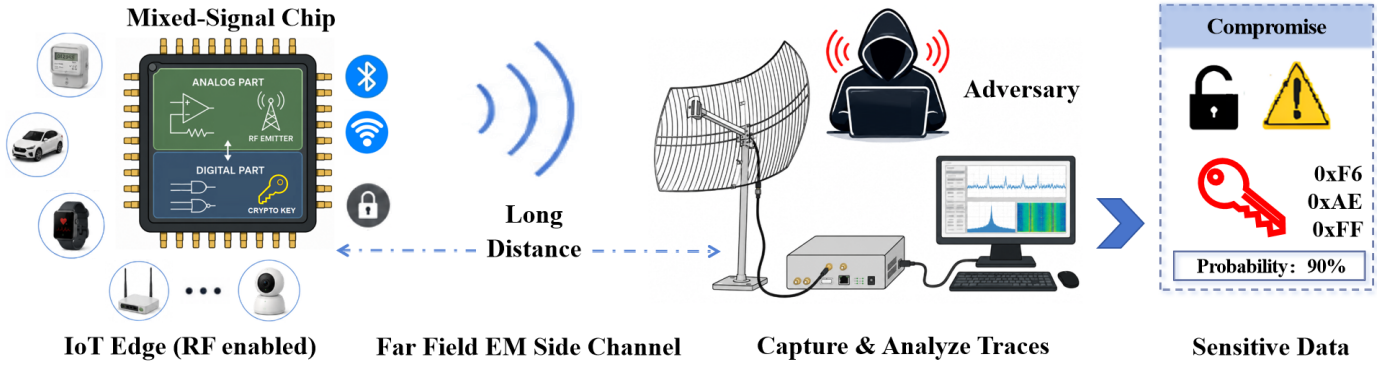


Fig. 1: Illustration of how screaming channel attacks can cause long-range threats to RF-enabled devices.

radio transmitters integrated into chips, permitting sensitive data to inadvertently modulate radio frequency signals, which are subsequently disseminated through the airwaves. Practical attack cases have been demonstrated remotely to successfully compromise Bluetooth device implementations of AES [23], [24], eavesdrop on clear-text data [25], and recover the key from protected crypto [26].

While some reviews on side-channel attacks exist [27]–[32], their coverage remains incomplete and insufficient for a comprehensive understanding of screaming channels. [33] concluded the conventional SCAs approaches, such as Differential Power Analysis (DPA) [18], Template Attacks (TAs) [34], Correlation Power Analysis (CPA) [35], and Test Vector Leakage Assessment (TVLA) [36]. Afterwards, Hettwer et al. reviewed the attacks based on Machine Learning (ML) techniques in [27], such as the Support Vector Machine (SVM), Decision Trees (DTs) and Random Forest (RF). In 2023, Picek et al. [29] provided a systematically review of Deep-Learning Side-Channel Attacks (DLSCAs) in the journal of ACM Computing Surveys, across a broad range of applications but with a specific focus on power and near-field EM analysis. In addition, [30] narrowed the focus scope to the timing analysis. In 2025, Picek et al. [31] investigated the up-to-date SCAs on implementations of Post-Quantum Cryptography (PQC) implementations by using the power consumption and near field EM radiation as side channels. Afterwards, the review in [32] specifically paid interest to side-channel attacks on Branch Prediction Unit (BPU). However, despite the growing body of research on FEM-SCAs, there remains a critical gap in the systematization and consolidation of existing knowledge. In 2026, [37] provided a high-level enumeration of screaming-channel-related studies, but offers limited technical detail and does not present a systematic taxonomy or in-depth comparative analysis. To better understand the threats to IoT security posed at radio frequencies and to aid in formulating countermeasures against screaming-channel attacks in the future, it is necessary to investigate the extent to which FEM-SCA techniques succeed under varying conditions. Building on these foundational insights, we advance the field by conducting the first in-depth, systematic survey of existing screaming channel attacks, analyzing their implications across scenarios, from the attack methodologies and practical case studies.

Before organizing the literature, it is necessary to clarify

the terminology used to describe this emerging attack class, since existing works have not yet adopted a unified name for it. In existing studies, related works have been referred to as screaming channel attacks, far-field EM side-channel attacks, Radio-Frequency Wireless Side-Channel Attacks (RF-WSCAs), or some related works call this type of attack as Amplitude-Modulated EM Side-Channel Attacks (AM-SCAs). Although these terms differ in wording, they essentially describe the same leakage mechanism first revealed by the CCS’18 screaming-channel work [23], in which the data-dependent activity from the digital core of a mixed-signal chip couples into the radio module and is unintentionally transmitted through the antenna, which is further captured by adversaries remotely to analyze the secret information. Therefore, in this section, we consider these studies as belonging to the same research line and, in the following discussion, we **uniformly refer to them as screaming channel attacks, or FEM-SCAs for short**. This follows the naming rule in two of the early publications in screaming channels [23], [38].

A. Contributions and Paper Structure

- **The first comprehensive survey of FEM-SCA.** This paper presents the first comprehensive survey dedicated to screaming channel attacks, addressing the lack of systematic understanding of this emerging remote side-channel threat. The framework covers four major dimensions: discovery and understanding, enhanced attack capability and practicality, attack targets and variants, and public FEM-SCA data collections, as shown in Figure 2. By combining scope clarification with structured taxonomy, this survey shows how the field has evolved from proof-of-concept demonstrations toward practical far-field threats.
- **A fine-grained analysis of representative studies.** Beyond summarizing existing works, this paper provides a cross-work analysis of representative studies from multiple technical dimensions, including the target implementation, attack distance, attack method, profiling requirement, key-enumeration complexity, acquisition environment, and other factors. By comparing these aspects across detailed chronological tables and visual aids, the survey allows readers to understand not only which

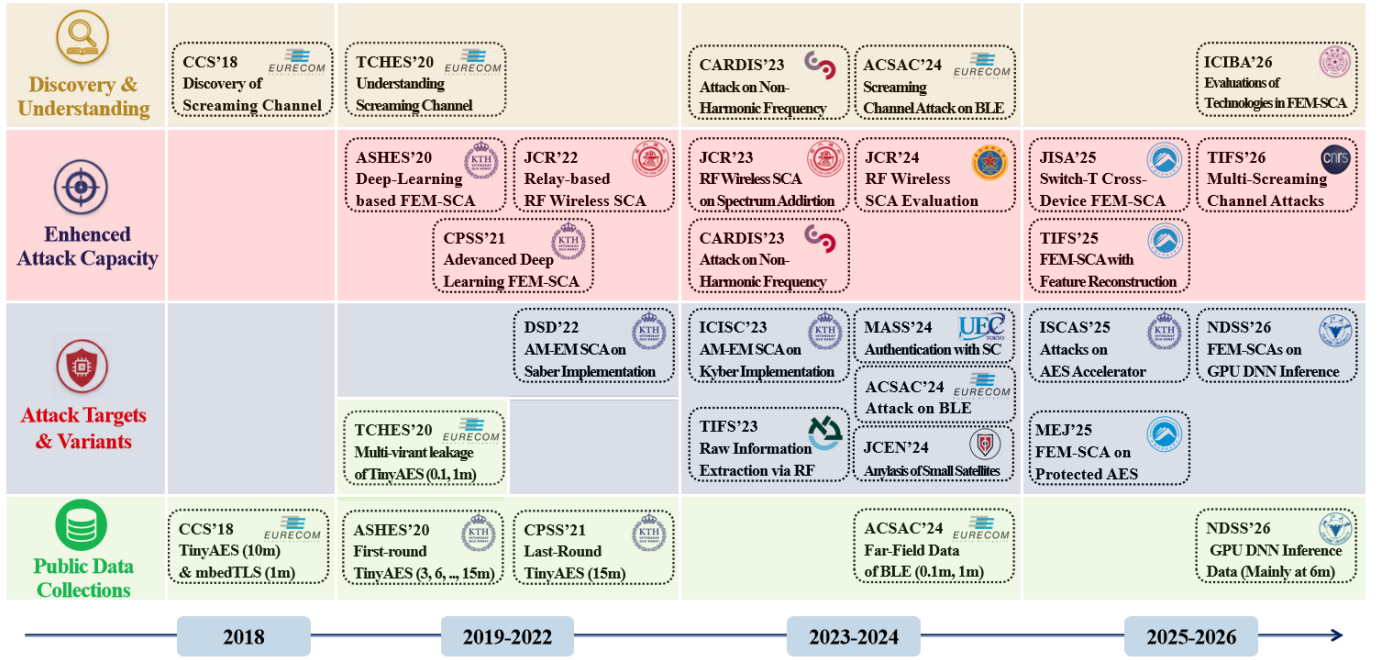


Fig. 2: A chronological overview of the development of screaming channel attacks (key-node works included).

attacks have been demonstrated, but also under what assumptions, with what cost, and with what level of practical threat realism.

- **A boundary-aware discussion of open challenges.** This survey identifies the key unresolved challenges that currently limit FEM-SCA research, such as the efficiency-distance trade-off, the limited generality of results beyond the commonly tested platforms, the lack of quantitative evidence for non-Bluetooth RF protocols, and the absence of structured benchmarks collected under unified experimental settings. These challenges clarify the current boundary of FEM-SCA research and outlines future research directions.

Notice that this survey adopts a selective approach to its source material. While valuable contributions have been made to the field, including notable Master theses such as [39]–[41], our analysis is confined to works published in high-reputation conferences and journals. This criterion guarantees that the discussed attacks meet a recognized standard of peer review and academic credibility, providing a robust foundation for our comparative study. Besides, we narrow down the scope of this survey to attack cases based on the RF-coupled screaming channels with a capturing frequency located at Ultra High Frequency (UHF). Consequently, other remote side-channel attacks, such as TEMPEST (Transient Electromagnetic Pulse Emanation Standard) [42], [43], EMIRIS (EM on IRIS) attacks [44] and remote EM attacks [45], which leverage the EM emanations not coupled to an RF communication carrier, are beyond its scope.

The structure of the paper is as below. Section II introduces a brief overview of side-channel attacks and how deep-learning techniques can support SCAs. Section III provides a technical explanation of how chip-level side-channel leakage can couple

into radio signals and be captured at long distances. Next, Section IV reviews the discovery and early understanding of screaming-channel leakage, with emphasis on its physical origin, coupling mechanism, and initial attack demonstrations. Section V summarizes the evolution of enhanced attack capability and practicality, highlighting how FEM-SCA has progressed in terms of attack efficiency, attack distance, signal acquisition, and robustness in different environments. Section VI further discusses attack targets and variants, and Section VII introduces existing public screaming channel data collections. Finally, Section VIII presents open challenges and future research directions, and Section IX summarizes this survey.

II. BACKGROUND

This section begins with a brief overview of side-channel attacks and then discusses how deep-learning techniques can be used to enhance the capability of SCAs.

A. Side-Channel Attack

Side-channel attacks aim to recover sensitive information from electronic devices by exploiting the unintentional and unavoidable physical leakage, such as power consumption and EM emissions, generated during the execution of the target device [46], [47]. Unlike traditional cryptanalysis, SCAs bypass the theoretical and mathematical strength of cryptography, effectively treating the running device as a secret teller against its will.

In the community, side-channel attacks are commonly classified into two categories: *non-profiled* and *profiled*. Non-profiled attacks aim to directly compromise the cryptographic implementations, exemplified by techniques like DPA [18] or CPA [35]. Profiled attacks begin by learning a leakage

profile that establishes a connection between the captured side-channel measurements and the key-dependent sensitive intermediate value of the cryptographic algorithm. This learned profile is then utilized to carry out the attack. In most cases, profiled attacks generally demonstrate superior attack performance compared to non-profiled attacks under the same attack condition. For example, a deep-learning based power analysis (in profiled setting) can recover the subkey of an AES implementation on an ATXmega128D4 MCU with only a single trace, while CPA typically demands approximately 50 traces to achieve a comparable success rate [48]. However, it is necessary to highlight that setting up profiled attacks typically involves significantly more preparation costs than non-profiled attacks. In order to understand the leakage profile of the device for all potential values of the sensitive intermediate state, adversaries are required to have full control over one or more copies of the victim device, called profiling device(s), to capture an extensive number of side-channel traces and associated data to construct the leakage profile. Template attacks [34], as an example, utilize traces obtained from the profiling device to generate a set of probability distributions. These distributions are then employed to characterize traces according to the corresponding key-dependent intermediate value.

B. Deep-Learning in SCAs

In the last two decades, the advance in deep learning techniques have made SCAs significant more threatening. With a few exceptions [49], [50], deep learning techniques are predominantly employed in profiled settings [10], [51]–[55]. Generally, a well-trained deep-learning model can make the attack several orders magnitude more efficient than conventional signal processing methods [56]–[59]. At present, various neural networks, including Multi-Layer Perceptrons (MLPs), Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), Transformers, and even Large Language Models (LLMs), are increasingly utilized by adversaries to analyze the traces for recovering the secret data in SCAs [60]–[63].

For example, [64] first utilized CNNs to overcome the effect caused by the jitter based countermeasures. Next, [65] adopted reinforcement learning for hyperparameter tuning in DLSCAs. Afterwards, neural networks are employed to augment template attacks, resulting in a model with fewer hyperparameters to tune, thereby simplifying its usability [66]. Deep neural networks have even been successfully employed to compromise the FPGA implementations of masked Kyber-512 as demonstrated in [67], in 2023. Besides, Zaid et al. [68] proposed a Conditional Variational AutoEncoder in TCHES, which bridges DL models and SCA paradigms based on theoretical findings from stochastic attacks. [69] used a Broad Learning System (BLS) [70], to make the attack more efficient as the model replaces the computationally expensive backpropagation used in deep learning with a fast, single-step calculation of output weights via pseudo-inverse, drastically reducing training time while maintaining high accuracy. Besides, in [71], a novel labeling method called Multi-point

Cluster-based (MC) approach is proposed, accounting for dependencies between leakage variables by exploiting multiple sample points for each one, in which lead to a successful attack on cryptoragphic implementations without the knowledge of plaintext or ciphertext.

III. THEORETICAL FOUNDATIONS OF SCREAMING CHANNELS

Prior to the discovery of screaming channels, covert data recovery via a radio transmitter was implemented by using the amplitude-modulating analog/RF hardware Trojans in IEEE 802.11a/g WiFi transceivers [72]. These stealthy hardware modifications subtly manipulate the transmitted signal's amplitude to create a covert channel for leaking sensitive information, all while remaining compliant with wireless standards and evading conventional post-fabrication tests. Potentially inspired by the attacks based on amplitude-modulating analog/RF hardware Trojans [72], [73], FEM-SCAs share the same threat model of unauthorized radio transmission but constitute a fundamentally different attack vector. Screaming channels constitute a side-channel attack that manipulates a device's intentional transmitter by exploiting unintentional EM emissions from its digital components, requiring no hardware modifications.

Unlike conventional side-channel attacks (e.g., power analysis), FEM-SCAs eliminate the proximity constraint, enabling adversaries to compromise cryptographic implementations remotely. This distinction becomes particularly critical when the victim device embedded mixed-signal circuits integrated systems which integrate noise-sensitive analog part (e.g., Bluetooth modules) with digital part (e.g., CPU core) on a single die. These circuits dominate modern electronics (e.g., smartphone, smartwatch, laptop) due to their cost efficiency and compact form factor, meeting market demands for affordable, portable devices.

However, the co-integration of digital and analog circuits within the same silicon die presents a challenge in managing noise generated during digital instruction executions. The RF block within the analog part demonstrates considerable sensitivity to this noise [74]. In such chips, digital circuits like microcontrollers or cryptographic accelerators perform data processing tasks by rapidly switching transistors, which generates sharp variations in voltage and current. These fluctuations are correlated with the data being processed and are especially intense at the frequency of the system clock and its harmonics. Ideally, this noise would remain confined to the digital domain. However, due to the tight physical proximity of analog components, particularly radio transceivers, the noise can propagate through the silicon substrate via resistive or capacitive coupling [75]. This leakage path enables a phenomenon called spectrum spraying. The CPU core within the digital circuit of the mixed-signal chip generates square wave noise due to the frequent switching of the clock signal. Its harmonic components are spread widely across the frequency spectrum. When these harmonics interact with data-dependent signals (side-channel leakage) inside the chip, they effectively modulate the harmonics with sensitive internal states. These

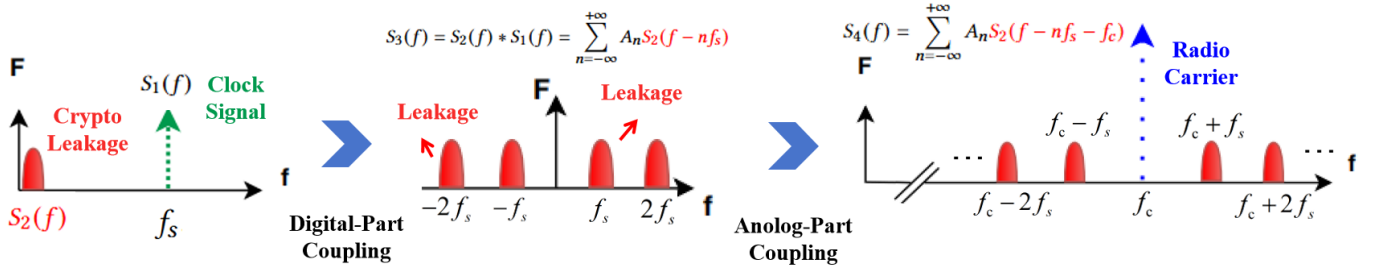


Fig. 3: Frequency-domain illustration of how side-channel leakage from the digital cryptographic module couples onto the analog radio carrier.

modulated signals can then couple into the analog part. The RF block and Voltage-Controlled Oscillator (VCO) then further modulate the received signal to a radio frequency as defined by the wireless transmission protocol, transmitting it using the on-chip antenna. This unintended transmission of leakage along the wireless channel could be detected by adversaries at a long distance and be used to derive the secret information. This is called FEM-SCA, or screaming channel attack.

What makes FEM-SCA especially threatening is that the side-channel leakage does not remain confined to near-field EM emissions [76], as is typical in traditional side-channel attacks. Instead, the mixed signal path acts as an amplifier and transmitter. The analog radio components broadcast the leaked modulated signals as part of the regular RF output. This mechanism allows the attacker to extract cryptographic secrets like AES keys from the far field EM emissions of a device at a distance, using only passive listening equipment such as a radio.

In a typical screaming channel scenario, it is assumed that the adversary can passively capture the signal at a specific radio spectrum and knows or can infer parameters such as the CPU clock frequency of the target device. Since the leakage appears at predictable offset of the radio carrier frequency, it is possible to tune the receiver to a harmonic where the side-channel signal is strong.

At the heart of the attack is the unintentional mixing of digital noise with radio output, a side-effect of modern chip miniaturization and integration trends. Because such leakage is a natural byproduct of placing digital and analog components on the same die, the screaming channel represents not a vendor-specific flaw, but a design-level vulnerability with broad implications for RF-enabled device security.

Next, we mathematically describe how the far field EM side channel is generated and captured remotely. Notice that we highlight the time-domain and frequency-domain side-channel leakage of the crypto part in red in the following analysis for easy tracking.

A. Generation

Fig. 3 illustrates how side-channel leakage from the cryptographic module is coupled onto the radio carrier in the frequency domain. First, we use formula 1 to present the clock signal $s_1(t)$ from the computational core, in which the clock frequency of the square wave is denoted as f_s .

$$s_1(t) = \sum_{n=-\infty}^{+\infty} A_n e^{i2n\pi f_s t}, \quad (1)$$

Formula 2 denotes the corresponding Fourier transform $S_1(f)$ of $s_1(t)$, in which A_n is used to present the Fourier series coefficients and δ is used to present the impulse function. Notice that the even terms of the Fourier series are not exactly equal to zero since the square wave noise is not an ideal square wave [20].

$$S_1(f) = \sum_{n=-\infty}^{+\infty} A_n \delta(f - nf_s) \quad (2)$$

Formula 3 defines A_n , in which τ is the duty cycle of the square wave.

$$A_n = \frac{\sin n\pi\tau}{n\tau} \quad (3)$$

Suppose the secret-dependent side-channel leakage generated from the Crypto block during the execution is denoted by $s_2(t)$. In the digital part, $s_2(t)$ is first modulated by the square wave of the clock signal $s_1(t)$. The resulting signal is denoted by s_3 , as shown in Formula 4. Note the leakage-related component is marked in red for easy catching during the following derivative process.

$$s_3(t) = s_1(t) \cdot s_2(t) \quad (4)$$

Formula 5 shows the resulting signal s_3 in frequency domain, in which $S_2(f)$ is the the corresponding Fourier transform of the crypto side-channel leakage $s_2(t)$.

$$S_3(f) = S_2(f) * S_1(f) = \sum_{n=-\infty}^{+\infty} A_n S_2(f - nf_s) \quad (5)$$

Afterwards, in the analog part, the RF block modulates the received signal $s_3(t)$ to a high frequency. Formula 6 presents the modulated signal in the time domain and formula 6 is for the frequency domain. We use $e^{i2\pi f_c t}$ to denote the radio carrier, in which f_c is the carrier frequency. After the modulation, the signal is first amplified and then transmitted through the antenna on chip.

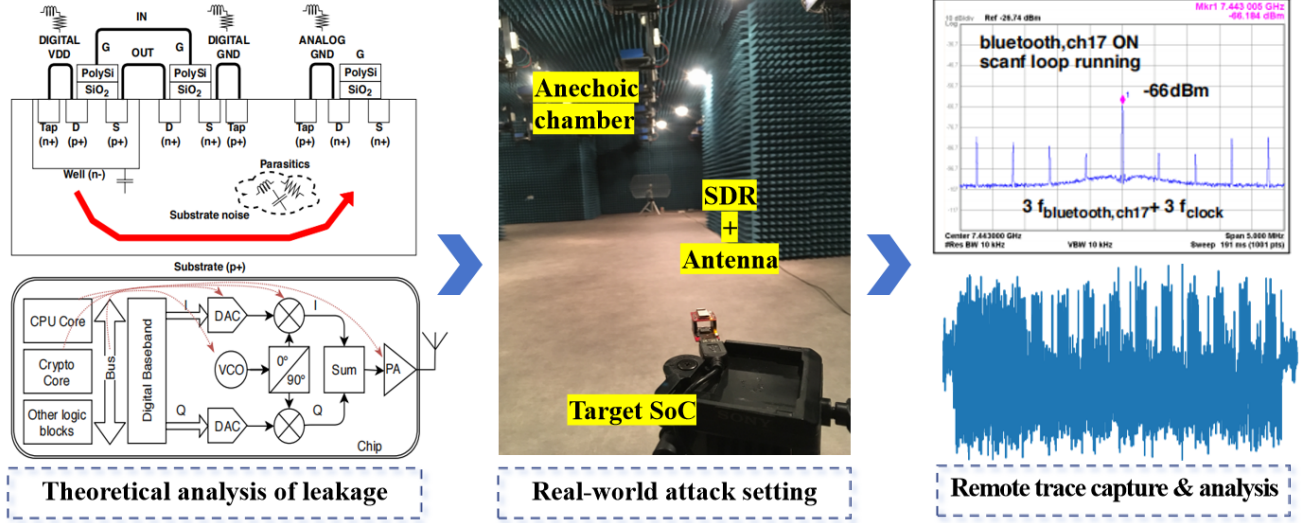


Fig. 4: Illustration of the first practical screaming channel attack work [23].

TABLE I: Detailed **full key** recovery results of the FEM-SCA conducted in [23].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Template attack	1 m	52,589	500	2^0	$70K \times 500$	Office
TinyAES	Template attack	3 m	718	500	2^0	$70K \times 500$	Anechoic chamber
TinyAES	Template attack	10 m	1,428	500	2^0	$130K \times 500$	Anechoic chamber

$$\begin{aligned}
 s_4(t) &= \sum_{n=-\infty}^{+\infty} A_n s_2(t) e^{i2\pi(nf_s + f_c)t} \\
 S_4(f) &= \sum_{n=-\infty}^{+\infty} A_n S_2(f - nf_s - f_c).
 \end{aligned} \tag{6}$$

B. Capture

At the receiver side, formula 7 shows the captured signal after the demodulation process in time and frequency domain ($r(t)$ and $R(f)$), with the center receiving frequency set to $f_c + Nf_s$. In formula 7, we define the front-end gain as G .

$$\begin{aligned}
 r(t) &= G \left(\sum_{n \neq N} A_n s_2(t) e^{i2\pi(n-N)f_s t} + A_N s_2(t) \right) \\
 R(f) &= G \left(\sum_{n \neq N} A_n S_2(f - (n-N)f_s) + A_N S_2(f) \right)
 \end{aligned} \tag{7}$$

From formula 7, we can find that the received signal $r(t)$ consists of 1) a scaled version of the side-channel leakage $s_2(t)$ at baseband, and 2) multiple modulated copies of $s_2(t)$ at frequencies $(n-N)f_s$, for all $n \neq N$. By using a low pass filter with a threshold related to the baseband, we can extract the side-channel leakage $s_2(t)$ from the received signal $r(t)$.

Next, we systematically review the existing screaming-channel attack cases. For each case, we include a technical visualization that outlines the trace acquisition setup, model profiling parameters, and recorded attack performance to facilitate clear understanding and comparison.

IV. DISCOVERY & UNDERSTANDING

In 2018, Camurati et al. [23] conducted the first FEM-SCA case at the CCS'18 conference, as the core discovery phase of the screaming channel. It was revealed that cryptographic computations executed on mixed-signal SoCs can unintentionally leak information through the RF transmission path when digital switching activity couples into the radio front-end. This discovery fundamentally challenged the conventional assumption that EM side-channel attacks require near-field access [77], demonstrating instead that sensitive information can be extracted from legitimate wireless emissions at distances. Importantly, this leakage does not originate from a dedicated side-channel radiation source, but rather from unintended modulation of an already existing communication carrier, thereby enabling a new class of side channel. In [23], they experimentally showed that, by using a Software-Defined Radio (SDR) [78], it is feasible to capture EM leakage of TinyAES implementations [79] over distances of up to 10 m. The leakage is strong enough to enable correlation analysis and template attacks to recover AES keys. In [23], they conducted template attacks in two different capturing environments, which are a normal office with a 1 m distance, and an anechoic chamber allowing measurements at distances of up to 10 m. Table. I presents the full key recovery results of the template attack conducted in [23].

Fig. 4 illustrates how they setup the remote attack in an anechoic chamber and an example 10-round AES trace captured remotely. Notice that the traces are normalized into $[0, 1]$ by using the min-max normalization method. We employ the metric Measurements to Disclosure (MTD), defined as the number of traces an attack requires to recover the secret key

TABLE II: Detailed **full key** recovery results of the FEM-SCA conducted in [24].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Profiled CPA	10 m	1,500	1,000	2^{28}	6K×500	Office
TinyAES	Profiled CPA	15 m	5,000	1,000	2^{23}	10K×500	Office

TABLE III: Detailed **full AES key** recovery results of the FEM-SCA on BLE session key derivation conducted in [80].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
BLE	Profiled CPA	1.2 m	10K	300	2^{33}	16K×300	Office
BLE	Profiled CPA	1.2 m	16K	1	2^{27}	16K×300	Office

(i.e., $PGE = 0$). The table shows a clear trade-off between distance and the number of traces required for a full key recovery, but the key takeaway is that the attack is successful even at a significant range. In a standard office environment at a distance of 1 m, the template attack requires around 52K traces, indicating that while effective, the signal-to-noise ratio at this range with common background interference is lower. However, the results become strikingly more efficient in the controlled laboratory environment. At 3 m, the number of required attack traces for the full AES key recovery decreases to just 718. This efficiency degrades slightly but remains highly feasible at an impressive 10 m range, requiring around 1.4K traces. The need for a larger template set (130K) at 10 m indicates the increasing challenge of distinguishing the signal. Although the screaming-channel attack is brought to the forefront of side-channel research by [23], many aspects of this novel threat remain insufficiently understood. Open questions include a deeper characterization of the underlying leakage sources, the development of attack strategies that fully exploit this unconventional channel, and comprehensive security evaluations under realistic deployment scenarios. Addressing these gaps is essential for advancing both the theoretical foundations and the practical countermeasures in this emerging research area.

Building upon the initial observation described above, the following-up TCHES'20 work [24] thoroughly characterized this novel attack vector, analyzing how leakage coexists with intended radio transmissions, how distance and frequency affect leakage strength and distortion, and whether profiling models can be reused across devices and environments. They tested the same attack method (template attack) as in [23] for both controlled chambers and realistic office environments, added support for conventional EM side-channel capture for comparison, and enabled experiments on a real authentication protocol (Google Eddystone). Multiple instances of the Nordic nRF52832 chip and different SDRs (HackRF, Ettus N210 USRP, B210 USRP) with antennas and amplifiers are employed, ensuring flexibility and realism in evaluating screaming-channel leaks. More specifically, they first examine how screaming-channel leakage compare quality to conventional EM side-channel leakage. Overall, the results indicate that screaming-channel leaks are weaker and less structured than conventional ones, though still viable for attacks under realistic conditions.

Afterwards, they investigated whether the capturing frequency at different screaming-channel leakage point affects

their characteristics and showed that the choice of harmonic channel frequency does not significantly alter the strength or shape of the leak. In addition, [24] analyzed how increasing distance influences the quality of screaming-channel leakage. As expected, the far field EM side-channel signal strength decreases quadratically with distance, requiring stronger amplification and better capturing equipment (SDR, antenna), making it hard to separate distance effects from setup quality. Experimentally, [24] showed that the correlation profile created with a cabled setup can be reused months later to successfully recover TinyAES keys from another device at 15 m in an office environment (with $5K \times 1K$ traces and key enumeration up to 2^{23}), and that leakage remains detectable even at 60 m. A subsequent KTH thesis work [81] further complemented this understanding by systematically comparing attacks under both power and far-field EM settings. In particular, the thesis experimentally demonstrated that leakage patterns learned from side-channel traces are highly sensitive to device diversity, measurement distance, and acquisition conditions, especially in far-field EM scenarios where RF emissions are indirectly modulated by digital switching activity through mixed-signal coupling.

Building on the foundation above, the CARDIS'24 work [82] further refined the spectrum-level understanding of screaming channel leakage by investigating how side-channel information is distributed beyond harmonic RF spectrums. Unlike earlier studies [23], [24], [81] that primarily focused on leakage appearing around CPU clock harmonics, this work demonstrated that exploitable information can also emerge in non-harmonic frequency regions, where leakage is not directly aligned with clock-driven spectral components. This observation significantly extends the frequency-domain interpretation of screaming channels, showing that leakage is not strictly periodic or harmonically constrained, but can be reshaped by nonlinear mixing effects within the RF front-end and signal processing pipeline. From a signal analysis perspective, [82] revealed that the interaction between digital switching activity and wireless modulation introduces subtle spectral distortions that may shift or disperse leakage energy away from expected harmonic locations. This implies that traditional frequency-targeted analysis strategies may fail to fully capture the leakage footprint, especially when the RF transmission chain introduces additional frequency transformation effects. Overall, the work strengthens the understanding that screaming channel leakage should be viewed as a broadband, modulation-dependent spectral phenomenon, rather than a purely clock-

Evolution of Understanding in Screaming Channel

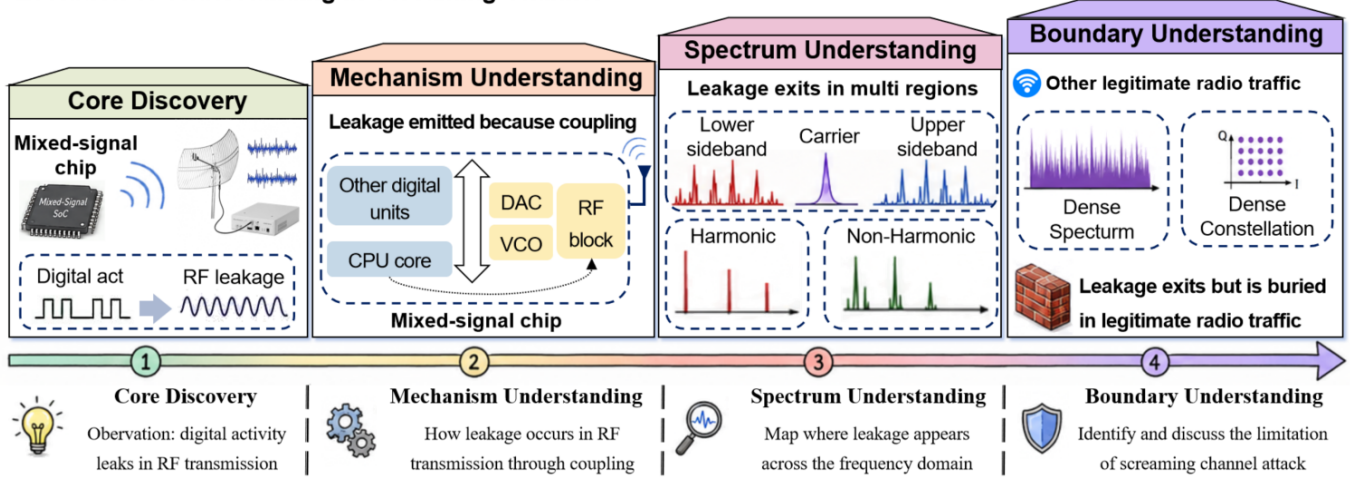


Fig. 5: An overview of the progressive understanding in screaming channel attacks: from discovery to boundaries.

synchronized harmonic artifact, thereby providing deeper insight screaming channels.

In 2024, the following work refined the understanding of screaming channel in more realistic wireless settings. Blue-Scream [80], demonstrated that screaming channel leakage is not limited to synthetic or custom firmware scenarios, but can also be triggered and exploited in real-world Bluetooth Low Energy (BLE) stacks through careful protocol-level manipulation of transmission timing and cryptographic execution windows. This confirmed that the leakage mechanism persists in practical IoT edges and can be systematically activated under standard communication conditions. Before the long-range attack on BLE stack in [80], Cao et al. [83] analyzed the Session Key (SK) derivation mechanism (re-keying process) of the BLE protocol based on the near-field EM SCA. In [80], they went one step further to conduct the attack on the same Bluetooth target remotely by using FEM-SCA. They showed that that by manipulating low-level BLE protocol parameters, the adversaries are feasible to force a victim device to perform the critical SK derivation concurrently with a radio transmission. This creates a far-field side channel, allowing the attacker to recover the Long Term Key (LTK) from up to 1 m away using a profiled correlation attack, with full key recovery demonstrated in a low-noise, office environment. Notice that the attack conducted in [80] exploits the moment the LTK is used as an AES key to generate a session key. By recovering the master LTK, the attacker compromises the entire trusted pairing, gaining the ability to decrypt all past and future communications for that device pair. Table III summarizes the full key recovery results of the FEM-SCA on BLE session key derivation conducted in [80].

A more recent work provides another fundamental perspective on the applicability limits of screaming-channel attacks by shifting the discussion from individual attack demonstrations to RFSoc-level security evaluation [37]. In this review, Du et al. emphasized that screaming-channel leakage is rooted in the high integration of mixed-signal chips. From this view, the applicability of FEM-SCA is not determined

only by whether a device uses Bluetooth or whether AES is implemented in software, but by whether the internal chip architecture provides a strong enough coupling path between sensitive computation and the RF module. The work also highlights several practical limits that remain insufficiently understood, including the difficulty of identifying dominant leakage sources inside RFSocS and the lack of evaluation indicators for screaming-channel resistance in existing cryptographic security standards.

Taken together, these works collectively establish a progression in the discovery and understanding of screaming channel attacks, from their initial usage to their practical limitations. Figure 5 summarizes this evolution in a four-stage framework. The core discovery stage shows that digital activity in mixed-signal devices can leak through RF emissions, enabling remote side-channel analysis. The mechanism understanding stage explains how leakage occurs in RF transmission through coupling and how different external conditions can affect the leakage. The framework then moves to spectrum understanding, where leakage is characterized in the frequency domain, appearing across carrier, sidebands, harmonic, and non-harmonic components. Finally, boundary understanding highlights that in modern radio communication-heavy systems, leakage becomes increasingly masked by dense legitimate signals, revealing the practical limits of screaming channel attacks.

Next, we move on to reviewing techniques that focus on enhancing the attack capability and practical threat level of screaming channel attacks.

V. ENHANCED ATTACK CAPABILITY & PRACTICALITY

The evolution of screaming channel attacks has not only expanded the theoretical understanding of mixed-signal chips' leakage in RF transmission, but has also significantly enhanced the practical attack capability in realistic cases. Therefore, this section focuses on the FEM-SCA enhancement techniques that aim to improve attack efficiency, robustness, and generalization under realistic conditions. Since most existing

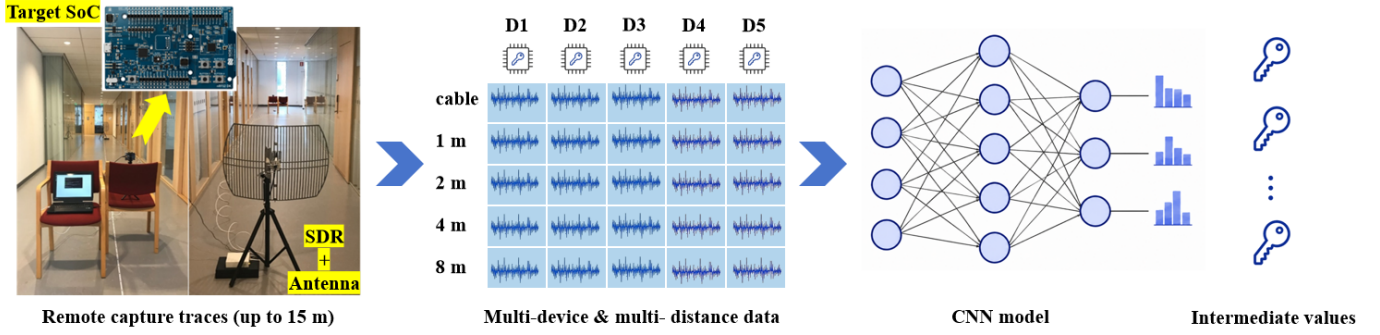


Fig. 6: Illustration of the multi-distance-device profiled FEM-SCA framework proposed in [38]. The CNN model is trained on traces captured from five devices at five different distances to generalize better.

TABLE IV: Detailed **partial key** recovery results of the FEM-SCA conducted in [38].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Remote-trace trained CNN	3 m	437	1k	2^0	$500K \times 100$	Office
TinyAES	Remote-trace trained CNN	6 m	1,089	1k	2^0	$500K \times 100$	Office
TinyAES	Remote-trace trained CNN	9 m	2475	1k	2^0	$500K \times 100$	Office
TinyAES	Remote-trace trained CNN	15 m	367	1k	2^0	$500K \times 100$	Corridor

works evaluate these enhancement strategies using a consistent target to enable fair comparison, they mainly focus on the TinyAES implementation as the attack target. The results and extensions targeting other cryptographic implementations, such as masked AES, post-quantum cryptographic schemes, and hardware AES accelerators, are discussed separately in the next section.

In 2020, the deep-learning techniques were first introduced into the context of screaming channel attacks [38], marking the beginning of a new paradigm in FEM-SCA. This work systematically explored to which extend the CNN model can make the far field EM side-channel attack more efficient, and proposed a multi-distance, multi-device generalization strategy for DL-based FEM-SCA. For better comparison, they setup the experiment as the same as in [23], in which the target device is a Nordic Semiconductor nRF52832 SoC supporting Bluetooth 5 [84] with the data transmission rate 2Mbps. For the attack, an Ettus Research USRP N210 is used as the receiver, with a Grid Parabolic Antenna TL-ANT2424B attached. Its center receiving frequency is set to 2.528 GHz, which is equal to $2f_{clock} + f_{Bluetooth}$, where $f_{Bluetooth} = 2.4$ GHz. They capture EM traces in an office corridor environment, with the distance up to 15 m.

Fig. 6 shows an overview of how the multi-distance-device profiled FEM-SCA proposed by [38] works. To train the deep-learning model, they collect 500K traces from five nRF52 devices under five different settings: captured by cable, at 1 m, 2 m, 4 m, and 8 m (with each setting contributing the training set equally). Each trace corresponds to 100 repeated encryptions, performed to mitigate noise and enhance the reliability of feature extraction. Each scenario contributes an equal proportion of traces to the training set, enabling the model to learn leakage representations across different devices and propagation conditions. By incorporating both device diversity and distance variations during training, this strategy

aims to mitigate the impact caused by the board diversity [48] and to generalize better across different attack distances.

Afterwards, they conduct the attack by using the trained model on another four nRF52 implementation of AES at different attack distances: 3 m, 6 m, 9 m, and 15 m. Table IV shows the attack results obtained from the CNN-based attack method, indicating that the deep-learning based attack framework can be more effective than conventional signal processing way [23], [24]. The most striking conclusion is the deep-learning based attack's consistent success in recovering the partial key, while each shows a key enumeration complexity of 2^0 , meaning no subkey candidate ranking or guessing is needed. Furthermore, the attack remains effective at considerable distances, up to 15 m. The number of traces required generally increases with distance due to signal attenuation, for example, rising from 437 traces at 3 m to 2,475 at 9 m in an office environment. However, the result at 15 m in a corridor environment (only 367 traces with each of 1K repetitions) indicates that environmental factors play a critical role. A corridor likely offers clearer line-of-sight and fewer signal obstructions, resulting in higher signal quality than in an office space. Notice that in the case of [38], each attack trace is the average of 1K measurements with the same encryption to degenerate the noise level.

However, an operational constraint for the attack in [38] is the need for the target device to perform encryption repeatedly, in this case 1K times per trace, which may limit attacks to scenarios where the device can be triggered to operate frequently. In a real attack scenario, it is highly impractical for adversaries to capture multiple traces per encryption from target implementations without physical access to the victim device. Furthermore, it is often infeasible for a remote attacker to obtain the plaintext of the cryptographic implementation as known information to facilitate key extraction, which means that the first-round *SBox* operation in AES is unsuitable as

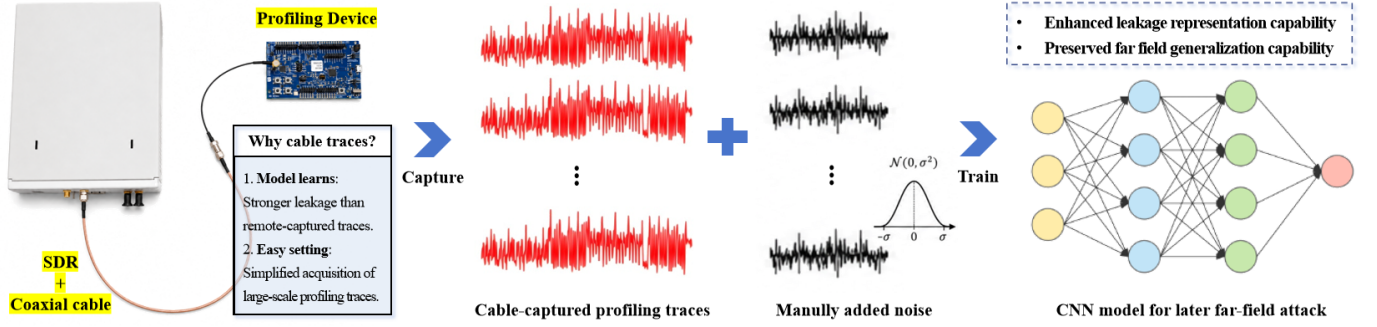


Fig. 7: Illustration of how the model is trained in the noise-aware domain augmentation FEM-SCA framework proposed in [85]. The CNN model is trained using high-quality “clean” traces acquired through a coaxial cable connection with manually added Gaussian noise to simulate realistic signal distortions.

TABLE V: Detailed **partial roundkey** recovery results of the FEM-SCA conducted in [85].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Cable-trace trained CNN	15 m	341	1	2^0	200K × 100	Corridor

an attack point under these constraints. These unresolved challenges persist in presented FEM-SCA research before 2021 [23], [24], [38].

To achieve a better attack performance so that attackers can eliminate the trace repetition requirement, [85] proposes a noise-aware augmentation profiling strategy (as shown in Figure 7). Unlike previous approaches that directly construct profiling models from far-field traces, in which the key-dependent features are too weak to be extracted, this method trains the deep-learning classifier using high-quality “clean” traces acquired through a coaxial cable connection. To bridge the distribution gap between the profiling domain and the noisy far-field attack domain, manually added Gaussian noise is introduced during the training process to simulate realistic signal distortions. Through this noise-aware training mechanism, the model learns leakage representations better than directly on remote-captured traces. Consequently, the trained model can achieve a 20-fold improvement in attack efficiency, as shown in Table V, compared to the multi-distance-device strategy [38]. By adopting this strategy, the CNN model trained in [85] achieves an impressive attack result, recovering a last-round AES sub-roundkey with only 341 traces captured at 15 m in a corridor environment, without any encryption repetition. Notice that using the last-round SBox output as the attack point eliminates the need for known plaintext, thereby removing a major practical obstacle for real-world adversaries.

Going one step further, the master thesis [86] investigated whether more realistic noise augmentation strategies can further improve the generalization capability of deep-learning-based FEM-SCA. Inspired by the noise-aware domain augmentation strategy in [85], which bridges the gap between profiling traces and noisy far-field measurements through manually injected Gaussian noise, this work explores the use of environment-dependent noise to better approximate practical attack scenarios. Specifically, instead of relying solely on Gaussian noise, they capture realistic noisy traces generated from actual measurement environments, together with other

data augmentation and preprocessing techniques, to evaluate their impact on model robustness and attack efficiency. The thesis provides a deeper analysis of the relationship between training-domain characteristics and attack performance, revealing that realistic noise augmentation does not always guarantee improved generalization over Gaussian noise, while factors such as signal amplitude, trace alignment, and propagation conditions can play more critical roles in determining FEM-SCA effectiveness.

Following the discussion of deep-learning-based enhancement, Zhang et al. [87] represents another direction for improving the practicality of screaming channel attacks, by introducing additional hardware assistance rather than improving the attack algorithm itself. Since FEM-SCAs are highly sensitive to environmental noise and signal attenuation, the authors introduced a repeater-assisted FEM-SCA framework, where an intermediate RF repeater is deployed between the target device and the receiver to amplify the leaked signal and improve its SNR. By introducing this intermediate signal enhancement stage, the attack pipeline is no longer constrained by the original propagation loss between the victim device and the attacker’s receiver. Their results demonstrate that the proposed method dramatically increases the SNR of the remote-captured traces, which directly translates to a reduction in the number of traces required for a successful CPA. Table VI shows the CPA attack results by using a wireless repeater placed between the victim implementation of AES and the attacker [87].

While a wireless repeater makes the CPA attack more reliable, it causes the attacker’s operation significantly less covert by introducing a detectable active radio element. The repeater’s effectiveness is greatest when placed close to the victim device (as shown in [87], where gain is maximized near the transmitter). Consequently, the attacker must physically approach the target area to deploy the repeater, which increases the risk of exposure and limits the practicality of FEM-SCAs. This trade-off highlights an inherent limitation of repeater-

TABLE VI: Detailed **full key** recovery results of the FEM-SCA conducted in [87].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	CPA	0.2 m	2,450	1	2^0	/	Office
TinyAES	CPA	0.7 m	6,450	1	2^0	/	Office

TABLE VII: Detailed **full key** recovery results of the FEM-SCA conducted in [88].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	CPA	0.5 m	3,600	1	2^0	/	Office

TABLE VIII: Detailed **partial key** recovery results of the FEM-SCA conducted in [89].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Profiled CPA	7 m	65	50	2^{23}	$15K \times 10$	Office

TABLE IX: Detailed **partial roundkey** recovery results of the FEM-SCA conducted in [90].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Switch-T (Transformer-based model)	15 m	2,976	1	2^0	$40K \times 100$	Corridor

based approaches: although they enhance signal acquisition capability, they sacrifice the remote and covert nature that makes screaming channel attacks particularly threatening.

In 2023, their subsequent work [88] proposed a spectral addition technique to mitigate the effect caused by the challenge of environmental noise, which degrades signal quality and makes far-field attacks to fail. The core contribution of their subsequent FEM-SCA work [88] is a systematic framework that synchronously captures screaming channel signals from two different frequency bands (specifically 2.464 GHz and 2.528 GHz leaked from the same nRF52832 Bluetooth chip), aligns them in phase, and coherently sums them to suppress uncorrelated Gaussian noise and enhance the SNR. In addition, they developed a signal propagation model to theoretically predict the SNR gain from this method and validate it experimentally in a high-noise office environment. The results demonstrate that their technique reduces the number of traces required for a successful CPA, compared to their wireless repeater based attack method in [87]. Table VII shows the CPA attack results based on the spectral addition technique proposed in [88].

It is worth noting that the receiver employed in [87], [88] utilize antennas with only 6 dBi gain, whereas many previous screaming channel studies [23], [24], [38], [85] adopt higher-gain directional antennas (e.g., 24 dBi) to improve leakage reception. We hypothesize that this limitation in receiver gain partially contributes to the relatively lower attack efficiency and shorter effective attack distance reported in these works, as the reduced antenna gain directly constrains the received leakage SNR.

In 2023, [89] experimentally demonstrated that the coupling of side-channel leakage with the RF signal is a complex process, influenced by propagation effects through the substrate, power, and ground planes. As a result, information-bearing leakage is not only present at harmonic frequencies but is also observable at non-harmonic frequencies across the spectrum. To understand the difference between harmonic and

non-harmonic frequencies, here we take a mixed-signal chip with a clock frequency of 64 MHz as an example. First, consider an ideal digital clock signal, which is a perfect square wave oscillating between 0 and 1 at a frequency of 64 MHz. This corresponds to a period of $T = \frac{1}{64 \times 10^6}$ seconds, meaning the signal completes one full cycle ($0 \rightarrow 1 \rightarrow 0$) every approximately 15.625 nanoseconds. According to Fourier analysis, such a square wave decomposes into an infinite series of sinusoidal components located at integer multiples of the fundamental frequency. These components are referred to as harmonics. In actual digital integrated circuits, however, EM leakage caused by transistor switching does not conform to this ideal model. The signal propagates through complex structures such as silicon substrates, power lines, and ground planes. This physical environment acts as a filter that distorts the original signal, attenuating certain harmonic components and generating new frequency elements through nonlinear effects. As a result, the emitted spectrum contains not only harmonic components but also non-harmonic frequencies that remain correlated with the device's internal operations. According to this theory, their experiments show that non-harmonic frequencies can be effective for recovering the AES key from the Bluetooth device implementations, especially in noisy environments where harmonics are polluted by interference. By following the same hardware setup as in prior works on screaming-channel attacks [23], [24], [38], [85], [89] comprehensively compared the effectiveness of attacks at harmonic vs. non-harmonic frequencies under two configurations, which are wired and wireless. In the wired setting, they tested 150 frequencies from 2.45 GHz to 2.6 GHz in 1 MHz steps, aiming to validate the effectiveness of non-harmonic frequencies as a basis for subsequent remote attacks. Afterwards, based on the most promising non-harmonic frequencies identified, they conduct profiled correlation attack [91] with the wireless setting at distances of up to 7 m. The results demonstrate that 5 out of the selected non-harmonic frequencies remain highly effective ($PGE \leq 2^{32}$). Notably, the best-performing

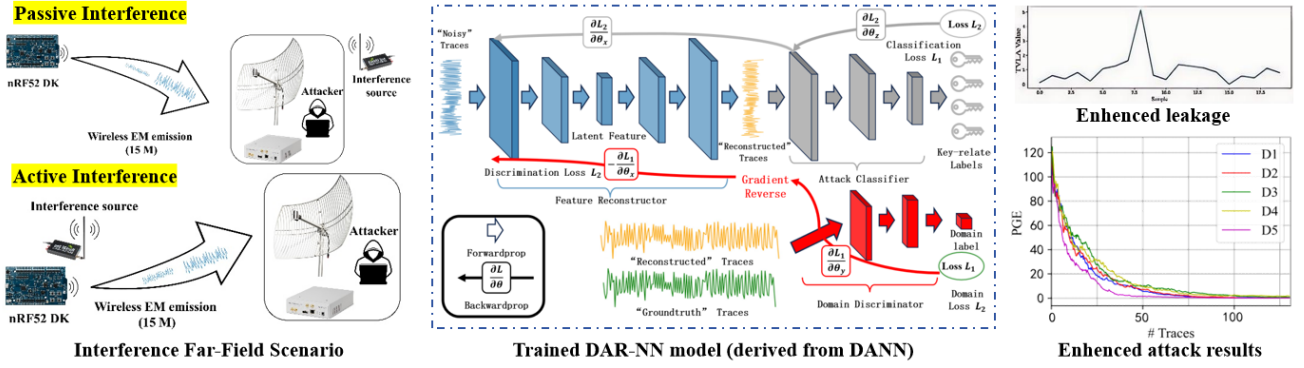


Fig. 8: Illustration of the DANN-based FEM-SCA proposed in [92].

TABLE X: Detailed **partial roundkey** recovery results of the FEM-SCA in [92].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	DAR-NN (DANN-based model)	15 m	141	1	2^0	$40K \times 100$	Corridor
TinyAES	DAR-NN (DANN-based model)	15 m	852	1	2^0	$40K \times 100$	Corridor with 2.5% manual interference
TinyAES	DAR-NN (DANN-based model)	15 m	771	1	2^0	$40K \times 100$	Corridor with 25% manual interference

non-harmonic frequency at 2.484 GHz requires only 65×50 to achieve $PGE \leq 2^{32}$ for recovering a subkey at 7 m. For detailed experimental results of [89], check Table. VIII. This significantly expands the attack surface, allowing attackers to bypass polluted harmonic bands and succeed.

In 2025, several advanced deep-learning techniques become a powerful ally to screaming channel attacks. [90] proposes a Transformer [93] based neural network, called Switch-T model, to learn sensitive features from different side channels. By employing the Elastic Weight Consolidation (EWC) mechanism [94], the proposed Switch-T model can continuously profile on other targets based on a different side channel (such as power consumption), while maintaining the capacity to use far field EM emission to compromise the nRF52 Bluetooth implementation of AES remotely. In their cross-channel experiment conducting on the publicly available FEM-SCA collection [85], they show that the Switch-T model requires only 1 epoch to adjust back to the nRF device attack task after profiling on new devices (STM32F3 MCU, ATXmega128D4), achieving an attack accuracy close to its initial performance on nRF52. While the experiment in [90] does not measure the PGE result of the proposed Switch-T model for recovering a subkey at 15 m distance to the victim device, their follow-up work [92] tests the model as a baseline, which can be used as a reference for us to systematically evaluate the Switch-T model's performance in the FEM-SCA scenario. Table IX summarizes the partial AES key attack results of [90].

Following the early demonstrations of screaming-channel attacks in relatively controlled environments, Wang et al. investigated how FEM-SCAs behave under more realistic long-range conditions where remotely captured traces suffer from substantial noise and interference [92]. To enhance the effectiveness of FEM-SCAs in complex and noisy environments, they proposed a Domain-Adversarial ReFeature Neural Network (DAR-NN) to reconstruct key-dependent features from "noisy" traces by learning a mapping to "clean" ref-

erence traces which advances prior noise-aware augmentation strategies from manually simulated distribution toward adaptive feature-level domain alignment. The DAR-NN model is derived from the Domain-Adversarial Neural Network (DANN) [95], which is originally designed for models to generalize better in unseen domains through the adversarial task between the feature reconstructor and the domain discriminator. The core innovation of DAR-NN is the integration of a Denoising Autoencoder (DAE) with two classification models deployed as regularization terms. This joint optimization is important because a conventional DAE trained only to minimize reconstruction error may suppress the weak leakage features together with environmental noise, which is particularly problematic for far-field traces.

Fig. 8 illustrates how the DANN-based FEM-SCA proposed in [92] works in FEM-SCA. This adversarial framework is designed to reconstruct key-dependent features when interference existing in the FEM-SCA context. By using the identical experimental equipments as in [38], [85], they define three attack tasks to evaluate their model: (1) a baseline with no manual interference, (2) a passive interference scenario where an interfering HackRF radio source is placed behind the receiver, (3) an active interference scenario where an interfering HackRF radio transmits from the same position as the victim device. Notice that instead of focusing on the commonly used 2.528 GHz to capture far field EM traces, they turn the center receiving frequency to 2.272 GHz (the Bluetooth radio frequency (2.4 GHz) offset by two times the CPU's clock frequency (64 MHz).) according to the experimental environments. Table X concludes the attack results of the proposed DAR-NN model, in which it achieves to use only 141 traces to recover a subkey at 15 m distance to the victim nRF Bluetooth implementation of AES, without repeating each encryption more than once.

Under the baseline condition without manually introduced interference, DAR-NN substantially improves the efficiency

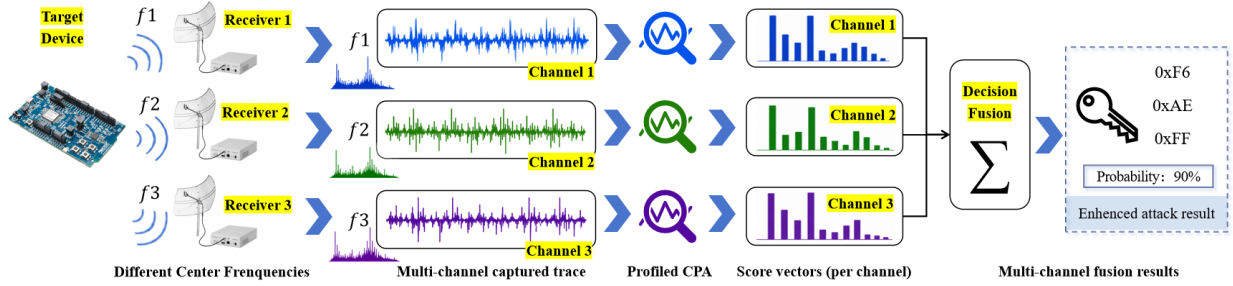


Fig. 9: Illustration of the multi-screaming-channel attack framework in [99], in decision-fusion operating mode.

TABLE XI: Detailed **partial key** recovery results of the FEM-SCA conducted in [99].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
TinyAES	Multi-channel profiled CPA	15 m	45	500	2^0	Not reported	Corridor
TinyAES	Multi-channel profiled CPA	30 m	1000	50	2^0	Not reported	Corridor

of long-range key recovery. Using the public 15 m collection in [85], the proposed model can recover an AES subkey with only 141 traces, which the authors report as a 58.7% improvement over the previous SOTA method. Next, they extended the evaluation beyond a relatively controlled corridor environment by introducingd RF interference at the same receiving frequency. The resulting experiments show that DAR-NN retains considerably stronger robustness than the baseline models [85], [90], [96]–[98] by a multiple-fold margin. Even in the presence of 25% active interference, the proposed method can still recover the target subkey at 15 m using approximately 2K traces, whereas the baseline models failed to recover the key with 5K traces under the same condition without resorting to key enumeration. Furthermore, the model proves its transferability by successfully attacking other MCU platforms (STM32, ATXmega) using power consumption traces, confirming its robustness and adaptability across different side channels and devices.

While the exploitation of leakage across different radio-frequency channels in FEM-SCAs has been preliminarily investigated [88], these efforts mainly regard multi-frequency leakage as redundant observations for signal enhancement. A systematic investigation of frequency diversity as multiple independent leakage channels, and how their complementary information can be effectively combined to improve attack performance, remains largely unexplored. In 2026, [99] introduces the concept of multi-screaming-channel attack framework in IEEE-TIFS, where leakage captured at different RF frequencies is treated as multiple side-channel sources rather than merely repeated observations of a single leakage signal. Building upon the observation that exploitable leakage is not only present at the traditional clock harmonics but also widely distributed across non-harmonic frequency regions [82], [99] investigates how frequency diversity can be leveraged to enhance FEM-SCA performance. Specifically, the work formulates different frequency components as independent leakage channels and systematically evaluates three multi-channel fusion strategies, including data fusion, feature fusion, and decision fusion, to combine their complementary information. Data fusion directly merges normalized traces from different

frequencies before performing the profiled correlation attack. Feature fusion jointly extracts frequency-dependent leakage features and applies dimensionality reduction methods such as Principle Component Analysis (PCA) [100] or Linear Discriminant Analysis (LDA) [101] before key recovery. Decision fusion independently performs attacks on each frequency channel and aggregates the resulting key probability scores. Among these approaches, decision fusion provides a practical solution because each frequency can be analyzed independently and the final key ranking can be improved by combining the obtained attack scores.

The practical effectiveness of multi-screaming-channel attacks [99] is validated in realistic long-range scenarios. At 15 m, the combination of two non-harmonic frequency channels reduces the trace requirement to reach a target GE from 125×500 and 146×500 traces for individual channels to only 45×500 traces with decision fusion. Extending beyond previous screaming-channel attacks, the authors further achieve the successful attack at 30 m in an RF-polluted environment, where frequency combination reduces the required traces by a factor of 2–2.77 compared with single-frequency attacks. These results demonstrate that exploiting frequency diversity can significantly enhance attack practicality by providing complementary leakage observations and mitigating frequency-dependent noise. Nevertheless, the improvement is primarily reflected in faster convergence and reduced trace complexity, while the final achievable attack performance remains constrained by the intrinsic leakage strength available across the selected frequencies.

Taken together, Table XII shows that the development of FEM-SCA on nRF52 TinyAES has moved from demonstrating feasibility toward improving attack efficiency and environmental robustness. Early screaming-channel attacks relied heavily on repeated encryptions and large profiling sets. From Table XII, we can find that the first template attack required averaged traces collected in a controlled laboratory setting, while subsequent profiled CPA and CNN-based attacks extended the distance to 15 m but still depended on substantial trace repetition or profiling effort. The 2021 cable-trained CNN attack marked an important step toward practicality by reducing the

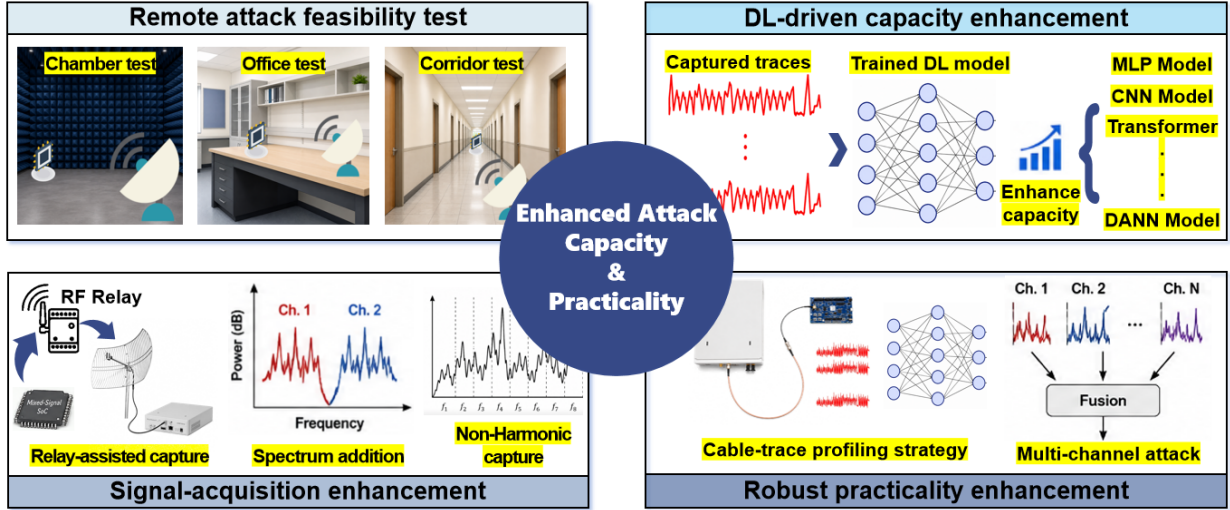


Fig. 10: An overview of the evolution of FEM-SCAs toward practical remote threats with enhanced attack capacity.

TABLE XII: Chronological summary of existing FEM-SCA works targeting on **TinyAES** implementations

Works	# Traces to extract the Key	# Attack distance	# Partial or full key	# Attack method	# Profiling data	# Key enumeration	Environment	Year
[23]	$1,400 \times 500$	10 m	Full Key	Template attack	$130K \times 500$	2^0	Lab	2018
[24]	$5,000 \times 1,000$	15 m	Full key	Profiled CPA	$10K \times 500$	2^{23}	Office	2020
[38]	$10,000 \times 1,000$	15 m	Partial key	Remote-trace trained CNN	$200K \times 100$	2^0	Corridor	2020
[85]	341×1	15 m	Partial roundkey	Cable-trace trained CNN	$200K \times 100$	2^0	Corridor	2021
[87]	$6,000 \times 1$	0.7 m	Full key	Relay-based capture with CPA	-	2^0	Office	2022
[88]	$3,600 \times 1$	0.5 m	Full key	Spectrum-addition capture with CPA	-	2^0	Office	2023
[89]	65×50	7 m	Partial key	Profiled CPA	$15K \times 10$	2^{23}	Office	2023
[102]	$25,000 \times 1$	5 m	Full key	Profiled CPA	$20K \times 1$	2^0	Office	2024
[90]	$2,976 \times 1$	15 m	Partial roundkey	Switch-T (Transformer-based model)	$40K \times 100$	2^0	Corridor	2025
[92]	141×1	15 m	Partial roundkey	DAR-NN (DANN-based model)	$40K \times 100$	2^0	Corridor	2025
[99]	$1,000 \times 5$	30 m	Partial key	Multi-channel profiled CPA	Not reported	2^0	Corridor	2026

attack requirement to hundreds of single-shot traces, showing that profiling traces could be transferred to far-field measurements. Later works further diversified the attack methodology, including relay-assisted acquisition, spectrum-addition-based CPA, non-harmonic-frequency exploitation, and feature-reconstruction methods for noisy long-distance traces. In this progression, [99] represents a complementary advance. Rather than relying on a single carefully selected frequency, it treats multiple screaming-channel frequencies as independent leakage channels and combines them to improve robustness when some bands are weak or polluted. This chronological trend indicates that FEM-SCA is no longer merely a laboratory curiosity, it is evolving into a practical remote attack framework in which distance, trace complexity, profiling assumptions, and environmental interference are gradually being addressed through better signal selection, learning-based modeling, and multi-channel exploitation.

As summarized in Table XII, the enhanced attack capability of FEM-SCA on nRF52 TinyAES implementations can be divided into four parts, which are 1) remote feasibility test, 2) DL-driven enhancement, 3) signal-acquisition enhancement, and 4) robust practicalization enhancement, as shown in Fig-

ure 10.

1) Remote attack feasibility test. The first part established the basic feasibility of FEM-SCA. Early works showed that cryptographic leakage unintentionally coupled into RF transmissions can be captured at distances and used for key recovery. However, these attacks still required large numbers of repeated encryptions, extensive profiling traces, and relatively controlled measurement conditions, indicating that the threat was technically real but not yet operationally mature.

2) DL-driven capacity enhancement. The second stage shifted the emphasis from proving leakage existence to reducing the number of traces needed for attack. CNN-based approaches replaced or complemented classical statistical analysis and learned discriminative leakage features from profiled traces. In particular, cable-trained or multi-device-trained neural models greatly improved the attack efficiency, reducing the required number of traces to recover the key from thousands or millions of averaged measurements to hundreds of single-shot far-field traces.

3) Signal-acquisition enhancement. The third part focused on improving the quality and availability of the captured RF leakage itself. Relay-based acquisition, spectrum addition and non-harmonic frequency exploitation, expanded the attacker's

ability to obtain usable traces under less ideal conditions. This stage demonstrates that FEM-SCA performance is shaped not only by the attack method, but also by signal propagation, frequency selection, receiver placement, and RF-channel manipulation.

4) Robust practicality enhancement. The most recent stage targets practical long-distance and noisy environments. Transformer-based learning, feature reconstruction based on DANN model, and multi-screaming-channel fusion to some extent mitigate the effect caused by cross-device variability, environmental interference, and polluted frequency bands. These works suggest that FEM-SCA is now gradually evolving from a specialized attack into a broader remote threat case, where robustness, adaptability, and reduced assumptions become central measures of attack practicality.

Next, we turn to attack targets and variants, examining how FEM-SCA has expanded from TinyAES to broader cryptographic implementations and usages.

VI. ATTACK TARGETS & VARIANTS

Beyond improving attack efficiency by using the TinyAES as the reference cryptographic target, recent FEM-SCA research has increasingly explored the generality of this leakage mechanism across different cryptographic implementations and application scenarios. Starting from TinyAES-based demonstrations, attacks have been extended to hardware accelerators, post-quantum cryptographic primitives, and practical wireless protocols, revealing the broad applicability of RF-mediated side-channel leakage.

Notice that some works included in this survey do not necessarily demonstrate long-distance over-the-air attacks, but they still exploit the core leakage mechanism of screaming channels: the unintended coupling between digital computation and analog/RF circuitry, through which sensitive information is modulated onto RF signals and becomes externally observable. Therefore, they remain relevant to the screaming-channel threat model even when the measurement setup is conducted by cable or only partially remote. In contrast, other remote side-channel works, such as the RF-based trapped-ion quantum-computer attack [103], TEMPEST attack [43], [104], [105], and EM eye [106], may involve remote EM acquisition, but they do not rely on digital-to-analog/RF coupling in mixed-signal chips. Their leakage originates from EM emanations themselves rather than from computation-induced leakage coupled into a communication carrier. For this reason, such works are better regarded as broader EM side-channel studies and are not discussed in detail in this survey. Besides, although some recent EM eavesdropping attacks [107], [108] exploit coupling between two EM signals, they do not focus on the RF range. We therefore exclude them from our review of screaming-channel attacks.

In 2022, Ruize et al. explored the RF-based leakage from two different PQC implementations [109], which are CRYSTALS-Kyber and Saber, by using screaming channel as the side channel [110], [111]. However, during the attack in both cases [110], [111], the side-channel signal is captured via a direct, conducted connection using an SMA coaxial cable,

which does not qualify as a true remote far-field scenario. This limitation is mainly from the fact that the RF leakage of PQC implementations is still insufficiently exploitable under realistic over-the-air conditions with current profiling methods. Even with cable-captured traces, which provide substantially cleaner and stronger leakage compared with remote RF acquisition, the attack efficiency remained relatively low. Consequently, extending these attacks to practical remote scenarios would require further advances in leakage enhancement, signal acquisition, and robust attack modeling.

In addition to the unprotected AES, [26] conducted the first screaming channel attack on Bluetooth device implementation of masked AES, specifically targeting the Rivain–Prouff (RP) masking scheme [113], in 2024. In this case, they first point out that TinyAES is seldom deployed in contexts where computational resources are not severely constrained. In security-critical applications, cryptographic implementations typically incorporate side-channel countermeasures [114]. Therefore, they experimentally evaluate to which extent the RP-masked AES implementation can be compromised under the FEM-SCA scenario. Except the receiving antenna, the hardware setup in [26] is kept as the same as in [38], [85]. To bypass the theoretical strength of the addition-chain based masking, the attack in [26] focuses the leakage from the *MixColumns* operation. The attack result is shown in Table XIII. The attack's inefficiency, characterized by the need for hundreds of thousands of traces to recover a subkey, stems from a combination of the victim's strong side-channel resistance and the attacker's suboptimal signal capture. Firstly, the RP-masking scheme is fundamentally designed to be provably secure against lower-order attacks by splitting sensitive variables into random shares, effectively diluting the key-dependent information in the side-channel output and forcing the attacker to perform a complex higher-order analysis. Secondly, this already faint signal is further compromised by the attacker's hardware. The replacement from the grid parabolic antenna TL-ANT 2424B (24 dBi gain) to vertical antenna VERT2450 (3 dBi gain) provides limited ability to focus on and collect the low-power, amplitude-modulated EM emanations from a distance. This results in traces with a very low signal-to-noise ratio, requiring the accumulation of a massive number of side-channel traces to statistically distinguish the subtle leakage patterns. Another FEM-SCA case focuses on the nRF52 implementation of RP-masked AES remotely is [115], in which the same research group goes one step further from [26] by shifting the attack point to the *ShiftRow* operation. This makes the CNN model in [115] be 80% more efficient than the attack in [26], which utilizes 50K traces without any repetition to recover a partial key from the target implementation of RP-masked AES.

While all reviewed FEM-SCAs focus on the software implementations of AES, [112] demonstrates the first successful screaming channel attack on hardware AES accelerator, in 2025. The attack exploits unintentional information leakage through RF signals emitted by the crypto part of the chip during AES-CCM mode encryption. Even though the experimental victim keeps identical as in [38], [85], [92], which is the same nRF52832 Bluetooth SoC target, they aim to compromise the hardware AES accelerator of the victim device

TABLE XIII: Detailed **partial key** recovery results of the FEM-SCA on RP-Masked AES conducted in [26].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
RP-Masked AES	Cable-trace trained MLP	0.1 m	290K	1	2^0	$500K \times 100$	Office

TABLE XIV: Detailed **full key** recovery results of the FEM-SCA on AES hardware accelerator conducted in [112].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
Hardware AES accelerator	CPA	1 m	180K	10K	$2^{42.8}$	/	Office

remotely. Note that hardware implementations of crypto are significantly more side-channel resilient than software, due to several architectural and physical advantages [116]. First, hardware designs can leverage parallelism and pipelining, which execute multiple operations simultaneously. This causes side-channel leakage to be an aggregate of many concurrent processes, effectively obscuring the leakage from any single, targeted operation like an *SBox* lookup. Second, hardware implementations benefit from synchronous clocking. The clock network distributes a global signal that triggers all flip-flops simultaneously, leading to a power consumption profile that is dominated by the clock edges themselves rather than the data-dependent switching of individual logic gates [117].

In [112], the core equipment in the experimental setup is a USRP-2944R SDR used as the receiver. To capture the screaming channel leakage, they demodulate the RF signals at a center frequency of 2.528 GHz, which is the Bluetooth channel frequency (2.4 GHz) offset by eight times the AES accelerator's clock frequency (16 MHz). By performing leakage analysis on a reference device with a known key, they infer several internal properties of the proprietary accelerator, including that the AES round appears to be fully parallel and that the state register after round computation is closely related to the last-round *SBox* input. Based on this reverse-engineering step, the attack targets the encryption of the counter block *Ctrl* in CCM mode, because the corresponding keystream block can be derived from known message and ciphertext information. The key-recovery stage in [112] combines correlation analysis with key enumeration. For each captured trace, the same AES-CCM encryption is repeated 10K times and averaged to improve the signal-to-noise ratio, reflecting the very weak RF leakage of the hardware accelerator. The authors evaluate both cable-captured traces and antenna-captured traces at a distance of 1 m in an office environment. Using the Hamming weight of the last-round *SBox* input as the leakage model, correlation analysis can recover most bytes of the last round key, but not all of them directly. For antenna-captured traces, four out of sixteen round-key bytes remain incorrectly ranked, requiring additional enumeration to reconstruct the original AES key. As shown in Table XIV, with 180K traces captured at 1 m, the full encryption key can be recovered with an enumeration complexity of approximately $2^{42.8}$. This result is important because it shows that the hardware AES-CCM accelerator is not immune to screaming-channel leakage. At the same time, the high trace cost, the need for massive averaging, and the large enumeration complexity indicate that attacking hardware accelerators through FEM-SCA remains substantially more

difficult than attacking software TinyAES implementations.

Building on the CPA-based feasibility study on hardware cryptographic accelerator [112], [118] further improves the attack efficiency against the same hardware AES-CCM by introducing an ensemble-learning analysis. Compared to [112], the attack setting in [118] remains largely unchanged. The key difference lies in the analysis method. Instead of relying only on correlation analysis, [118] trains an ensemble of MLP models to classify traces. The profiling stage uses 300K cable-captured traces, with each obtained by averaging 10K repeated encryptions. From these profiling traces, the authors extract five short intervals around the last rounds of several AES-CCM encryptions and use them to train 3×16 MLP models, where three models are trained for each byte position to reduce common prediction errors through ensemble voting. During the attack stage, traces are captured from two unseen target devices, either through a cable or by antenna at 1 m in an office environment. As shown in Table XV, with 90K traces captured at 1 m, each again averaged from 10K repeated encryptions, the method recovers the full AES key after key enumeration. Compared with the correlation-based attack on the same target [112], this reduces the required number of attack traces by half and lowers the enumeration complexity to 2^{24} . This result shows that profiled learning can make hardware-accelerator-oriented FEM-SCA more efficient, but it also highlights the remaining practical cost: the attack still requires massive repeated encryptions, a large cable-based profiling set, and a carefully controlled acquisition process.

Although FEM-SCA on AES has achieved substantial progress in attack efficiency and practicality, the broader studies on different targets and variants reveal that extending these advances to more realistic applications remains difficult. Attacks on PQC primitives, RP-masked AES, and hardware AES accelerators show that RF-mediated leakage can still be observed beyond unprotected software AES, but the resulting attacks commonly suffer from low SNR, large profiling requirements, extensive trace collection, repeated encryptions, or limited key recovery. Similarly, system-level leakage studies demonstrate that raw digital data from buses, memory access, UART, and peripheral interfaces can be unintentionally radiated through the RF front-end, yet the recovered information is often partial or probabilistic under practical conditions. Therefore, while TinyAES has served as an important benchmark for demonstrating and improving FEM-SCA techniques, the results on broader attack targets suggest that FEM-SCA is still far from a universally efficient remote attack. Its practicality remains highly dependent on the leakage strength of the target,

TABLE XV: Detailed **full key** recovery results of the FEM-SCA on AES hardware accelerator conducted in [118].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Key enumeration	# Profiling traces	Environment
Hardware AES accelerator	Ensemble learning-based attack	1 m	90K	10K	2^{24}	300K $\times$ 10K	Office

TABLE XVI: Detailed **clear-text data** (ranging from 0x00 to 0x0f) recovery results of the FEM-SCA conducted in [25].

Target	Attack method	Distance	# Attack traces	Encryption repetitions	Single-trace accuracy	# Profiling traces	Environment
nRF UART	LSTM-based attack	20 m	1	1	60%	Few hundreds	Office

the RF coupling path, the attacker’s acquisition setup, and the ability of profiling models to tolerate weak and noisy far-field traces.

Shifting the focus from cryptographic key extraction, [25] demonstrates that a wide range of digital components within a modern embedded system can unintentionally leak raw, sensitive information through the device’s own radio transmitter. They experimentally show that signals from internal buses, serial ports, memory accesses, and even external protocols like NFC can be modulated and amplified by the RF front-end, enabling an attacker to directly read out this data from the far field. The attack setup involved using the same SDRs and antenna as in [23], [24], [38], [85] to capture RF transmissions from common IoT devices like the Nordic nRF, ESP32, and TI CC2642. The results confirmed that an adversary could successfully demodulate and extract clear-text data, such as bytes sent over a UART interface or specific values written to memory, from a single trace and at distances of up to 20 m. Furthermore, the paper illustrates that even without a direct galvanic connection, signals from components located tens of centimeters away on the PCB can be unintentionally picked up, amplified, and broadcast by the device’s radio, proving the pervasiveness and severity of this leakage channel. Afterwards, they show that if an attacker can inject malicious code (e.g., via malware or a software vulnerability), they are no longer limited to what the system happens to leak. They can now orchestrate the leakage. The injected code can actively modulate sensitive data (like user data) in a way that is perfectly tailored for long-range RF exfiltration. They show the attack specification details for the case on UART byte-value classification, in which they train a Long-Short Term Memory (LSTM) model by using only few hundred 16-sample traces to extract the “clear-text” data (ranging from 0x00 to 0x0f). The attack result shows that it is feasible to classify the byte based on a single trace capturing with a 60% accuracy, which is illustrated in Table XVI. While the specific UART attack distance is not explicitly stated, we infer it to be up to 20 m, as this was the maximum far-field range established for their general experimental setup.

Another noteworthy extension of screaming-channel research toward satellite-related communication hardware is presented in [119], which does not evaluate an actual satellite but instead studies several small-satellite-relevant sub-GHz SoC transceivers to examine whether their RF transmissions exhibit leakage correlated with digital processor activity. Following the conceptual discussion in [120], this work treats a leakage as visible when a continuous RF transmission changes into a

periodic dashed or intensity-varying pattern synchronized with the processor’s sleep-encryption cycle. Using this method, they first reproduced the known nRF52832 Bluetooth leakage detection process, then examines several small-satellite-relevant sub-GHz SoC transceivers. The TI CC1111 SoC shows a clear dashed-line pattern around its intended transmission band, suggesting a potential screaming-channel leakage path. The TI CC1310 SoC shows weaker evidence: no obvious dashed lines are observed, but some amplitude changes appear correlated with processor state. The Seeed Wio-E5, used as a LoRa-like SoC target, does not show a clear relationship between processor activity and RF amplitude. Therefore, this work is useful as a qualitative leakage-screening study for satellite-related RF SoCs, but it does not provide a quantitative FEM-SCA attack result.

More recently, the scope of far-field EM side-channel analysis has been further extended beyond cryptographic implementations and RF-enabled embedded SoCs. In particular, ModelSpy, A DNN remote attack framework proposed in NDSS’26 [121], demonstrated that remotely observable EM emanations in the radio channel can reveal not only secret-dependent cryptographic operations, but also high-level structural information associated with complex computing workloads. Rather than targeting secret keys, ModelSpy focuses on black-box DNN architecture snooping from GPUs, with the goal of reconstructing the number and types of neural-network layers as well as their layer-wise hyperparameters. Recovering such information is particularly relevant because knowledge of the victim architecture can improve subsequent black-box attacks [122]–[125]. Different from conventional screaming-channel attacks, ModelSpy does not rely on an intentional RF carrier generated by a wireless communication module. Instead, the carrier originates from the continuous radiative EM emissions of GPU hardware components, such as voltage regulators, memory clocks, and memory-refresh circuits [126]. Since these hardware activities inherently generate relatively high-frequency EM radiation in the MHz-to-GHz range, their emissions can effectively serve as high-frequency carrier signals. In [121], the practical evaluation further demonstrates that such architecture-dependent leakage can be captured at meter-scale distances. The experimental receiver consists of a USRP B210 and either an omnidirectional antenna or a 20×20 cm panel antenna, operating around a center frequency of 5 GHz with an 8 MHz sampling rate. Experiments are conducted on five consumer NVIDIA GPUs and a diverse collection of DNN architectures, including variants of AlexNet [127], VGG [128], ResNet [129],

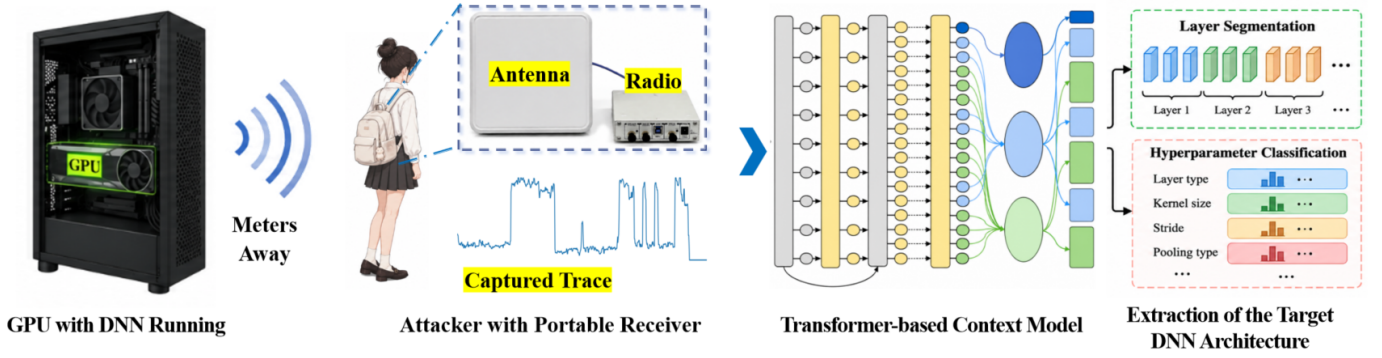


Fig. 11: Illustration of the remote FEM-SCA conducted in [121], which is to reconstruct the DNN architecture by sniffing EM signals leaked from the victim's GPU.

TABLE XVII: Detailed **DNN layer segmentation and hyperparameter** recovery results of the FEM-SCA on the commercial GPU target conducted in [121].

Target	Attack method	Distance	# Test architecture	Layer segmentation accuracy	Hyperparameter accuracy	Environment
DNNs in GPU	ModelSpy (Transformer-based reconstruction)	1 m	260	97.6%	94.0%	Office
DNNs in GPU	ModelSpy (Transformer-based reconstruction)	0, 1, ..., 7 m	100	86.7% (5 m)	81.7% (5 m)	Open field
DNNs in GPU	ModelSpy (Transformer-based reconstruction)	Not Reported	100	> 90.1%	> 85.7%	Office with obstacles
DNNs in GPU	ModelSpy (Transformer-based reconstruction)	1 m	100	88.4%	80.7%	Office with Wi-Fi interference at 1 m

and BERT [130], together with randomly generated CNN, LSTM, Transformer, and linear architectures. Across the overall evaluation, ModelSpy achieves an average 97.6% layer-segmentation accuracy and 94.0% hyperparameter-estimation accuracy on unseen DNN architectures. The attack remains effective at distances of up to approximately 6 m under the main experimental configuration, whereas the layer-segmentation accuracy decreases substantially to 42.3% at 7 m. Thus, unlike earlier DNN architecture-snooping techniques that depend on millimeter-range measurements near the GPU or its power cable [5], [131], ModelSpy [121] demonstrates that detailed model information can be extracted from radiative EM signals at several meters away.

Afterwards, [121] further evaluated through-wall attacks using wood, concrete, and glass walls while placing the victim GPU and attacker in separate rooms, where the radio receiver can be concealed inside a backpack. For the layer-segmentation accuracy and hyperparameter-estimation accuracy, they still achieved 96.0%/87.7% through wood, 96.1%/85.7% through concrete, and 96.3%/87.3% through glass, respectively, indicating that common physical obstacles introduce only limited degradation to the attack. The robustness was further evaluated under intended RF interference by introducing an active Wi-Fi access point operating at 5.18 GHz. When the interfering AP is placed only 1 m from the victim, the layer-segmentation and hyperparameter-estimation accuracies decreased by 8.7 and 7.7 percentage points, respectively, demonstrating that strong nearby RF activity can degrade the captured leakage. Moreover, the experimentally validated 6-m range does not appear to represent the physical limit of the leakage: a preliminary experiment using a larger parabolic antenna successfully extends the operating distance to beyond 10 m. Table XXIII summarizes the attack results in [121]. From the perspective of the evolution of FEM-

SCAs, ModelSpy proposed in [121] represents a notable shift in attack target level, providing an important example of how FEM-SCA can be expanded from cryptographic secret recovery toward high-level semantic inference of complex computing workloads.

The next section introduces existing publicly available FEM-SCA collections and their role in supporting reproducible evaluation.

VII. PUBLIC FEM-SCA DATA COLLECTIONS

Public FEM-SCA data collections are essential for transforming screaming-channel research from isolated proof-of-concept demonstrations into a reproducible and comparable research field. Unlike conventional power or near-field EM analysis, far-field EM leakage is strongly affected by propagation conditions and environmental interference. Without shared data collections, it is difficult to determine whether an improvement comes from a genuinely stronger attack model or simply from a cleaner measurement setup. To date, six public screaming-channel data collections have provided reusable experimental foundations for this area (as concluded in Figure 2), covering the original CCS'18 screaming channel collection [23], the CHES'20 screaming channel collection [24], the ASHES'20 DL-oriented collection (first-round AES) [38], the CPSS'21 DL-oriented collection (last-round AES) [85], the ACSAC'24 BlueScream collection [80], and the NDSS'26 GPU-DNN collection [121]. However, these resources are not yet well-organized or systematic enough to be regarded as standardized datasets such as [132]–[134], as they often cover only several isolated attack distances, target devices, or experimental scenarios without a unified structure and labeling format. Therefore, we refer to them as public data collections rather than datasets in the following.

TABLE XVIII: Summary of traces included in the CCS'18 screaming channel data collection [23].

Subset	Target	Environment	Distance	Included executions	# Sample each trace	Encryption Repetitions	# Traces
tinyaes_anechoic_attack	TinyAES	Chamber	10 m	1st & 2nd AES rounds	500	1,499	3,000
tinyaes_anechoic_template	TinyAES	Chamber	10 m	1st & 2nd AES rounds	1,499	500	243,911
mbdtdls_office	mbdTLS	Office	1 m	Full AES encryption	550	500	38,645
Total	—	—	—	—	—	—	285,556

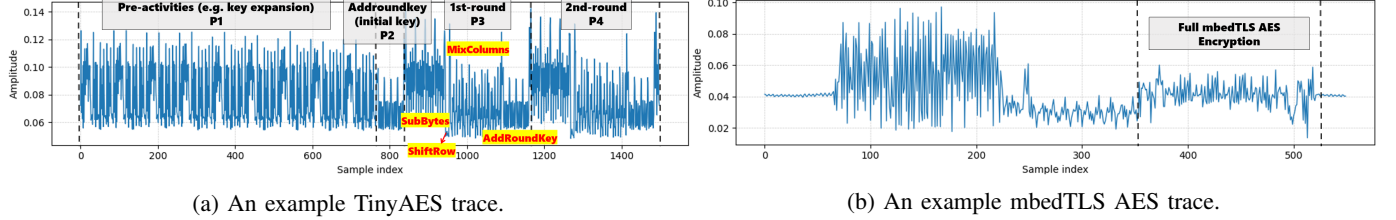


Fig. 12: A visual illustration of traces in the CCS'18 screaming channel data collection [23], with each execution part denoted according to the TVLA leakage detection results.

Notice that although some works claim to release data alongside the publication, we do not treat all of them as independent public data collections, as the provided resources may be access-restricted, only partially available, or derived from previously released trace collections. For example, [112], [118] state that all related data and scripts are available through a KTH BOX link, which currently redirects to a SSO login page, making it inaccessible to users outside KTH. Therefore, this work is not included in our discussion of public FEM-SCA data collections. Another example is that although [92] states that its code and traces are publicly available, the trace data used in its evaluation are derived from the CPSS'21 DL-oriented collection [85]. Therefore, we do not treat it as an independent public FEM-SCA data collection in this survey.

The first publicly available screaming-channel data collection was introduced by [23], which established the fundamental feasibility of remote EM leakage exploitation. In the local package, the released traces are stored as NumPy arrays and divided into three subsets: a `tinyaes_anechoic_10m_attack` subset with 3,000 attack traces, a `tinyaes_anechoic_10m_template` subset with 243,911 template/profiling traces, and an `mbdtdls_1m_home` subset with 38,645 traces. Each subset is accompanied by a fixed AES key file and a plaintext file, allowing the traces to be linked to known cryptographic inputs for correlation or template-based key recovery. The TinyAES traces correspond to the 10 m anechoic-chamber scenario, where the victim repeatedly executes AES while Bluetooth transmission is active, and the resulting digital leakage is coupled into the RF front-end and captured remotely. The mbedTLS subset represents a more realistic 1 m office scenario against a software AES implementation from a practical cryptographic library. The mbedTLS library [135] is a lightweight open-source cryptographic library widely used in embedded and IoT systems to provide implementations of protocols and primitives such as TLS, AES, and other security functions. The repository in [23] is with a size of approximately 2.6 GB, with all data details presented in Table XVIII. Notice that in this data collection, each single trace is the average of 500

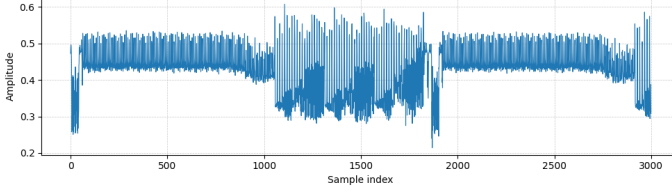
measurements of the same repeated encryption to eliminate the effect caused by the environmental noise and interference.

For the CCS'18 screaming channel data collection, we further examined the first-round SBox-output leakage by using TVLA [136] of the first key byte using a fixed-versus-random style partition based on the Hamming weight of the intermediate value. We take the `tinyaes_anechoic_10m_template` subset as an example. Specifically, 80K traces were divided according to $HW(SBox(P[0] \oplus K[0])) > 4$ and $HW(SBox(P[0] \oplus K[0])) < 4$, while traces with $HW = 4$ were excluded to avoid an ambiguous middle class. The resulting Welch's t-test shows clear leakage around the later part of the trace, with a maximum absolute t-value of 8.659 at sample index 848 (exceeding the common $|t| > 4.5$ leakage threshold [36]), which falls within the first-round AES operation after the initial AddRoundKey stage. From this located leakage point, the remaining execution structure can be visually derived by aligning the surrounding waveform patterns with the AES execution flow. As shown in Figure 12 (a), the trace first contains pre-activities such as key expansion, followed by the initial AddRoundKey operation, the first-round operations including SubBytes, ShiftRows, MixColumns, and AddRoundKey, and then the subsequent second-round activity. For the mbedTLS subset, we conduct the same leakage detection process and among 38,645 traces, the Welch's t-test shows clear leakage around sample index 375, where the maximum absolute t-value reaches 13.958, with five samples exceeding the common $|t| > 4.5$ threshold. Figure 12 (b) shows an example trace in the `mbdtdls_1m_home` subset.

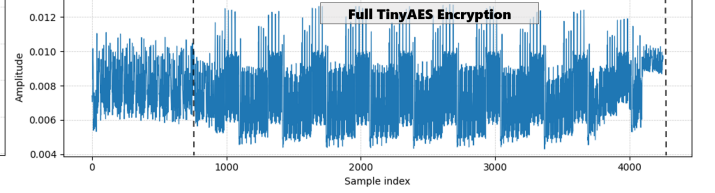
The CHES'20 screaming channel collection [24] extends the CCS'18 proof-of-concept traces into a more systematic resource for understanding the physical and statistical properties of leakage. The CCS'18 screaming channel data collection primarily captures AES leakage through quadrature amplitude demodulation centered at 2.528 GHz, demonstrating that exploitable cryptographic information can be recovered from a specific RF spectral component. However, for the same Nordic nRF52 Bluetooth 5 target operating in the 2.4 GHz

TABLE XIX: Summary of traces included in the CHES'20 screaming channel data collection [24].

Subset	Target	Environment	Distance	Included executions	# Sample each trace	Encryption repetitions	# Traces
compare_frequencies	TinyAES	Office	0.1 m	1st & 2nd AES rounds	1,499	500	36,000
hwcrypto	HW AES-128	Office	0.1 m	Full AES execution	2,999	500	75,602
shannon_080719	TinyAES	Office	1 m	Full AES execution	4,250	500	16,190
Total	—	—	—	—	—	—	119,792



(a) An example hardware AES trace.



(b) An example full-round TinyAES trace.

Fig. 13: A visual illustration of traces in the CHES'20 screaming channel data collection [24], with each execution part denoted according to the TVLA leakage detection results (the hardware AES trace is not partitioned since the lack of corresponding plaintext and key in the collection for conducting the leakage detection).

band, screaming-channel leakage is not confined to a single frequency, but can emerge at multiple harmonic frequencies. Thus, a single center frequency provides only a partial view of the RF manifestations of the underlying cryptographic activity. The CHES'20 screaming channel collection [24] further extends the measurement scope by collecting traces at multiple leakage frequencies for the same nRF52 target, allowing the frequency-dependent characteristics of screaming-channel leakage to be examined more systematically. This observation subsequently motivates more advanced studies that exploit multiple screaming-channel frequencies as independent leakage channels, rather than treating them merely as alternative or redundant capture frequencies. Notice that although the GitHub page claims that the CHES'20 trace release covers a broad set of experiments from leakage characterization to leakage detection at 34 m, our detailed inspection of the downloaded package only identified three explicitly organized subsets, called `compare_frequencies`, `hwcrypto`, and `shannon_080719`.

Table XIX shows the summary of traces included in the CHES'20 screaming channel data collection [24]. In the released package, the `compare_frequencies` subset contains TinyAES traces captured with a USRP B210 at 10 cm for four target frequencies, namely 2.528, 2.530, 2.554, and 2.608 GHz. For each frequency, both variable-key profiling traces and fixed-key attack traces are provided, with 1,499 samples per trace and 500 repeated acquisitions per trace. Since the target in the `compare_frequencies` subset shares the same TinyAES firmware as the TinyAES target in the CCS'18 collection, its traces exhibit a comparable AES execution structure and leakage pattern as shown in Figure 12. For the `hwcrypto` subset, the traces correspond to the CHES'20 paper's attempt to evaluate screaming-channel leakage from the dedicated AES-128 hardware block of the nRF52832. Different from the TinyAES software target used in the main leakage-characterization experiments, this subset focuses on a hardware cryptographic implementation, where

the AES computation is executed inside the on-chip accelerator rather than through software instructions. The paper reports that the screaming channel traces reveal leakage related to the transfer of plaintext, key, and ciphertext between memory and the hardware block, but the internal AES round operations are not clearly visible under their setup. Therefore, this subset is mainly useful for studying the boundary of FEM-SCA on hardware-assisted cryptography, showing that hardware AES is substantially harder to exploit than software TinyAES. For the `shannon_080719` subset, the traces share the same TinyAES target as the `compare_frequencies` subset, but they capture a longer execution window that contains the full AES encryption rather than only the first two rounds. This makes the subset useful for observing the complete temporal structure of the software AES execution, including the repeated round-level operations across the full encryption. Compared with `compare_frequencies`, which is more suitable for analyzing frequency-dependent leakage behavior in a shortened trace window, `shannon_080719` provides a more complete view of how the AES execution unfolds in the screaming channel. It can therefore support full-trace leakage characterization, round-level localization, and qualitative analysis of how screaming-channel leakage persists across the whole encryption.

While the CHES'20 collection mainly serves as an experimental resource for understanding the physical behavior of screaming-channel leakage, the ASHES'20 DL-oriented collection (first-round AES) [38] shifts the focus toward attack scalability under more systematically varied remote conditions. In particular, ASHES'20 introduces traces collected across more gradually changing attack distances, making it possible to observe how leakage quality degrades as the receiver moves farther from the target. More importantly, this collection is explicitly evaluated with deep-learning-based attack models, marking a transition from statistical characterization and profiled correlation analysis toward learning-based FEM-SCA evaluation. Therefore, ASHES'20 data col-

TABLE XX: Summary of traces included in the ASHES'20 DL-oriented screaming channel data collection [38].

Subset	Target	Environment	Distance	Included executions	# Sample each trace	Encryption repetitions	# Traces
for_training	TinyAES	Office	cable, 1, 2, 4, 8 m	First-round AES	400	100	1400K
for_testing	TinyAES	Office, corridor	3, 6, 9, 15 m	First-round AES	400	1, 100, 1000	120K
Total	—	—	—	—	—	—	1520K

TABLE XXI: Summary of traces included in the CPSS'21 DL-oriented screaming channel data collection [85].

Subset	Target	Environment	Distance	Included executions	# Sample each trace	Encryption repetitions	# Traces
for_training	TinyAES	Office	cable	Last-round AES	400	100	200K
for_testing	TinyAES	Corridor	15 m	Last-round AES	400	1, 10, 100	75K
Total	—	—	—	—	—	—	275K

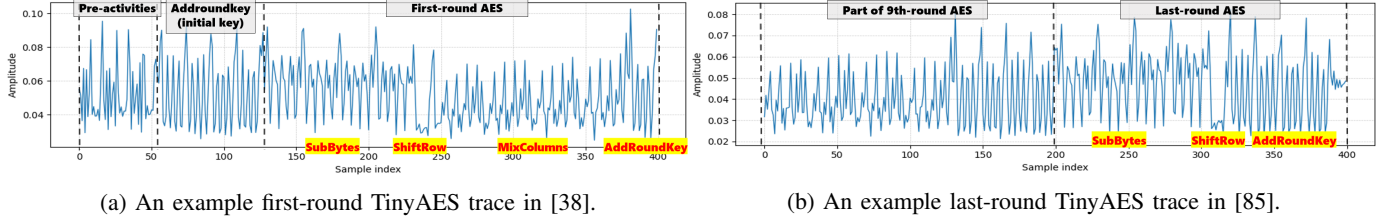


Fig. 14: A visual illustration of traces in the ASHES'20 and CPSS'21 screaming channel data collection [38], [85], with each execution part denoted according to the TVLA leakage detection results.

lection can be regarded as an intermediate step between early leakage-understanding data release and later deep-learning-oriented screaming channel data testbed. It focuses on Nordic nRF52 Bluetooth SoC running a TinyAES software implementation of AES, with traces captured by an Ettus USRP N210 SDR connected to a TP-Link TL-ANT2424B parabolic antenna. The released collection contains two subset, called `for_training` and `for_testing`, which is organized around deep-learning-based attack evaluation. The training traces are captured at a distance of 1 m, 2 m, 4 m, 8 m and by coaxial cable, while testing traces are provided for 3 m, 6 m, 9 m, and 15 m, with 1, 100, and 1000 encryption-repetition variants. For all data in the collection, each trace contains 400 sampling points, including the first-round execution pattern of the TinyAES. Table IV shows the summary of traces included in the ASHES'20 DL-oriented collection (first-round AES).

Following the ASHES'20 collection, which evaluates deep-learning attacks under gradually changing over-the-air distances, the CPSS'21 collection further refines the data design by separating the profiling and attack conditions more aggressively. Instead of training neural networks on traces captured at remote distances, [85] collects cleaner profiling traces through a coaxial cable and then tests whether the trained CNN can generalize to far-field traces captured from victim devices at 15 m. The target remains a Nordic nRF52832 Bluetooth SoC running a TinyAES software implementation of AES-128, while the leakage is captured by an Ettus USRP N210 receiver tuned to 2.528 GHz with a 5 MHz sampling rate. In the profiling stage, the collection uses 100K cable traces combined from five profiling devices, with each trace averaged from 100 measurements of the same encryption. In the attack stage, it provides remote traces from different devices captured at 15 m, including non-repeated traces and averaged-trace variants.

Therefore, compared with ASHES'20, the CPSS'21 collection shifts the dataset focus from distance-dependent generalization to cross-domain learning between high-SNR cable traces and low-SNR far-field traces, making it an important resource for evaluating domain robustness in deep-learning-based FEM-SCAs. Table V shows the summary of traces included in the CPSS'21 DL-oriented collection (last-round AES).

The two representative trace plots in Figure 14 show the close relationship between the ASHES'20 and CPSS'21 data collections. Since both collections were generated by the same research group on the nRF52 TinyAES target, they share several common characteristics, including a 400-sample trace window, similar amplitude-based waveform representation, and operation-level temporal segmentation. The ASHES'20 trace on the left mainly covers the beginning of the AES execution, including pre-activities, the initial AddRoundKey, and the first-round AES operations, where SubBytes, ShiftRows, MixColumns, and AddRoundKey can be visually located. In contrast, the CPSS'21 trace on the right shifts the observation window toward the end of the encryption, containing part of the ninth round and the last AES round, where the visible operations include SubBytes, ShiftRows, and AddRoundKey. This similarity in trace format, together with the different selected AES windows, reflects the methodological continuity between the two collections while also showing how CPSS'21 reuses the established acquisition style to support more targeted deep-learning attacks on later-round leakage. Notice that the CPSS'21 trace collection focuses on the last-round AES execution, and the recovery target is therefore designed as the last-round key rather than the original cipher key directly. In this setting, the adversary first learns the leakage associated with last-round intermediate values and then uses the recovered round-key bytes to derive the AES

TABLE XXII: Summary of traces included in the ACSAC'24 BlueScream data collection [80].

Subset	Target	Environment	Distance	Included executions	# Sample each trace	Encryption repetitions	# Traces
pairing_10cm_anechoic	BLE re-keying AES	Chamber	0.1 m	Full AES execution	4000	1	81,920
2lna_highgain_norep	BLE re-keying AES	Office	1.2 m	Full AES execution	4000	1	106,051
Total	–	–	–	–	–	–	187,971

TABLE XXIII: Summary of traces included in the NDSS'26 GPU-DNN data collection [121].

Subset	Target	Environment	Distance	Included executions	# Sample each trace	Execution repetitions	# Traces
cross_GPU_evaluation	Five GPUs	Office	1 m	CNN, LSTM, and Transformer inference	5,023	1	10,696
distance_evaluation	RTX 3060 Ti	Open field	0, 1, 2,..., 7 m	Mixed DNN inference	5,023	1	6,946
cross_wall_evaluation	RTX 3060 Ti	Office	Not reported	Mixed DNN inference	5,023	1	2,421
Total	–	–	–	–	–	–	20,063

master key through the inverse key schedule. Consequently, the attack must correctly recover every byte of the last-round key. Even a single erroneous subkey byte can prevent successful reconstruction of the original AES key or substantially increase the subsequent key-enumeration cost. The shift to the last-round key in CPSS'21 is motivated by a more realistic remote-attack assumption: when traces are captured from a distance, the attacker may not be able to control or observe the plaintext, whereas the ciphertext is often more accessible from the transmitted data or protocol output. Therefore, CPSS'21 models the attack around last-round AES leakage, where the relevant intermediate values can be computed from the known ciphertext and guessed last-round key bytes. Under this setting, the adversary recovers the last-round key first and then derives the original AES key through the inverse key schedule.

In 2024, the BlueScream data collection is built and released in [80] at the ACSAC'24 conference. Different from the ASHES'20 and CPSS'21 collections, which mainly focus on TinyAES traces generated from controlled firmware, BlueScream shifts the data-collection scenario toward a more realistic BLE protocol stack. The collection targets the BLE key derivation mechanism, also known as the re-keying procedure, on a Nordic nRF52832 development kit running NimBLE-based firmware [137]. The collection considers three firmware variants, called *Fcustom* for controlled experiments, *Finstru* for instrumented BLE evaluation with controllable AES inputs, and *Fdefault* for a stock BLE setting where only one AES input is known. By manipulating BLE communication, the attacker forces the victim to transmit during the cryptographic operation, allowing the RF front-end to broadcast the leakage. Therefore, compared with earlier TinyAES-oriented collections, BlueScream provides a more protocol-aware FEM-SCA data collection, covering different distances, averaging settings, and firmware assumptions.

Table XXII listed the statistical information of the ACSAC'24 BlueScream data collection, in which the publicly available traces mainly correspond to the most realistic *Fdefault* setting, rather than covering all firmware variants equally. There are two trace subsets in the collection, which are called the *pairing_10cm_anechoic* set and the *2lna_highgain_norep* set. There are around 65K profiling traces and 16K testing traces in the

pairing_10cm_anechoic subset, with each trace is captured at 10 cm to the target at an anechoic chamber by using an omnidirectional WiFi antenna. For the *2lna_highgain_norep* subset, there are approximate 65K profiling traces and 41K testing traces locally, with each one captured at 1.2 m distance to the victim device at an normal office environment by using a high-gain directional antenna with two LNAs. The BlueScream data collection is well suited for evaluating realistic wireless-protocol attack scenarios, although its scope remains centered on BLE AES leakage rather than a broad set of targets.

In 2026, the NDSS'26 GPU-DNN Collection [121] further extended publicly available far-field data from cryptographic implementations to GPU-based DNN inference workloads. Unlike conventional screaming-channel collections that primarily associate remotely captured traces with cryptographic intermediate values or secret-dependent labels, this collection records traces generated during the execution of different DNN architectures on commodity NVIDIA GPUs. The NDSS'26 GPU-DNN Collection contains 20,063 traces, with each trace consisting of 5,023 samples. These traces cover different GPU devices, DNN workloads, propagation distances, and physical obstacles. We broadly divide the collection into three subsets according to its experimental settings, as shown in summarized in Table XXIII. The first subset focuses on *cross_GPU_evaluation* and contains 10,696 traces collected from five NVIDIA GPUs under a measurement setting at 1 m. It covers representative CNN, LSTM, and Transformer inference workloads, introducing diversity in both GPU hardware and neural-network computation. This subset therefore enables the evaluation of whether architecture-dependent characteristics remain observable across different GPU platforms rather than being specific to an individual device. The second subset focuses on *distance_evaluation* and contains 6,946 traces collected from an RTX 3060 Ti in an open environment. The measurement distance ranges from 0 to 7 m, with mixed DNN inference workloads executed across these settings. By explicitly varying the transmitter-to-receiver distance, this subset captures the progressive degradation of remotely observable leakage characteristics caused by propagation loss and provides data for examining the practical distance boundary of GPU-based FEM-SCAs. The third sub-

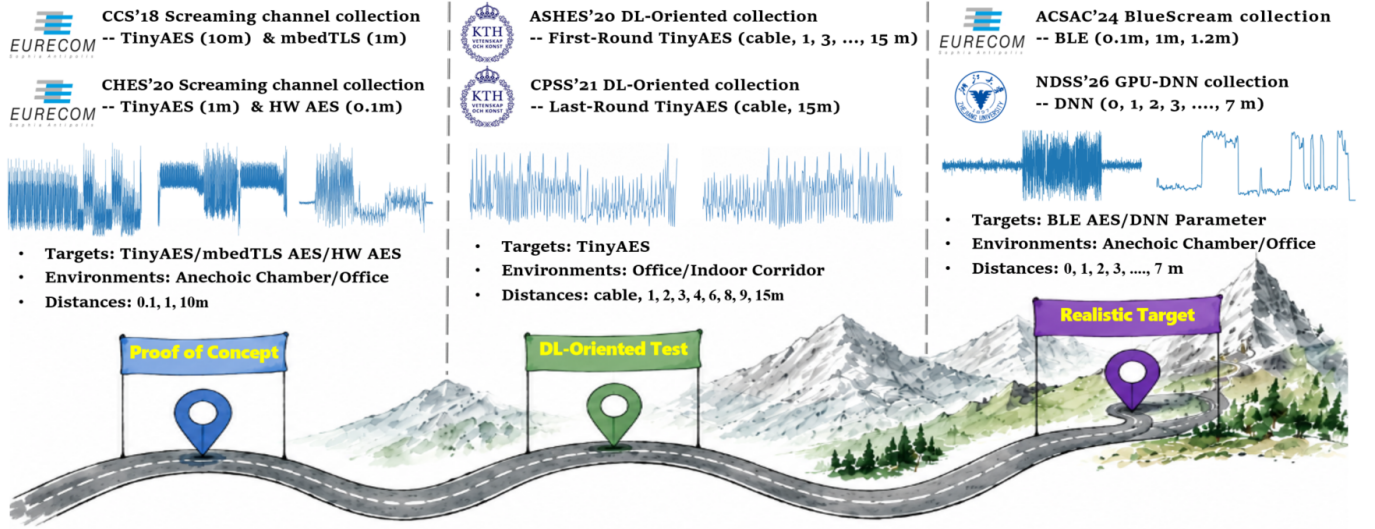


Fig. 15: An overview of the screaming channel public data collection evolution.

set considers `cross_wall_evaluation`, containing 2,421 traces collected from an RTX 3060 Ti with concrete, glass, and wood walls introduced between the victim and receiver. Similar to the distance subset, these measurements contain mixed DNN inference executions and retain a uniform trace length of 5,023 samples. The inclusion of different wall materials extends the collection beyond conventional line-of-sight measurements and provides representative data for studying whether architecture-dependent leakage remains observable through common physical obstacles.

Overall, the major distinction of the NDSS'26 GPU-DNN collection from previous FEM-SCA data collections lies in the shift of the leakage target from cryptographic implementations to high-level DNN architecture information.

The public FEM-SCA data collections can be understood as a staged route from proof-of-concept leakage discovery, to deep-learning-oriented attack evaluation, and finally to more realistic wireless-protocol targets. As summarized in Fig. 15, the first stage is represented by the CCS'18 and CHES'20 screaming-channel collections released by the EURECOM group [23], [24]. These collections establish the basic feasibility and physical understanding of RF-mediated AES leakage on mixed-signal Bluetooth SoCs, covering TinyAES, mbedTLS AES, and hardware AES settings under anechoic-chamber and office environments, with representative distances including 0.1 m, 1 m, and 10 m. Their main role is therefore proof of concept: they show that cryptographic computation can unintentionally modulate the RF carrier and become observable in the far field, while also providing early traces for leakage localization, frequency comparison, implementation comparison, and basic profiled attacks.

The second stage is represented by the ASHES'20 and CPSS'21 DL-oriented collections from KTH [38], [85], which shift the emphasis from demonstrating the existence of leakage to evaluating whether data-driven models can exploit such leakage. Both collections focus on TinyAES running on nRF52-class Bluetooth targets, but they organize the traces for different learning objectives: the ASHES'20 collection

targets first-round AES leakage and provides traces captured across cable and gradually increasing over-the-air distances, whereas the CPSS'21 collection focuses on last-round AES leakage, using cable traces for profiling and 15 m far-field traces for testing. These collections are therefore especially useful for studying DL-based attacks, model transferability, distance-induced distribution shifts, and the difference between first-round and last-round recovery assumptions.

The third stage is represented by the ACSAC'24 BlueScream collection [80] and the NDSS'26 GPU-DNN collection [121], move beyond cryptographic implementation toward more realistic and diverse targets. Instead of only evaluating standalone AES firmware, BlueScream captures leakage from BLE re-keying AES executions. This makes it a more realistic target collection, suitable for studying whether screaming-channel attacks can be applied to protocol-level wireless activity where the attacker must interact with BLE communication rather than directly controlling a dedicated cryptographic benchmark. The GPU-DNN collection further extends the scope beyond cryptographic implementations by capturing far-field EM leakage from DNN inference on five GPU models. Together, these publically available screaming channel data collections mark a broader transition of FEM-SCA research from controlled cryptographic benchmarks toward complex, system-level applications.

Therefore, the six public data collections do not form a uniform benchmark suite, but rather a chronological experimental roadmap: CCS'18 and CHES'20 collections provide the proof-of-concept and mechanism-understanding foundation, ASHES'20 and CPSS'21 collections provide deep-learning-oriented trace resources for attack-model evaluation, and ACSAC'24 BlueScream and NDSS'26 GPU-DNN collections extend public FEM-SCA traces toward practical attack targets.

VIII. DISCUSSION: HOW TO DEAL WITH THE RADIO

The preceding sections have traced the development of FEM-SCA from the discovery and physical understanding of

screaming-channel leakage, through enhanced attack methodologies and target variants, to the emergence of public trace collections. Across these studies, a consistent pattern has emerged: improvements in one dimension often expose constraints in another, such as longer attack distance requiring more traces, stronger models depending on narrower target assumptions, or more realistic protocol scenarios leading to lower attack efficiency. This section distills the discussion into one key trade-off, three major limitations, and three future research roadmaps for FEM-SCAs.

A. Key Trade-Off: Attack Efficiency vs. Distance

The key trade-off in FEM-SCA lies between remote attack capability and attack efficiency. Once screaming-channel attacks acquire the ability to exploit leakage from the far field, the most direct cost is a substantial reduction in attack efficiency compared with conventional power analysis and near-field EM attacks. However, this longer-range capability is obtained by inserting an additional physical path between the sensitive computation and the measurement device. In power analysis, the leakage is measured from the power consumption caused directly by data-dependent switching activity. In near-field EM analysis, the leakage is captured from localized electromagnetic radiation near the circuit or PCB. In FEM-SCA, by contrast, the digital leakage must first couple into the analog/RF transmission chain, modulate or distort the radio signal, propagate through space, and then be captured by the receiving antenna. Each step makes the leakage more accessible from a distance, but also weakens, mixes, and distorts the key-dependent information. Therefore, the far-field nature of FEM-SCA is not a free improvement over traditional SCAs. It expands the attack surface spatially, but sharply reduces the signal quality available for statistical or learning-based exploitation.

This loss of efficiency can be observed by comparing FEM-SCA with conventional side-channel attacks on similar cryptographic targets. For unprotected AES implementations on ARM-class microcontrollers, relatively direct deep-learning-based power-analysis attacks can recover the full key with fewer than ten traces in some reported settings [138], [139], because the power trace contains strong and temporally localized data-dependent leakage. In a screaming-channel setting, the same type of sensitive operation is no longer observed at the leakage source. Instead, the attacker observes an RF waveform in which the useful leakage has been coupled into a much stronger communication signal and contaminated by channel effects, receiver noise, and unrelated radio activity. Consequently, even when the victim device is placed at a very short distance from the receiver, FEM-SCA typically requires far more measurements, such as several hundreds traces to recover a subkey [85].

This difference is not merely due to immature attack algorithms. It reflects a basic physical constraint: the coupling that makes the leakage radiate also reduces its amplitude, separability, and stability. The attack model must therefore learn from features that are weaker, less repeatable, and more entangled with the RF carrier and environment.

The second layer of this trade-off appears when the attack distance increases. As the receiver moves farther away from the victim device, the RF signal suffers from path loss, environmental attenuation, multipath propagation, misalignment, and interference from other transmitters. These effects reduce the effective signal-to-noise ratio of the leakage component, even when the radio communication signal itself can still be received. This distinction is important: a receiver may be able to observe the radio transmission, but the side-channel component embedded in that transmission can still be too weak for key recovery or even segment alignment. Therefore, increasing the attack distance usually forces the adversary to compensate in other ways. They may need to collect more traces, average repeated encryptions, use a higher-gain directional antenna, add low-noise amplifiers, profile on cleaner cable traces, exploit multiple receiving channels, or train more complex neural networks. Each compensation increases the cost of the attack. For example, repeated encryption improves the averaged leakage quality, but it requires the attacker to observe many same cryptographic executions, which is highly impractical in most scenarios.

However, the relationship between distance and attack efficiency should not be described as a simple linear or exponential decay. RF propagation is spatially irregular. Reflections from walls, floors, objects, furniture, and human bodies can create constructive and destructive interference. As a result, the received signal strength and the leakage strength may fluctuate across positions. In some environments, a point farther away from the victim may receive a stronger RF component than a closer point because it lies near a constructive multipath region. Conversely, a nearby receiver may suffer from fading or poor antenna orientation. This means that attack efficiency may decrease in a spiral-like or non-monotonic manner: the overall trend worsens as distance increases, but local conditions can temporarily improve or degrade the leakage. Such behavior also explains why distance alone is insufficient to characterize an FEM-SCA experiment. The same distance can correspond to very different attack difficulties depending on the room geometry, antenna placement, obstacles, receiver orientation, carrier frequency, and radio traffic.

This non-monotonicity makes trace collection itself a core technical challenge in FEM-SCA. In traditional power analysis, once the probe is connected and the trigger is stable, collecting thousands of traces is usually straightforward. In FEM-SCA, each trace depends not only on cryptographic execution, but also on the wireless transmission state, RF channel condition, synchronization quality, and environmental stability. The attacker may need to wait for suitable protocol events, trigger repeated pairing or encryption operations, align traces captured through noisy RF reception, and discard corrupted measurements. If the victim uses frequency hopping, packet scheduling, or variable radio activity, trace acquisition becomes extremely harder. Collecting hundreds or thousands of usable traces from a remote victim may require prolonged observation and carefully positioned equipment, all of which affect practicality.

From our perspective, this trade-off should become a central evaluation principle for future FEM-SCA studies. Reporting

only that an attack succeeds at a certain distance can be misleading, because distance does not capture the full cost of the attack. Similarly, reporting only the number of traces can hide the fact that these traces may require a large set of captured but not involved data [92]. A more meaningful evaluation should jointly report attack distance, number of attack traces, number of captures to get a useful trace, quantitative environmental conditions, and synchronization effort. Only by considering these dimensions together can the field distinguish between attacks that are technically feasible under strong laboratory assumptions and attacks that represent practical remote threats.

B. Key Limitations

Although recent FEM-SCA studies have made clear progress in attack distance, trace efficiency, modeling capability, and protocol awareness, the field is still shaped by several structural limitations. These limitations do not invalidate existing results, but they define the boundary of what can currently be concluded from the literature. In particular, the evidence base remains concentrated on a narrow set of platforms, a narrow set of wireless technologies, and a fragmented set of public trace releases. These issues make it difficult to assess whether FEM-SCA is a broadly generalizable threat to mixed-signal wireless devices or a set of strong but platform-dependent demonstrations.

1) *Limited platform generality*: The most visible limitation of existing FEM-SCA research is its concentration on the Nordic nRF52 family [23], [24], [38], [85], [99]. On the one hand, it makes results easier to compare across papers, supports the reuse of public traces, and provides a stable reference platform for studying the coupling between digital execution and the RF transmission chain. In this sense, nRF52 has played a similar role to a benchmark device for early-stage FEM-SCA research. However, the same concentration also limits the external validity of the field. FEM-SCA leakage is not determined only by the cryptographic algorithm or the software implementation. It is produced by a cross-layer physical path involving the processor, memory bus, clock tree, power distribution network, analog/RF front-end, PCB layout, antenna path, firmware scheduling, and radio transmission behavior. Changing any of these layers may alter the strength, stability, and frequency-domain structure of the leakage. Evidence from attacks on masked AES, hardware AES accelerators, and BLE protocol-level implementations already suggests that a change in target implementation or execution context can significantly reduce attack efficiency [26], [115], [118]. Therefore, a model or acquisition strategy that works well on one nRF52 board cannot be assumed to transfer directly to other wireless SoCs, even if they execute the same cryptographic primitive. Our view is that the next stage of FEM-SCA research should treat cross-platform validation as a core requirement rather than an optional extension. Without this step, current conclusions about FEM-SCA practicality will remain persuasive for a well-studied device family, but uncertain for the broader range of embedded wireless systems.

2) *Bluetooth-centric evidence*: The second limitation is that the quantitative evidence for FEM-SCA is still overwhelmingly Bluetooth-centric. The foundational screaming-channel

studies exploit leakage coupled into Bluetooth transmissions, and the major public data collections also mainly rely on Bluetooth-related acquisition settings [23], [24], [38], [80], [85]. Nevertheless, the dominance of Bluetooth leaves the broader radio landscape underexplored. WiFi and Zigbee have different carrier structures, bandwidths, modulation schemes, packet durations, channel-access mechanisms, and baseband processing pipelines. These differences may change not only how leakage is coupled into the RF signal, but also how traces should be synchronized, filtered, segmented, and modeled. Some works have suggested that digital activity from embedded components can be unintentionally picked up and radiated by wireless front-ends beyond a single cryptographic benchmark [23], [37]. However, compared with Bluetooth, there is still a lack of systematic quantitative evidence for WiFi- or Zigbee-based FEM-SCA, especially in terms of key-recovery success rate, trace complexity, attack distance, profiling requirement, and robustness under realistic conditions.

Our view is other radio channels such as WiFi and Zigbee should not be treated as simple extensions of Bluetooth-based FEM-SCA. A receiver-frequency change alone is unlikely to capture the full difference between radio technologies. Instead, each wireless protocol should be studied as a distinct leakage environment with its own modulation, timing, and interference structure. Such evidence is necessary before FEM-SCA can be described as a general RF-mediated side-channel threat rather than a threat currently supported mainly by Bluetooth experiments.

C. Lack of structural data benchmark

The third limitation is the absence of a structured FEM-SCA benchmark that covers diverse attack conditions under the same experimental setting. Existing public data collections are valuable, but they were built for different purposes and with different acquisition assumptions. The CCS'18 and the CHES'20 collection mainly supports the proof-of-concept demonstration of screaming-channel leakage [23], [24], the ASHES'20 and CPSS'21 collections support deep-learning-based evaluation on first-round and last-round TinyAES leakage [38], [85], and the ACSAC'24 BlueScream collection moves toward BLE protocol-level leakage [80]. Together, these resources provide an important empirical basis for the field, but they do not form a unified benchmark in which different algorithms, platforms, distances, environments, and obstacles are evaluated under a consistent experimental configuration. This limitation makes cross-paper and cross-method comparison difficult. More importantly, they do not provide a controlled matrix of variables. For example, the field still lacks a public benchmark that measures multiple cryptographic algorithms, multiple wireless SoCs, multiple distances, different indoor and outdoor environments, and different obstacle conditions while keeping the receiver, antenna, sampling rate, synchronization method, firmware design, and data-format standard consistent. Without such a benchmark, it is difficult to determine whether a reported improvement comes from a genuinely better attack method or from a more favorable acquisition condition. A model that appears more efficient on

one collection may simply benefit from less environmental distortion and better trace alignment.

Our view is that the field needs a structural FEM-SCA benchmark designed around controlled comparison rather than isolated reproduction. Such a benchmark should include a systematic experimental grid covering different cryptographic target, attack distances, environments, and obstacle conditions under a unified acquisition setup. In this sense, the lack of a structural benchmark is not merely a data-sharing problem. It is a methodological bottleneck that limits the maturity and comparability of FEM-SCA research.

D. Future Roadmaps

The limitations discussed above suggest that the next stage of FEM-SCA research should not focus only on improving attack success rates under already familiar settings. We outline three research roadmaps that may help the field move from isolated demonstrations toward mature security evaluation.

1) *Countermeasure*: The first roadmap is the systematic design and evaluation of countermeasures. Although existing FEM-SCA works have mainly focused on attack construction, the demonstrated leakage mechanism already suggests the need for protection in security-critical wireless devices. Since FEM-SCA is generated through the coupling between digital computation and the analog/RF transmission chain, countermeasures should not be limited to traditional cryptographic masking or hiding [140]. The design of effective countermeasures against side-channel attacks generally follows two core principles [141]: (1) to degenerate the statistical relationship between the secret data and the physical leakage, and (2) to increase the effort for an adversary to capture exploitable traces. Applying these principles specifically to the screaming channel attack, we can conceptualize countermeasure development roadmaps operating at three different levels.

Algorithmic Level. The focus is on modifying the cryptographic computation itself to degenerate or to remove the data-dependency of the leakage. This approach directly addresses the first principle by breaking the statistical link between secrets and emanations. The most prominent technique is masking [142], [143], which splits every sensitive variable into multiple random shares. The computation is then performed on these shares, ensuring that the EM emanation at any given moment is correlated to a random value rather than the actual secret. For a screaming channel attack, which relies on identifying distinct EM signatures corresponding to specific data values, effective masking renders the EM radiation profile statistically random, thereby removing the exploitable signal an adversary seeks.

Implementation Level. In this direction, countermeasure design aims to change the device's operation in traces to disrupt trace alignment and analysis. These methods primarily serve the second principle, significantly increasing the number of traces an adversary must collect and the complexity of processing them. Techniques such as introducing clock jitter [144], [145], duplicating the cryptographic execution [146], [147], or inserting dummy operations create desynchronization between the device's internal state and the measured side-

channel traces [148], [149]. While the fundamental data-dependent leakage may still exist, this desynchronization prevents an attacker from perfectly aligning thousands of traces. Consequently, the SNR of the leaked signal remains low, substantially increasing the number of measurements required for successful side-channel analysis [150] and often impractical for remote attacks where trace quality is already limited.

Physical Level. This class of countermeasure directly embodies the second principle by increasing the adversary's effort. A highly effective strategy is to actively introduce interference to pollute the electromagnetic spectrum, as tested in [92]. Beyond the power consuming active interference sources, shielding, which involves enclosing the device or its sensitive components within a conductive cage, is another primary potential way to go to against screaming channel attacks. It has been shown that different types of covers can provide varying levels of shielding effectiveness against near-field EM leakage [151]–[153]. When it comes to the screaming channel attack case, a significant challenge for designers is the inherent trade-off between side-channel resistance and the device's intended RF communication performance, as a shield that blocks leakage can also degrade legitimate wireless signals [154].

2) *Different Attack Targets and RF Protocols*: The second roadmap is to expand FEM-SCA research to different attack targets and RF protocols. Future studies should evaluate different boards, SoC vendors, PCB layouts, and cryptographic implementations. This includes not only software cryptographic implementations, but also hardware accelerators, masked implementations, post-quantum cryptographic primitives, authenticated encryption, and protocol-level security operations. At the same time, FEM-SCA should move beyond Bluetooth-enabled SoCs and examine WiFi, Zigbee, and other wireless protocols. Different protocols employ distinct RF architectures, operating frequencies, modulation schemes, and transmission behaviors, which may significantly affect the coupling and propagation of secret-dependent leakage. Future studies should therefore investigate whether exploitable leakage can be consistently observed across these protocols and, more importantly, demonstrate their practical vulnerability through quantitative key-recovery results under realistic remote attack settings. Cross-target and cross-protocol studies are essential for determining whether FEM-SCA is a general attack class or a threat that is currently concentrated on several favorable platforms and cryptos. The field needs comparative experiments where different targets and protocols are evaluated under consistent acquisition and reporting standards.

3) *Boundary Analysis and Modeling*: The third roadmap is boundary analysis and modeling. Existing studies have shown that FEM-SCA can work under certain distances, environments, and target assumptions, but the field still lacks a clear model of where the attack becomes infeasible. Future work should therefore characterize the boundary conditions of FEM-SCA, including maximum useful distance, minimum required leakage strength, tolerable interference level, required number of repetitions, antenna placement sensitivity, obstacle effects, and protocol-triggering constraints. This requires both

empirical measurement and theoretical modeling. Empirical measurements can map where leakage remains distinguishable and where it collapses into noise, while analytical models can relate RF propagation and digital-to-RF coupling to side-channel success indicators such as key rank or classification confidence. Such modeling would make FEM-SCA evaluation more predictive. Instead of only reporting that an attack succeeds in one setting, researchers could estimate the conditions under which the same attack is likely to remain effective. This would also help defenders identify high-risk deployment scenarios and design meaningful security tests for wireless embedded devices.

IX. CONCLUSION

*"Now I'm fine, so when the songs are playing loud on the radio, I'm over that
dum dum dadadada dum..."*

This paper provides the first systematic view of screaming channel attacks, or called FEM-SCAs, as a distinct class of radio-coupling-based remote side-channel attacks. By organizing existing studies around leakage understanding, attack enhancement, target variants, and public data collections, we establish a coherent picture of how this research area has evolved since the first demonstration of the screaming-channel phenomenon. The reviewed works show that FEM-SCA is no longer only a lab curiosity: sensitive computation can be carried by ordinary RF transmissions and recovered at a distance under certain conditions. Early studies primarily focused on establishing the existence and physical origin of secret-dependent leakage unintentionally coupled into legitimate RF transmissions, whereas subsequent research progressively improved attack efficiency, robustness, and operating distance. More recent efforts have further explored different implementation settings and increasingly realistic wireless environments, gradually shifting FEM-SCA research from proof-of-concept demonstrations toward practical remote attack scenarios. These developments establish FEM-SCA as an important extension of conventional side-channel analysis and highlight a previously underestimated attack surface in RF-enabled embedded and IoT systems.

At the same time, the available evidence also defines a clear boundary for the current state of FEM-SCA research. Existing attacks still face an efficiency–distance trade-off, as increasing the measurement distance typically weakens the exploitable leakage and substantially increases the effort required for successful analysis. Moreover, current studies remain largely concentrated on Bluetooth-enabled platforms, while the feasibility and characteristics of such leakage under other RF protocols and device architectures have received only limited investigation. Although several public datasets have been released to improve reproducibility, they are generally collected under different experimental conditions and therefore do not yet constitute a structured benchmark with unified acquisition settings and evaluation criteria. This lack of standardized evaluation makes direct and fair comparison between existing attacks challenging and leaves uncertainty about whether techniques demonstrated under specific experimental setups can generalize to different cases. Addressing

these limitations is therefore essential for moving FEM-SCA research from isolated demonstrations toward systematic and practically relevant security evaluation.

Future FEM-SCA research therefore needs to become more comparative, more cross-platform, and more countermeasure-aware. Progress should be measured not only by whether an attack succeeds, but also by the cost, assumptions, distance, environment, and target conditions under which it succeeds. A mature understanding of screaming channel leakage may require both stronger attacks and clearer failure boundaries.

REFERENCES

- [1] Y. Li, Y. Guo, T. Gu, and C. Ge, "On exploiting single-trace side-channel leakage of SEAL-embedded library," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 21, pp. 5388–5399, 2026.
- [2] A. Liu, A. Wang, J. Liu, Y. Ding, J. Zhang, Z. Liu, and L. Zhu, "Mask leakage independence: A collision-based profiled approach for side-channel analysis on cryptosystems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, p. Early Access, 2026.
- [3] T. Tosun and E. Savas, "Zero-value filtering for accelerating non-profiled side-channel attack on incomplete NTT based implementations of lattice-based cryptography," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2024.
- [4] H.-Z. Xie and T. Su, "Power side-channel security of spiking neural networks: Attacks, analysis, and low-overhead defenses," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2026.
- [5] Y. Gao, H. Qiu, Z. Zhang, B. Wang, H. Ma, A. Abuadbbba, M. Xue, A. Fu, and S. Nepal, "Deeptheft: Stealing dnn model architectures through power side channel," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024, pp. 3311–3326.
- [6] L. Batina, S. Bhasin, D. Jap, and S. Picek, "CSI NN: Reverse engineering of neural network architectures through electromagnetic side channel," in *USENIX Security Symposium (USENIX Security)*, 2019, pp. 515–532.
- [7] A. Moradi and T. Schneider, "Improved side-channel analysis attacks on xilinx bitstream encryption of 5, 6, and 7 series," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2016, pp. 71–87.
- [8] Q. Yang, P. Gasti, K. Balagani, Y. Li, and G. Zhou, "Usb side-channel attack on tor," *Computer Networks*, vol. 141, pp. 57–66, 2018.
- [9] Q. Yang, P. Gasti, G. Zhou, A. Farajidavar, and K. S. Balagani, "On inferring browsing activity on smartphones via USB power analysis side-channel," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 12, no. 5, pp. 1056–1066, 2016.
- [10] Y. Yu, M. Moraitis, and E. Dubrova, "Why deep learning makes it difficult to keep secrets in FPGAs," in *2020 Workshop in Dynamic and Novel Advances in Machine Learning and Intelligent Cyber Security*, 2020, pp. 1–9.
- [11] D. He, H. Wang, T. Deng, J. Liu, and J. Wang, "Improving IIoT security: Unveiling threats through advanced side-channel analysis," *Computers & Security*, p. 104135, 2024.
- [12] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, and Q. Xu, "On code execution tracking via power side-channel," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2016, pp. 1019–1031.
- [13] J. Hu, H. Wang, T. Zheng, J. Hu, Z. Chen, H. Jiang, and J. Luo, "Password-stealing without hacking: Wi-fi enabled practical keystroke eavesdropping," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2023, pp. 239–252.
- [14] M. Cardaioli, M. Conti, K. Balagani, and P. Gasti, "Your pin sounds good! augmentation of pin guessing strategies via audio leakage," in *European Symposium on Research in Computer Security (ESORICS)*. Springer, 2020, pp. 720–735.
- [15] T. Ni, X. Zhang, and Q. Zhao, "Recovering fingerprints from in-display fingerprint sensors via electromagnetic side channel," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2023, pp. 253–267.
- [16] C. Luo, Z. Xie, Y. Huang, G. Chen, H. Yao, J. Zhang, L. Cheng, W. Xu, and J. Li, "Laserkey: Eavesdropping keyboard typing leveraging vibrational emanations via laser sensing," *IEEE Transactions on Mobile Computing*, vol. 24, no. 6, pp. 4829–4844, 2025.

- [17] C. Gu, Y. Zhang, and N. Abu-Ghazaleh, "I know what you sync: Covert and side channel attacks on file systems via syncfs," in *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2025, pp. 3636–3652.
- [18] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*. Springer, 1999, pp. 388–397.
- [19] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.
- [20] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel (s)," in *International workshop on cryptographic hardware and embedded systems (CHES)*. Springer, 2002, pp. 29–45.
- [21] B. Nassi, O. Vayner, E. Iluz, D. Nassi, J. Jancar, D. Genkin, E. Tromer, B. Zadov, and Y. Elovici, "Optical cryptanalysis: Recovering cryptographic keys from power led light fluctuations," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2023, pp. 268–280.
- [22] D. Genkin, A. Shamir, and E. Tromer, "Acoustic cryptanalysis," *Journal of Cryptology*, vol. 30, no. 2, pp. 392–443, 2017.
- [23] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018, pp. 163–177.
- [24] G. Camurati, A. Francillon, and F.-X. Standaert, "Understanding screaming channels: From a detailed analysis to improved attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, pp. 358–401, 2020.
- [25] M. Guri, "Air-gap electromagnetic covert channel," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 2127–2144, 2023.
- [26] H. Wang, "Amplitude-modulated EM side-channel attack on provably secure masked AES," *Journal of Cryptographic Engineering*, pp. 1–13, 2024.
- [27] B. Hettwer, S. Gehrler, and T. Güneysu, "Applications of machine learning techniques in side-channel attacks: a survey," *Journal of Cryptographic Engineering*, vol. 10, no. 2, pp. 135–162, 2020.
- [28] C. Shepherd, K. Markantonakis, N. Van Heijningen, D. Aboulkassimi, C. Gaine, T. Heckmann, and D. Naccache, "Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis," *Computers & Security*, vol. 111, p. 102471, 2021.
- [29] S. Picek, G. Perin, L. Mariot, L. Wu, and L. Batina, "Sok: Deep learning-based physical side-channel analysis," *ACM Computing Surveys (CSUR)*, vol. 55, no. 11, pp. 1–35, 2023.
- [30] J. Zhang, C. Chen, J. Cui, and K. Li, "Timing side-channel attacks and countermeasures in CPU microarchitectures," *ACM Computing Surveys (CSUR)*, vol. 56, no. 7, pp. 1–40, 2024.
- [31] P. Dobias, A. Rezaeezade, Ł. Chmielewski, L. Malina, and L. Batina, "SoK: Reassessing Side-Channel Vulnerabilities and Countermeasures in PQC Implementations," *Cryptology ePrint Archive*, 2025.
- [32] J. Kim, H. Jang, and Y. Shin, "A survey of side-channel attacks on branch prediction units," *ACM Computing Surveys*, vol. 57, no. 11, pp. 1–36, 2025.
- [33] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.
- [34] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2002, pp. 13–28.
- [35] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International workshop on cryptographic hardware and embedded systems (CHES)*. Springer, 2004, pp. 16–29.
- [36] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi *et al.*, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, 2011, pp. 115–136.
- [37] D. Lei, S. Wang, M. You, and X. Jiuba, "A review of security analysis technologies for screaming channel based on rfoc," in *2026 IEEE 5th International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, vol. 5. IEEE, 2026, pp. 1–11.
- [38] R. Wang, H. Wang, and E. Dubrova, "Far field EM side-channel attack on AES using deep learning," in *Proceedings of the ACM Workshop on Attacks and Solutions in Hardware Security (ASHES)*, 2020, pp. 35–44.
- [39] L. Keyi, "Far field EM side-channel attack based on deep learning with automated hyperparameter tuning," Master's thesis, KTH Royal Institute of Technology, 2021.
- [40] G. Evensen, "An efficiency evaluation of far-field electromagnetic deep learning side-channel attacks in controlled environments," Master's thesis, Uppsala University, 2022.
- [41] Y. Ibrahim, "Far-field electromagnetic side-channel analysis in noisy environments," Master's thesis, The University of New South Wales, 2025.
- [42] J. Choi, H.-Y. Yang, and D.-H. Cho, "Tempest comeback: A realistic audio eavesdropping threat on mixed-signal SoCs," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2020, pp. 1085–1101.
- [43] S. Fernández, E. Martínez, J. Varela, P. Musé, and F. Larroca, "Deep-TEMPEST: Using deep learning to eavesdrop on HDMI from its unintended electromagnetic emanations," in *Proceedings of the Latin-American Symposium on Dependable and Secure Computing*, 2024, pp. 91–100.
- [44] W. Li, J. Wang, G. Zhang, Y. Yang, R. Spolaor, X. Cheng, and P. Hu, "EMIRIS: Eavesdropping on iris information via electromagnetic side channel," in *The Network and Distributed System Security Symposium (NDSS)*, 2025.
- [45] P. Horvath, I. Shumailov, L. Chmielewski, L. Batina, and Y. Yarom, "Kraken: Higher-order EM side-channel attacks on DNNs in near and far field," *arXiv preprint arXiv:2603.02891*, 2026.
- [46] P. Wang, S. Nagaraja, A. Bourquard, H. Gao, and J. Yan, "SoK: Acoustic side channels," *ACM Computing Surveys*, vol. 58, no. 7, pp. 1–33, 2026.
- [47] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure integrated circuits and systems*. Springer, 2009, pp. 27–42.
- [48] H. Wang, M. Brisfors, S. Forsmark, and E. Dubrova, "How diversity affects deep-learning side-channel attacks," in *IEEE Nordic Circuits and Systems Conference (NORCAS)*. IEEE, 2019, pp. 1–7.
- [49] B. Timon, "Non-profiled deep learning-based side-channel attacks with sensitivity analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, pp. 107–131, 2019.
- [50] N.-T. Do, V.-P. Hoang, and V. S. Doan, "A novel non-profiled side channel attack based on multi-output regression neural network," *Journal of Cryptographic Engineering (JCEN)*, vol. 14, no. 3, pp. 427–439, 2024.
- [51] K. Ngo, R. Wang, and E. Dubrova, "Higher-order boolean masking does not prevent side-channel attacks on LWE/LWR-based PKE/KEMs," in *International Symposium on Multiple-Valued Logic (ISMVL)*, 2023, pp. 190–195.
- [52] C. Xiao, M. Tang, S. Karayalcin, and W. Cheng, "LD-PA: Distilling univariate leakage for deep learning-based profiling attacks," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 20, pp. 17 – 30, 2024.
- [53] F. Hu, J. Shen, H. Ma, and Q. J. Wu, "Cross-attention for aes mode variation in side-channel analysis," in *2025 62nd ACM/IEEE Design Automation Conference (DAC)*. IEEE, 2025, pp. 1–7.
- [54] S. Karayalcin, M. Krček, L. Wu, S. Picek, and G. Perin, "It's a kind of magic: a novel conditional GAN framework for efficient profiling side-channel analysis," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2024, pp. 99–131.
- [55] J. Long, C. Ou, Y. Cheng, T. Wang, Z. Wang, and F. Zhang, "The mysteries of LRA: Roots and progress in side-channel applications," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 8978 – 8993, 2025.
- [56] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, and S. Sen, "X-DeepSCA: Cross-device deep learning side channel attack," in *Proceedings of the 56th Annual Design Automation Conference (DAC)*, 2019, pp. 1–6.
- [57] S. Hajra, M. Alam, S. Saha, S. Picek, and D. Mukhopadhyay, "On the instability of softmax attention-based deep learning models in SCA," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2023.
- [58] M. Staib and A. Moradi, "Deep learning side-channel collision attack," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, pp. 422–444, 2023.
- [59] L. Wu, G. Perin, and S. Picek, "Weakly profiling side-channel analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHSE)*, vol. 2024, no. 3, pp. 707–730, 2024.
- [60] J. Xi and C. Fan, "Multi-byte side-channel attacks on chaotic block cipher: Autoencoder-based feature selection and CNN-Transformer collaborative attack framework," *Chaos, Solitons & Fractals*, vol. 200, p. 117097, 2025.
- [61] Y. Chen, B. Wang, C. Su, A. Li, Y. Tang, and G. Li, "Enhancing model generalization for efficient cross-device side-channel analysis," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 10 114 – 10 129, 2025.

- [62] W. Zhou, A. Wang, Y. Ding, A. Liu, J. Zhang, J. Li, and L. Zhu, "SCA-GPT: A generation-planning-tool assisted LLM agent for fully automated side-channel analysis on cryptosystems," *Cryptology ePrint Archive*, 2025.
- [63] Z. Li, A. Liu, A. Wang, and W. Wang, "Chatgpt as preprocessing agents: A case study on cryptographic side-channel analysis," in *International Conference on Applied Cryptography and Network Security*. Springer, 2025, pp. 193–210.
- [64] E. Cagli, C. Dumas, and E. Prouff, "Convolutional neural networks with data augmentation against jitter-based countermeasures," in *International Conference on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2017, pp. 45–68.
- [65] J. Rijdsdijk, L. Wu, G. Perin, and S. Picek, "Reinforcement learning for hyperparameter tuning in deep learning-based side-channel analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, pp. 677–707, 2021.
- [66] L. Wu, G. Perin, and S. Picek, "The best of two worlds: Deep learning-assisted template attack," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, pp. 413–437, 2022.
- [67] Y. Ji, R. Wang, K. Ngo, E. Dubrova, and L. Backlund, "A side-channel attack on a hardware implementation of crystals-kyber," in *IEEE European Test Symposium (ETS)*. IEEE, 2023, pp. 1–5.
- [68] G. Zaid, L. Bossuet, M. Carbone, A. Habrard, and A. Venelli, "Conditional variational autoencoder based on stochastic attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, pp. 310–357, 2023.
- [69] Y. Yang, C. Ou, Y. Wei, W. Li, Y. Fan, and X. Shen, "Broader but more efficient: Broad learning in power side-channel attacks," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2024, pp. 1528–1533.
- [70] C. P. Chen and Z. Liu, "Broad learning system: An effective and efficient incremental learning system without the need for deep architecture," *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)*, vol. 29, no. 1, pp. 10–24, 2017.
- [71] A. Rezaeizade, T. Yap, D. Jap, S. Bhasin, and S. Picek, "Breaking the blindfold: deep learning-based blind side-channel analysis," in *Proceedings of the USENIX Conference on Security Symposium*. USENIX, 2025, p. 20.
- [72] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "ACE: Adaptive channel estimation for detecting analog/RF trojans in WLAN transceivers," in *2017 IEEE/ACM International Conference on Computer-Aided Design*. IEEE, 2017, pp. 722–727.
- [73] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Amplitude-modulating analog/RF hardware Trojans in wireless networks: Risks and remedies," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 15, pp. 3497–3510, 2020.
- [74] R. M. Secareanu, S. Warner, S. Seabridge, C. Burke, T. E. Watrobski, C. Morton, W. Staub, T. Teulier, and E. Friendman, "Physical design to improve the noise immunity of digital circuits in a mixed-signal smart-power system," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, vol. 4. IEEE, 2000, pp. 277–280.
- [75] D. R. Gnad, J. Krautter, and M. B. Tahoori, "Leaky noise: New side-channel attack vectors in mixed-signal iot devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 305–339, 2019.
- [76] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2015, pp. 207–228.
- [77] Z. Huang, H. Wang, B. Cao, D. He, and J. Wang, "A comprehensive side-channel leakage assessment of CRYSTALS-Kyber in IIoT," *Internet of Things*, vol. 27, p. 101331, 2024.
- [78] M. Ettus and M. Braun, "The universal software radio peripheral (USRP) family of low-cost SDRs," *Opportunistic spectrum sharing and white space access: The practical reality*, pp. 3–23, 2015.
- [79] "Small portable aes128/192/256 in C," Github, 2013, <https://github.com/kokke/tiny-AES-c/>.
- [80] P. Ayoub, R. Cayre, A. Francillon, and C. Maurice, "Bluescream: Screaming channels on Bluetooth low energy," in *2024 Annual Computer Security Applications Conference (ACSAC)*. IEEE, 2024, pp. 636–649.
- [81] H. Wang, "Deep learning side-channel attacks on advanced encryption standard," Ph.D. dissertation, KTH Royal Institute of Technology, 2023.
- [82] M. Nomura, D. Miyahara, Y. Li, and K. Sakiyama, "A case study of side-channel authentication using screaming channel," in *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*. IEEE, 2024, pp. 488–489.
- [83] P. Cao, C. Zhang, X.-J. Lu, H.-N. Lu, and D.-W. Gu, "Side-channel analysis for the re-keying protocol of bluetooth low energy," *Journal of Computer Science and Technology*, vol. 38, no. 5, pp. 1132–1148, 2023.
- [84] M. Collotta, G. Pau, T. Talty, and O. K. Tonguz, "Bluetooth 5: A concrete step forward toward the IoT," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 125–131, 2018.
- [85] R. Wang, H. Wang, E. Dubrova, and M. Brisfors, "Advanced far field EM side-channel attack on AES," in *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop (CPSS)*, 2021, pp. 29–39.
- [86] A. Zedigh, "Improving deep learning assisted far-field electromagnetic sidechannel attacks on AES," Master's thesis, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, 2022.
- [87] Z. Hong-Yi, G. Da-Wu, Z. Chi, L. Yan, and Y. Yi-Dong, "Wireless side-channel analysis method based on repeater (in Chinese)," *Journal of Cryptologic Research*, vol. 9, no. 1, pp. 175–188, 2022.
- [88] Z. Hong-Yi, G. Da-Wu, C. Pei, Q. Shi-Pei, and L. Xiao-Wei, "Wireless side-channel analysis method based on spectral addition (in Chinese)," *Journal of Cryptologic Research*, vol. 10, no. 4, pp. 862–878, 2023.
- [89] J. Guillaume, M. Pelcat, A. Nafkha, and R. Salvador, "Attacking at non-harmonic frequencies in screaming-channel attacks," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2023, pp. 87–106.
- [90] J. Liao, H. Wang, J. Wang, and Y. Tang, "Switch-T: A novel multi-task deep-learning network for cross-device side-channel attack," *Journal of Information Security and Applications (JISA)*, vol. 93, p. 104146, 2025.
- [91] F. Durvaux and F.-X. Standaert, "From improved leakage detection to the detection of points of interests in leakage traces," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2016, pp. 240–262.
- [92] H. Wang, D. He, T. Deng, and J. Wang, "Feature reconstruction: Far field em side-channel attacks in complex environment," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 20, pp. 10066 – 10081, 2025.
- [93] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," *Advances in neural information processing systems*, vol. 30, 2017.
- [94] J. Kirkpatrick, R. Pascanu, N. Rabinowitz, J. Veness, G. Desjardins, A. A. Rusu, K. Milan, J. Quan, T. Ramalho, A. Grabska-Barwinska et al., "Overcoming catastrophic forgetting in neural networks," *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3521–3526, 2017.
- [95] Y. Ganin, E. Ustinova, H. Ajakan, P. Germain, H. Larochelle, F. Laviolette, M. March, and V. Lempitsky, "Domain-adversarial training of neural networks," *Journal of Machine Learning Research*, vol. 17, no. 59, pp. 1–35, 2016.
- [96] H. Yu, H. Shan, M. Panoff, and Y. Jin, "Cross-device profiled side-channel attacks using meta-transfer learning," in *ACM/IEEE Design Automation Conference (DAC)*. IEEE, 2021, pp. 703–708.
- [97] L. Wu, L. Weissbart, M. Krček, H. Li, G. Perin, L. Batina, and S. Picek, "Label correlation in deep learning-based side-channel analysis," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 18, pp. 3849–3861, 2023.
- [98] F. Hu, J. Shen, and P. Vijayakumar, "Side-channel attacks based on multi-loss regularized denoising autoencoder," *IEEE Transactions on Information Forensics and Security*, 2023.
- [99] J. Guillaume, M. Pelcat, A. Nafkha, and R. Salvador, "Multi-screaming-channel attacks: Frequency diversity for enhanced attacks," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 21, pp. 4360–4372, 2026.
- [100] M. Greenacre, P. J. Groenen, T. Hastie, A. I. d'Enza, A. Markos, and E. Tuzhilina, "Principal component analysis," *Nature Reviews Methods Primers*, vol. 2, no. 1, p. 100, 2022.
- [101] P. Xanthopoulos, P. M. Pardalos, and T. B. Trafalis, "Linear discriminant analysis," in *Robust data mining*. Springer, 2012, pp. 27–33.
- [102] H. Xie, X. Tian, W. Liao, and Z. Xiong-Jie, "Cryptographic chip security evaluation method based on radio frequency side channel (in Chinese)," *Journal of Cryptologic Research*, vol. 11, no. 3, pp. 706 – 718, 2024.
- [103] G. Grigolo, D. Schiffer, L. Gerster, M. Ringbauer, and P. Erker, "Radio-frequency side-channel analysis of a trapped-ion quantum computer," *arXiv preprint arXiv:2603.06562*, 2026.
- [104] Z. Liu, N. Samwel, L. Weissbart, Z. Zhao, D. Lauret, L. Batina, and M. Larson, "Screen gleaning: A screen reading TEMPEST attack on

- mobile devices exploiting an electromagnetic side channel,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2021.
- [105] P. De Meulemeester, B. Scheers, and G. A. Vandenbosch, “Differential signaling compromises video information security through am and fm leakage emissions,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 62, no. 6, pp. 2376–2385, 2020.
- [106] Q. Zhang, D. Liu, X. Zhang, Z. Cao, F. Zeng, H. Jiang, and W. Jin, “Eye of Sauron: long-range hidden spy camera detection and positioning with inbuilt memory EM radiation,” in *USENIX Security Symposium (USENIX Security)*, 2024, pp. 109–126.
- [107] A. Onishi, S. H. Bhupathiraju, R. Bhatt, S. Rampazzi, and T. Sugawara, “Sound of interference: Electromagnetic eavesdropping attack on digital microphones using pulse density modulation,” in *USENIX Security Symposium*, 2025, pp. 3865–3884.
- [108] H. Yan, Z. Shao, S. Zhang, Q. Jiang, and Y. Long, “Injected and leaked: Actively inducing side-channel leakage using electromagnetic injection and hardware nonlinearity,” in *USENIX Security Symposium*, 2026, pp. 2485–2504.
- [109] M. J. Kannwischer, R. Petri, J. Rijneveld, P. Schwabe, and K. Stoffelen, “PQM4: Post-quantum crypto library for the ARM Cortex-M4,” <https://github.com/mupq/pqm4>.
- [110] R. Wang, K. Ngo, and E. Dubrova, “Side-channel analysis of Saber KEM using amplitude-modulated EM emanations,” in *Euromicro Conference on Digital System Design (DSD)*. IEEE, 2022, pp. 488–495.
- [111] R. Wang and E. Dubrova, “A message recovery attack on LWE/LWR-based PKE/KEMs using amplitude-modulated EM emanations,” in *International Conference on Information Security and Cryptology (ICISC)*. Springer, 2022, pp. 450–471.
- [112] Y. Ji, E. Dubrova, and R. Wang, “Screaming channels revisited: Encryption key recovery from AES-CCM accelerator,” in *2025 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2025, pp. 1–5.
- [113] M. Rivain and E. Prouff, “Provably secure higher-order masking of AES,” in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2010, pp. 413–427.
- [114] X. Lou, T. Zhang, J. Jiang, and Y. Zhang, “A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–37, 2021.
- [115] B. Cao, H. Wang, T. Deng, D. He, Z. Huang, and J. Wang, “Exploiting ShiftRow vulnerabilities in addition-chain masked AES: A novel wireless side-channel attack approach,” *Microelectronics Journal*, p. 106866, 2025.
- [116] S. Sen and A. Ghosh, “Circuit-level techniques for side-channel attack resilience: A tutorial,” *IEEE Solid-State Circuits Magazine (SSC-M)*, vol. 16, no. 4, pp. 96–108, 2024.
- [117] M. Yang, T. Ahmed, S. Inagaki, K. Sakiyama, Y. Li, and Y. Hara-Azumi, “Hardware/software cooperative design against power side-channel attacks on IoT devices,” *IEEE Internet of Things Journal (IoTJ)*, vol. 11, no. 9, pp. 16 758–16 768, 2024.
- [118] Y. Ji, E. Dubrova, and R. Wang, “Is your Bluetooth chip leaking secrets via RF signals?” in *IEEE International Symposium on Multiple-Valued Logic (ISMVL)*, 2025, pp. 141–146.
- [119] T. Gallagher, “Identifying system-on-a-chip data leaks over radio transmissions of small satellites,” *International Journal of Applied Technology and Leadership*, vol. 3, no. 1, pp. 1–19, 2024.
- [120] —, “Understanding how system-on-a-chip data can leak over radio transmissions,” *International Journal of Applied Technology and Leadership*, vol. 3, no. 1, pp. 1–17, 2024.
- [121] R. Xiao, S. Feng, S. Ramesh, J. Han, and J. Han, “Peering inside the black-box: Long-range and scalable model architecture snooping via gpu electromagnetic side-channel,” in *The Network and Distributed System Security Symposium (NDSS)*, 2026.
- [122] M. Yan, C. W. Fletcher, and J. Torrellas, “Cache telepathy: Leveraging shared resource attacks to learn {DNN} architectures,” in *USENIX Security Symposium*, 2020, pp. 2003–2020.
- [123] H. T. Maia, C. Xiao, D. Li, E. Grinspun, and C. Zheng, “Can one hear the shape of a neural network?: Snooping the GPU via magnetic side channel,” in *USENIX Security Symposium*, 2022, pp. 4383–4400.
- [124] T. Nayan, Q. Guo, M. Al Duniawi, M. Botacin, S. Uluagac, and R. Sun, “SoK: All you need to know about On-Device ML model extraction—the gap between research and practice,” in *USENIX Security Symposium*, 2024, pp. 5233–5250.
- [125] Y. Ge, P. Chen, Q. Wang, L. Zhao, N. Mou, P. Jiang, C. Wang, Q. Li, and C. Shen, “More simplicity for trainers, more opportunity for attackers: {Black-Box} attacks on speaker recognition systems by inferring feature extractor,” in *USENIX Security Symposium*, 2024, pp. 2973–2990.
- [126] R. Callan, A. Zajić, and M. Prvulovic, “FASE: Finding amplitude-modulated side-channel emanations,” *ACM SIGARCH Computer Architecture News*, vol. 43, no. 3S, pp. 592–603, 2015.
- [127] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in *Advances in Neural Information Processing Systems*, vol. 25, 2012, pp. 1097–1105.
- [128] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” in *International Conference on Learning Representations*, 2015.
- [129] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2016, pp. 770–778.
- [130] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “Bert: Pre-training of deep bidirectional transformers for language understanding,” in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2019, pp. 4171–4186.
- [131] R. Xiao, T. Li, S. Ramesh, J. Han, and J. Han, “MagTracer: Detecting gpu cryptojacking attacks via magnetic leakage signals,” in *Proceedings of the Annual International Conference on Mobile Computing and Networking*, 2023, pp. 1–15.
- [132] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, “Deep learning for side-channel analysis and introduction to ASCAD database,” *Journal of Cryptographic Engineering*, vol. 10, no. 2, pp. 163–188, 2020.
- [133] A. A. Magazin and K. M. Abdellatif, “Open EM side-channel dataset for ML-KEM (Kyber) implementations,” *Cryptology ePrint Archive*, 2026.
- [134] D. Galli, G. Chiari, D. Zoni *et al.*, “Chameleon: A dataset for segmenting and attacking obfuscated power traces in side-channel analysis,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, vol. 2025, no. 3, pp. 389–412, 2025.
- [135] “Mbed TLS documentation hub,” <https://mbed-tls.readthedocs.io/en/latest/>, accessed: 2026-08-18.
- [136] G. T. Becker, J. Cooper, E. DeMulder, G. Goodwill, J. Jaffe, G. Kenworthy, T. Kouzminov, A. Leiserson, M. E. Marson, P. Rohatgi, and S. Saab, “Test vector leakage assessment (tvla) methodology in practice,” in *International Cryptographic Module Conference*, 2013, p. 13.
- [137] A. Mynewt, “Bluetooth low energy user guide: NimBLE,” <https://mynewt.apache.org/master/network/index.html>, accessed: 2026-08-21.
- [138] D. He, W. Cheng, Y. Liu, J. Ming, and Y. Zhou, “PD-Net: Learning device-invariant representations for heterogeneous cross-device side-channel attacks,” in *Proceedings of the 56th Annual Design Automation Conference (DAC)*, 2026.
- [139] A. Liu, A. Wang, S. Sun, C. Wei, Y. Ding, Y. Wang, and L. Zhu, “CL-SCA: A contrastive learning approach for profiled side-channel analysis,” *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 20, pp. 5109–5122, 2025.
- [140] H. Groß and S. Mangard, “A unified masking approach,” *Journal of cryptographic engineering*, vol. 8, no. 2, pp. 109–124, 2018.
- [141] T. B. Singha, R. P. Palathinkal, and S. R. Ahamed, “Securing aes designs against power analysis attacks: A survey,” *IEEE Internet of Things Journal (IoTJ)*, vol. 10, no. 16, pp. 14 332–14 356, 2023.
- [142] B. Gigerl, F. Klug, S. Mangard, F. Mendel, and R. Primas, “Smooth passage with the guards: Second-order hardware masking of the AES with low randomness and low latency,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, vol. 2024, no. 1, pp. 309–335, 2024.
- [143] V. Hadžić and R. Bloem, “Efficient and composable masked AES S-Box designs using optimized inverters,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, vol. 2025, no. 1, pp. 656–683, 2025.
- [144] B. Hettwer, K. Das, S. Leger, S. Gehrler, and T. Güneysu, “Lightweight side-channel protection using dynamic clock randomization,” in *2020 30th International Conference on Field-Programmable Logic and Applications (FPL)*. IEEE, 2020, pp. 200–207.
- [145] D. Jayasinghe, Y. Zhong, and S. Parameswaran, “JitFilt: Mitigate jitter-based side channel analysis attacks,” in *IEEE/ACM International Conference On Computer Aided Design (ICCAD)*. IEEE, 2025, pp. 1–9.
- [146] M. Moraitis, M. Brisfors, E. Dubrova, N. Lindskog, and H. Englund, “A side-channel resistant implementation of AES combining clock randomization with duplication,” in *IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2023, pp. 1–5.

- [147] M. Brisfors, M. Moraitis, G. K. Landin, and T. Jilborg, "Attacking and securing the clock randomization and duplication side-channel attack countermeasure," in *International Symposium on Foundations and Practice of Security*. Springer, 2023, pp. 372–387.
- [148] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2000, pp. 252–263.
- [149] J.-S. Coron and I. Kizhvatov, "An efficient method for random delay generation in embedded software," in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2009, pp. 156–170.
- [150] Y. Yano, K. Iokibe, Y. Toyota, and T. Teshima, "Signal-to-noise ratio measurements of side-channel traces for establishing low-cost countermeasure design," in *2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (AP EMC)*. IEEE, 2017, pp. 93–95.
- [151] P. Clerico, L. Pichon, X. Mininger, O. Dubrunfaut, F. Monsef, C. Gannouni, D. He, J. Bai, and L. Prevond, "Assessment of broadband shielding effectiveness of composite panels for protective enclosures," *IEEE Transactions on Electromagnetic Compatibility*, vol. 64, no. 5, pp. 1750–1757, 2022.
- [152] D. Dobkin, E. Katz, D. Popovtzer, and I. Levi, "EMI shielding for use in side-channel security: Analysis, simulation, and measurements," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 22, no. 1, pp. 1–22, 2025.
- [153] P. Chen, J. Li, W. Cheng, and C. Cheng, "Uncover secrets through the cover: A deep learning-based side-channel attack against Kyber implementations with anti-tampering covers," *IEEE Transactions on Computers (TC)*, vol. 74, no. 6, pp. 2159–2167, 2025.
- [154] D. Park, J. Jeon, and H. Kim, "Antenna sensitivity variation depending on the installation of a shield can," *Microwave and Optical Technology Letters*, vol. 62, no. 6, pp. 2311–2315, 2020.