IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2026, No. 1, pp. 376–401. DOI:10.46586/tches.v2026.i1.376-401

Active Electromagnetic Side-Channel Analysis: Crossing Physical Security Boundaries through Impedance Variations

Taiki Kitazawa[1], Lennert Wouters[2], Benedikt Gierlichs[2], Daisuke Fujimoto[1], Ingrid Verbauwhede[2] and Yuichi Hayashi[1]

[1] Nara Institute of Science and Technology (NAIST), Japan
{kitazawa.taiki.kq8,fujimoto,yu-ichi}@is.naist.jp
[2] COSIC, KU Leuven, Belgium
{lennert.wouters,benedikt.gierlichs,ingrid.verbauwhede}@esat.kuleuven.be

Abstract. Embedded devices that are physically unreachable or contained within tamperproof enclosures are often considered naturally resilient to physical side-channel attacks. We present an active EM side-channel attack technique that enables side-channel attacks across the security boundaries introduced by these physical security measures. Our technique actively induces side-channel leakage based on a relay mechanism, which serves as a means of leakage propagation from the cryptographic IC to the attacker via intermediate Relay Points located within the boundary. In the first leakage path, the instantaneous current consumption caused by transistor switching inside the cryptographic IC affects the impedance of nearby nonlinear elements (such as regulators) that act as Relay Points. This phenomenon is inevitable due to the necessity of the regulator's operations to ensure the provision of a stable voltage to the cryptographic IC. In the second path, EM waves irradiated by the attacker from outside the security boundary create a leakage channel where reflected waves are modulated by the impedance variation of Relay Points, and leak outside as side-channel information. We experimentally demonstrate that side-channel attacks can be performed from the power cable on the primary side of an AC/DC adapter, even in environments protected by physical security measures, including a shielded box and ferrite cores. This attack can be executed non-invasively using EM waves in the hundreds of MHz band, and has the advantage of being able to actively control the presence and intensity of leakage. The proposed attack technique may be applicable in a wide range of applications as it exploits the behavior of nonlinear elements present in all embedded systems. As countermeasures against the proposed attack, we discuss the effectiveness of EM fault sensors for detecting continuous wave irradiation, induced EM interference detectors with broadband monitoring capabilities, and tamper detection systems utilizing radio frequencies. This research highlights the importance of considering active EM measurements as a new threat model in physical security evaluations.

Keywords: Side-channel Analysis · Power/Electromagnetic/Backscatter/Impedance Analysis

1 Introduction

Side-Channel Analysis (SCA) is the art of recovering secret information through the analysis of a physical observable such as the instantaneous current consumption [KJJ99]. Power analysis primarily exploits the dynamic power consumption associated with transistors switching inside Integrated Circuits (ICs) as a leakage source. Electromagnetic

Licensed under Creative Commons License CC-BY 4.0.
Received: 2025-07-15 Accepted: 2025-09-15 Published: 2026-01-16

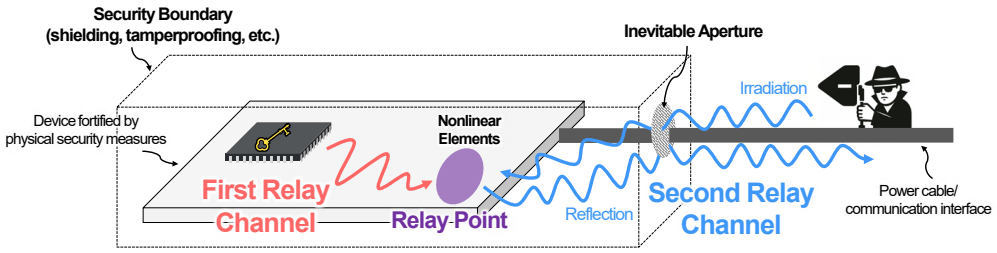


Figure 1: Overview of Active EMA

Analysis (EMA), which exploits unintentional electromagnetic (EM) emanations during cryptographic operations, is a natural extension of power analysis [QS01, GMO01]. Unlike power analysis, EMA enables attacks using EM probes or antennas, without requiring physical contact or modification.

SCA fundamentally consists of two stages: "measurement" and "analysis" of side-channel information. This two-stage nature of SCA leads to a basic defense principle: if measurement can be prevented, subsequent analysis cannot succeed. Based on this principle, various countermeasures have been proposed at the board design [HHM+13], circuit level [HB25], architecture, and algorithm levels [TG07]. Among these, forming security boundaries using physical security measures is one of the most robust approaches.

Physical security measures create distinct security boundaries between potential attackers and target devices [Com22, Nat01, Nat19]. For example, tamper detection [GS22, OI18, ION+18] protects by detecting and responding to unauthorized physical access, while shielding [Int15] prevents emanations from leaking outside the security boundary while also suppressing external interference and disturbance. These technologies are complemented by other physical security measures such as tamper evidence, tamper resistance, and zoning [Wei00]. The strength of physical layer countermeasures lies in their ability to enforce physical spatial separation between attackers and devices, providing algorithm-independent security that continues protection even when new vulnerabilities are discovered in cryptographic devices.

Even if such security boundaries are established through physical security measures, inevitable apertures exist to accommodate power delivery and communication interfaces [OI18]. Information leakage through such apertures on security boundaries has been demonstrated as leakage from conducted EM emissions [1] through power and communication cables [HSK+10, SHH+09, GPT15], and leakage from clock jitter and phase noise in input/output (I/O) signals of communication interfaces [SMTG23, O'F24, AHC+24].

However, such attacks are performed through passive observation of side-channel information from outside the security boundary. Therefore, it is possible to try to confine this leakage within the boundary by applying techniques such as filtering and isolation. In such cases, leakage generated from cryptographic devices is reduced below background noise levels outside the security boundary, making passive SCA infeasible for attackers without physical access to the inside of the boundary.

Physical security measures that impede physical access while confining leakage within the security boundary can be considered exceptionally robust. In this work, we propose the use of active EM measurement methods that allow us to pierce the security boundaries put in place by such physical security measures. The proposed Active EMA technique exploits electrical characteristics of nonlinear components in embedded devices and is based on the

[1] Conducted EM emissions are unintended RF currents and voltages that travel along power or signal conductors (e.g., power or communication lines). Radiated EM emissions, by contrast, are unintended EM fields that propagate through free space from structures acting as unintentional antennas (e.g., cables, PCB traces, or enclosures) [PSS22].

following relay mechanism (see Figure 1).

First Relay Channel: This channel relays side-channel leakage to nonlinear elements in the device. These nonlinear components are electrically and electromagnetically coupled with the target IC. Specifically, the transient current generated by Complementary Metal-Oxide-Semiconductor (CMOS) transistors switching inside cryptographic ICs causes voltage fluctuations (so-called ground bounce) through parasitic EM coupling on the IC and board. These voltage fluctuations affect the impedance of nonlinear elements such as regulators, creating Relay Points. In particular, since cryptographic ICs and regulators are electrically coupled for stable operation of the device, this relay path inevitably exists.

Second Relay Channel: This channel enables us to cross the physical security boundary by actively irradiating EM waves from outside the boundary. Specifically, when irradiated EM waves reach nonlinear elements serving as Relay Points, modulated reflected waves emerge due to variations in their impedance. These reflected waves thus serve as a relay channel that pierces the physical security boundary from within.

Through the relay mechanisms, we demonstrate attacks against cryptographic devices with physical security measures that are considered challenging or even impossible to compromise using conventional passive measurement techniques. Specifically, we recover full Advanced Encryption Standard (AES) secret keys from the primary side of the Alternating Current (AC)/Direct Current (DC) adapter, even in environments protected by a shielded box and ferrite cores. The technique introduced here is related to other side-channel approaches such as impedance- and backscatter-based analysis, but differs from them in that it actively induces leakage (see Section 2.3). Furthermore, Active EMA has the following advantageous characteristics: (1) Controllability: Through active measurement, attackers can actively control the presence and intensity of leakage. (2) Non-invasive, non-contact execution: EM wave attacks in the hundreds of MHz band enable attack execution without physical contact. (3) Applicability: Exploits nonlinear elements commonly found in typical electronic devices, making it applicable to various embedded systems under realistic scenarios.

The contributions of this paper are as follows:

- We propose a novel active EM side-channel measurement method based on the relay mechanism.
- We experimentally demonstrate that secret keys can be recovered from cryptographic devices with physical security measures, such as shielding and ferrite cores, applied to the primary side power cable of AC/DC adapters.
- We demonstrate that attackers can arbitrarily adjust the intensity and range of leakage by controlling the intensity of irradiated signals.
- We summarize defense guidelines against the proposed attack method for strengthening physical security boundaries.

In the remaining paper, we will summarize related works in Section 2. In Section 3, we will explain the threat model of Active EMA. In Section 4, we will present the details of the relay mechanism of our proposed method: Active EMA. Our experimental setups and results are described in Section 5. In Section 6, we summarize countermeasures and future challenges. Finally, Section 7 concludes the paper.

2 Related Work and Background

2.1 Electromagnetic Analysis (EMA)

EMA is a kind of SCA that recovers secret keys and data using EM waves unintentionally radiated from cryptographic devices [QS01, GMO01, AARR03]. Attackers capture EM waves using antennas or probes and analyze them with receivers. EMA includes "Local EMA" [PSQ07, SSS+13, SBO+15, LDMPT15], which observes localized EM waves from ICs, and "Far-Field EMA" [AARR03, SHH+09, GPT15], which leak far away as unintended emissions in the MHz to GHz bands. Recently, threats have been reported where side-channel information is superimposed on wireless communications due to coupling between digital and analog circuits in System-on-a-Chip (SoC), the so-called Screaming Channels [CPM+18, CFS20, GPNS25].

The advantage of EMA lies in non-invasive and non-physical contact measurement [KOP09, HMF07]. Still, since it is based on passive measurement, it is possible to reduce radiation intensity and make attacks difficult through design considerations of Electromagnetic Compatibility (EMC), Power Integrity (PI), and Signal Integrity (SI), as well as shielding and filtering. Screaming Channels can also prevent observation of side-channel information on communication channels by suppressing internal EM coupling.

2.2 SCA from the Primary Side

As SCA from the primary side, some attacks utilize pulse width changes in switching power supplies [SLT16, KFH24]. However, the target of conventional research is DC/DC regulators that directly supply power to cryptographic cores, requiring attackers to have proximity access to cryptographic devices. Furthermore, in real systems, as signals pass through multiple stages of regulators, side-channel information on primary side power lines is expected to be filtered down to background noise levels. Additionally, since these attacks are executed through passive measurement, leakage can be suppressed by countermeasures in the same way as passive EMA.

2.3 Impedance-/backscatter-based Analysis

Research has been reported on measuring internal IC impedance variations using THz-band EM waves [AJCZ19, WPZ22], but secret key recovery has not yet been achieved. Furthermore, the THz band has high attenuation, making measurements from a distance difficult and limiting them to those directly above the chip. In contrast, Monfared et al. proposed LeakyOhm using the several GHz band [MMT23, AGR24]. While it utilizes Power Delivery Network (PDN) impedance changes associated with channel formation changes in CMOS inside ICs, it requires the suspension of operation of cryptographic devices and a physical connection to the power supply. Additionally, the GHz band also has high attenuation, and non-contact attacks have not been realized.

2.4 Active/Passive TEMPEST

TEMPEST targets EM leakage of unencrypted I/O signals from computer peripherals, assuming attacks under Non-Line-of-Sight (NLOS) conditions from distances of tens of meters or more [KAK+22, vE85, Kuh05]. The recently reported Echo TEMPEST is an active attack that irradiates MHz-band EM waves and recovers I/O information from reflected waves [KFKH23, PLHD25]. While attack distance and resolution are controllable, the target is low-speed digital signals, making the measurement of side-channel information inside ICs difficult. This is because internal CMOS gates are small and can only be observed with EM waves above the GHz band, making propagation from a distance difficult.

3 Threat Model

Adversary's Goal: The attacker's objective is to obtain secret keys and data from cryptographic devices installed within security boundaries, without physical contact. Specifically, the attacker aims to actively relay side-channel information confined within the boundary outward, and recover secret keys by collecting and analyzing the leaked signals.

Scenario: The targeted cryptographic devices are assumed to be mission-critical systems such as Automated Teller Machines (ATMs), infrastructure control systems, servers equipped with Hardware Security Modules (HSMs), and smart meters. In these devices, clear security boundaries are formed by physical security measures such as shielding [Int15] and tamperproofing [GS22, OI18, ION+18], which thwart physical access within the boundary and SCA through passive measurement. However, practically inevitable apertures for the connection of power supply lines and communication interfaces still remain and serve as attack surfaces. In this scenario, we assume a situation where attackers irradiate high-frequency EM waves in the hundreds of MHz band into the boundary through these inevitable apertures. The EM waves propagate to nonlinear elements (Relay Points) whose impedance varies due to ground bounce generated during operation of cryptographic ICs (First Relay Channel). Subsequently, the modulated reflected waves generated from these nonlinear elements are emitted beyond the boundary (Second Relay Channel).

Attack Setup: The attacker utilizes the following equipment: a signal generator, a receiver, transmitting/receiving antennas/probes, and analysis equipment (e.g., Personal Computer (PC)). By optionally using signal amplifiers, it is possible to enhance irradiation intensity and reception sensitivity, allowing for attacks from greater distances and improving the quality of acquired traces.

4 Flow of Active EMA

This section explains the attack flow of Active EMA based on the relay mechanism (see Figure 2).

First Relay Channel (Section 4.1): A relay channel where side-channel information generated inside cryptographic ICs propagates to surrounding nonlinear elements through EM and electrical coupling. We refer to the nonlinear elements relaying side-channel information between the First Relay Channel and the Second Relay Channel as "Relay Points".

Second Relay Channel (Section 4.2): A relay channel where side-channel information that has reached Relay Points propagates beyond the security boundary by actively irradiated EM waves.

4.1 First Relay Channel Induced Through Ground Bounce

4.1.1 Ground Bounce Generated by Cryptographic Operations

The source of side-channel information leakage is the switching operation of CMOS gates within cryptographic ICs [MOP07]. When logic values of each logic circuit transition, dynamic power consumption occurs due to charging current and short-circuit current associated with transistor on/off operations. During cryptographic operations, many such switching events occur simultaneously, and their collective power consumption depends on data, enabling secret key recovery [KJJ99].

In power analysis, voltage fluctuations on the PDN of the cryptographic IC are measured[2]. Such voltage fluctuations are known in the fields of EMC and PI as ground

[2]Similar information can be obtained from current fluctuations measured via shunt resistors

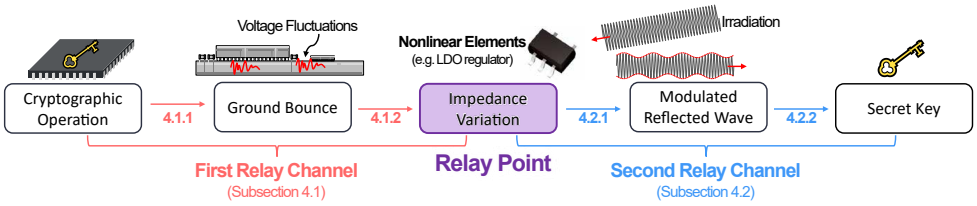


Figure 2: Flow of Active EMA

bounce caused by the simultaneous switching of CMOS gates [SE07]. Ground bounce occurs when transient charging current and short-circuit current induce voltage through parasitic components on the IC core, package, and PDN. Therefore, such phenomena inevitably occur with IC operation, i.e., side-channel information is widely distributed on the PDN as voltage fluctuations.

4.1.2 Formation of Relay Points via Ground Bounce

Ground bounce containing side-channel information induces impedance variations in nonlinear elements existing on the same PDN of cryptographic ICs. These nonlinear elements function as Relay Points, effectively enabling us to cross security boundaries. The requirements for nonlinear elements to act as Relay Points are: (1) the impedance of nonlinear elements varies due to the influence of ground bounce, and (2) EM waves efficiently propagate from outside to inside the security boundary, reaching the relevant elements to generate reflected waves.

Impedance Variation: Nonlinear elements exist in typical components on Printed Circuit Boards (PCBs), including digital circuits within ICs, diodes (Transient Voltage Suppressors (TVSs), Light Emitting Diodes (LEDs), etc.), Multi-Layer Ceramic Capacitors (MLCCs), and regulators. The PDN of a cryptographic IC is no exception; nonlinear elements are used in peripheral circuits both inside and outside cryptographic ICs to ensure normal operation. These nonlinear elements show significant impedance changes compared to linear elements, even with weak voltage changes from ground bounce, potentially enabling the exploitation of side-channel information.

As a specific example, we explain impedance variations in Low-Dropout (LDO) regulators (see Figure 3). LDO regulators are widely used for both on-chip and off-chip power supply circuits, and its operation utilizes the characteristics of internal nonlinear elements. The purpose of the LDO regulator is to convert the voltage supplied from the input side (primary side) to the output side (secondary side) while dynamically adjusting the output current to maintain a constant voltage value. In detail, the operation works as follows: (1) the load consumes current, (2) the LDO's output voltage drops, (3) a difference from the reference voltage is detected, (4) the equivalent resistance of the power Field Effect Transistor (FET) changes, causing impedance variation, (5) output is compensated to maintain constant voltage. Assuming (1) and (2) are the result of current consumption and ground bounce due to cryptographic operations, we find that regulator impedance variation occurs at step (4). Furthermore, this behavior is essential for the stable operation of output-side loads, making impedance variations of peripheral nonlinear elements unavoidable [SJL+21].

Beyond regulators, other ubiquitous nonlinear components on the PDN can act as Relay Points. (1) P-N junction devices, including TVSs, ESD protection circuits, and indicator LEDs, are known to have capacitance and conductance that change depending on the applied bias. Even small ground-bounce fluctuations can therefore alter their electrical behavior [SB15, ch. 5]. (2) Decoupling MLCCs, particularly those using Class II dielectrics such as X5R or X7R, show a strong dependence of their capacitance and

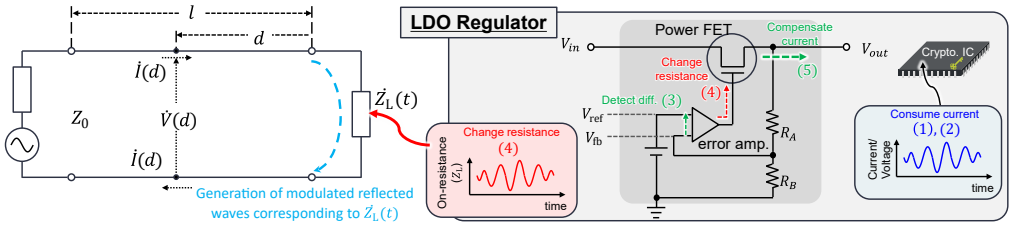


Figure 3: Flow from the occurrence of ground bounce to the generation of modulated reflected waves. (Left) Simplified transmission line model using a distribution multiplier circuit. The reflected waves are modulated according to the time variation of $Z_{\mathrm{L}}(\mathrm{t})$. (Right) Example of impedance variation accompanying cryptographic operations of nonlinear elements. LDO regulator stabilizes the load operation, so the on-resistance variation is unavoidable.

losses on both DC and AC bias [NWM+11][3]. This makes them especially susceptible to changes in operating conditions around cryptographic devices. (3) I/O interfaces and power-management circuits inside integrated-circuit packages also include non-linear transistors and protection structures.

Transfer Characteristics from Outside to Relay Points: Impedance variations at Relay Points are actively sensed via EM waves, as explained in Section 4.2.1 below. Therefore, Relay Points require sensitivity in frequency bands where EM waves—irradiated by the attacker and passing through apertures in the security boundary—can efficiently reach the nonlinear elements serving as Relay Points without attenuating below the background-noise level[4].

First, we explain why impedance changes associated with channel formation states of CMOS gates inside cryptographic ICs, which were focused on in conventional impedance-based analysis [MMT23, AGR24, AJCZ19, WPZ22], are not suitable as Relay Points. Such impedance change points are located within the internal digital circuits of ICs, and their physical structures are extremely small at the nanometer scale. To propagate EM waves from there and sense them, it is necessary to inject EM waves in the GHz/THz bands with short wavelengths. However, as EM waves have increasing attenuation rates at higher frequencies, they are unsuitable for sensing from distant locations. Indeed, conventional research has required physical access to cryptographic devices (connection to the PDN via Sub Miniature Type-A (SMA) connectors) and temporary suspension of cryptographic processing to extract secret keys.

In contrast, the nonlinear elements focused on in this research are surface-mounted on PCBs or larger I/O circuits within the IC. Particularly, regulators are placed between power planes, making them easily reachable by EM waves from outside. Furthermore, as the physical structures of these elements are on the micrometer scale, they show sensitivity to the hundreds of MHz band with longer wavelengths than the GHz band [KFKH23]. As a result, they have smaller propagation attenuation when compared to the GHz/THz bands and offer good transfer characteristics, which have been confirmed in actual EM information leakage [KFKH23, dMSV20, IMK+25].

[3]In actual components, the voltage dependence of capacitance can be confirmed from datasheets and tools published by manufacturers (e.g., Murata Manufacturing Co., Ltd., SimSurfing, https://ds.murata.com/simsurfing/mlcc.html, accessed 28 September 2025)

[4]Due to EM reciprocity, propagation characteristics from nonlinear elements to the point where attackers observe EM waves are similar, so we consider only one direction here.

4.2 Second Relay Channel by Active EM Measurement

4.2.1 Modulated Reflected Waves Generated at Relay Points

We describe how to generate a Second Relay Channel that leverages the impedance variations at Relay Points. The Second Relay Channel uses active EM measurements to pierce the security boundaries. Specifically, attackers inject continuous waves into cryptographic devices, resulting in amplitude and phase modulated reflected waves, because of impedance changes at Relay Points. First, we explain the physical mechanism of modulated reflected wave generation, and then describe the method for constructing a relay channel by optimizing parameters such as irradiation frequency, amplitude, and transmission mode.

Mechanism of Modulated Reflected Wave Generation: The derivations in this Subsection follow the textbook [Poz21, ch. 2]. To explain how EM waves irradiate and propagate to cryptographic devices, we use the model of Figure 3, where a transmission line of length l is excited at an excitation source and terminated with load impedance $\dot{Z}_{\mathrm{L}} = R + jX$. When the line length is sufficiently long relative to the excitation source wavelength, the line is treated as a distributed-element model, and voltage $\dot{V}$ and current $\dot{I}$ at distance $d = 0$ from the receiving end are expressed as follows[5]

$$\dot{V} = \dot{V}_{\mathrm{i}} + \dot{V}_{\mathrm{r}}, \quad \dot{I} = \dot{I}_{\mathrm{i}} + \dot{I}_{\mathrm{r}} = \frac{\dot{V}_{\mathrm{i}}}{Z_0} - \frac{\dot{V}_{\mathrm{r}}}{Z_0} \tag{1}$$

Here, Z_0 is the characteristic impedance of the line. The first terms ($\dot{V}_{\mathrm{i}}$, $\dot{I}_{\mathrm{i}}$) are incident wave components. In contrast, the second terms ($\dot{V}_{\mathrm{r}}$, $\dot{I}_{\mathrm{r}}$) are reflected wave components, which change depending on the impedance of the load. Specifically, they are expressed by the following relational expressions using the reflection coefficient $\dot{\Gamma}$.

$$\dot{V}_{\mathrm{r}} = \dot{\Gamma}\,\dot{V}_{\mathrm{i}} = |\dot{\Gamma}|\dot{V}_{\mathrm{i}}e^{-j\phi}, \quad \dot{I}_{\mathrm{r}} = -\dot{\Gamma}\,\dot{I}_{\mathrm{i}} = -|\dot{\Gamma}|\dot{I}_{\mathrm{i}}e^{-j\phi} \tag{2}$$

$$\because \quad \dot{\Gamma} = (\dot{Z}_{\mathrm{L}} - Z_0)/(\dot{Z}_{\mathrm{L}} + Z_0) \tag{3}$$

$|\dot{\Gamma}|$ is the absolute value of the reflection coefficient, where $0 \leq |\dot{\Gamma}| \leq 1$. ϕ shows the phase component of the reflection coefficient. As seen from Equation 2 and Equation 3, reflected waves relative to incident waves change according to load impedance. That is, assuming the load impedance $\dot{Z}_{\mathrm{L}}$ is the time-varying impedance of Relay Points containing side-channel information $\dot{Z}_{\mathrm{L}}(t)$, voltage $\dot{V}(t)$ and reflected current $\dot{I}(t)$ on the transmission line become:

$$\dot{V}(t) = \dot{V}_{\mathrm{i}} + \dot{V}_{\mathrm{r}}(t) = \dot{V}_{\mathrm{i}}\left(1 + |\dot{\Gamma}(t)|e^{-j\phi(t)}\right), \quad \dot{I}(t) = \dot{I}_{\mathrm{i}} + I_{\mathrm{r}}(t) = \dot{I}_{\mathrm{i}}\left(1 - |\dot{\Gamma}(t)|e^{-j\phi(t)}\right) \tag{4}$$

From this, we see that when the load (Relay Point) changes impedance over time, modulated signals with amplitude and phase modulation relative to the incident waves are generated. Thus, attackers can generate reflected waves modulated with side-channel information from Relay Points by propagating continuous EM waves with constant amplitude and phase as sensing signals.

Generation Method of Reflected Waves Modulated with Side-channel Information: From the above mechanism, attackers must first ensure that continuous waves reach the Relay Points. At that time, measurements are taken while optimizing the amplitude and frequency of EM waves used for sensing. This leads to problems where increasing amplitude reduces modulation depth due to self-interference, and challenges in searching for optimal irradiation frequency bands.

[5] At this time, input impedance $\dot{Z}_{\mathrm{in}}$ seen from $d = 0$ is $\dot{Z}_L = \dot{Z}_{\mathrm{in}}$. For simplicity, the attenuation constant $\alpha = 0$.

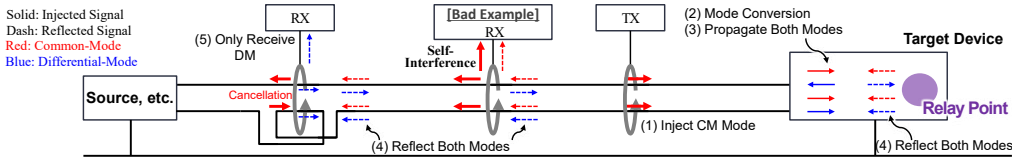


Figure 4: Active EMA measurement methods executed through transmission lines. When using the same mode, signals output from the transmitter directly superimpose on the receiver, degrading modulation depth due to self-interference effects, consequently leading to a decline in the accuracy of information acquisition. When using different modes, signals output from the transmitter cancel out on the receiver side, enabling the reduction of self-interference effects.

Algorithm 1: Frequency Sweep TVLA for Relay Channel Search

Input: $f_{\text{start}}, f_{\text{end}}, f_{\text{step}}, P_{\text{TX}}, N$
Output: T-test values $T[f_c]$ for each frequency f_c
for $f_c = f_{start}$ **to** f_{end} **step** f_{step} **do**
  `injection_on`(P_{TX}, f_c);
  `adjust_gain`$()$;
  $(\text{traces}_{\text{fixed}}, \text{traces}_{\text{random}}) \leftarrow$ `collect_traces`$(2N)$;
  $(\text{traces}^{pp}_{\text{fixed}}, \text{traces}^{pp}_{\text{random}}) \leftarrow$ `apply_preprocessing`$(\text{traces}_{\text{fixed}}, \text{traces}_{\text{random}})$;
  $T[f_c] \leftarrow$ `TVLA`$(\text{traces}^{pp}_{\text{fixed}}, \text{traces}^{pp}_{\text{random}})$;
  `injection_off`$()$;

The former challenge regarding self-interference can be addressed by the measurement method that focuses on different transmission modes, as shown in Figure 4. Self-interference is a problem where irradiated EM waves from the transmission side directly interfere with the reception side, reducing modulation depth and degrading information recovery accuracy. Particularly for attacks from distant locations, the power of reflected waves $\dot{P}_r$ becomes very small relative to incident waves $\dot{P}_i$ ($\dot{P}_i > \dot{P}_r$) due to increased attenuation effects with long propagation paths, making demodulation difficult. This method enables reception of reflected waves while suppressing direct interference of transmitted waves by using different transmission modes on the transmission and reception sides [PSS22, ch. 6]. For example, in transmission lines composed of two wires, EM waves propagate in either differential mode (DM)[6] or common mode (CM)[7]. First, we inject CM or DM signals into the transmission lines. (2) Then, due to changes in geometric structure or the existence of parasitic coupling, some EM energy converts their mode. (3) The EM waves of both modes reach the relay points. (4) Both modes are reflected from the relay points. (5) Although both modes reach the receiver, we only observe one mode on the transmission side. This is because, if we set the same mode as the transmitter, direct interference occurs.

Next, the frequency to create the relay channel is determined by algorithm 1. (1) Sweep frequencies in the range of hundreds of MHz to several GHz that tend to be well distributed on electronic devices. (2) Receive reflected waves at each frequency and adjust receiver gain based on their intensity (`adjust_gain()`). (3) Acquire multiple traces and optionally apply preprocessing techniques (`collect_traces()`,`apply_preprocessing()`). (4) Perform Test Vector Leakage Assessment (TVLA) on acquired traces (`TVLA()`). (5) Based on TVLA results, we determine the most suitable frequency bands for relaying

[6] In differential mode, one wire serves as the forward path and the other as the return path for EM wave propagation.
[7] In common mode, EM waves propagate in the same direction on both wires, using the reference ground plane as the return path.

side-channel information.

Note that propagation characteristics to the Relay Points depend on board size and shape, cable length, and chassis structure. If these elements do not change significantly then the same carrier frequency bands can be used for similar target scenarios [HHM+13][8].

4.2.2 Analysis of Received EM Waves

Preprocessing: Reception and signal processing of EM waves consists of demodulation, outlier removal, and filtering. First, we apply demodulation to the received signals. Reflected signals generated by EM irradiation are expressed as amplitude and phase modulated signals $s_{\mathrm{r}}(t) = A(t)\sin(2\pi f_{\mathrm{inj}} t + \phi(t))$. Here, f_{inj} is the irradiation frequency, and $A(t)$ and $\phi(t)$ are the modulated amplitude and phase signals. After the reflected waves are down-converted to baseband signals at the receiver, they are represented as orthogonal components as follows:

$$I(t) = A(t)\cos\phi(t), \quad Q(t) = A(t)\sin\phi(t), \tag{5}$$

Here, variations in Relay Point impedance are obtained by applying amplitude and phase demodulation.

$$A(t) = \sqrt{I(t)^2 + Q(t)^2}, \quad \phi(t) = \mathrm{atan2}\big(Q(t),\, I(t)\big). \tag{6}$$

Time-series data obtained through this demodulation processing directly reflects impedance variations at Relay Points, and this data is used for analysis. In this research, we utilized amplitude demodulation traces, which allowed for clearer observation of impedance changes.

Next, in Active EMA measurements under real environments, surge-like noise may be present on traces due to external EM noise or unintended modulation from other device operations, so outlier removal is optionally applied. Abnormal traces are removed by anomaly detection using the Interquartile Range (IQR) method. A detailed explanation is shown in Appendix A.

Finally, a High-Pass Filter (HPF) and a Low-Pass Filter (LPF) are applied. The HPF is used to suppress carrier intensity drift caused by temperature characteristics of transmission lines, peripheral equipment, and cryptographic devices themselves [MMT23]. If needed the LPF is applied to reduce high-frequency noise within the reception frequency band.

Leakage assessment. We use TVLA [GJJR11]: two trace sets (fixed plaintext vs. random plaintexts) are compared using Welch's t-test. Here, if $|t| > 4.5$, leakage is determined to exist with a confidence level of > 0.99999. For key recovery on AES, we employ the widely used Hamming weight of the S-box output leakage model to perform CPA [MOP07], since impedance variations at Relay Points are caused by ground bounce accompanying transistor switching, they are amplitude/phase modulated in reflected waves.

5 Experimental Results

This section experimentally verifies the feasibility of AES secret key recovery through Active EMA based on the relay mechanism. First, Section 5.1 presents a preliminary setup for evaluating the basic feasibility of the proposed method and for profiling the relay channel, as well as a setup with security boundaries, assuming a real environment with physical security measures such as shielding and filtering applied. Next, Section 5.2 demonstrates leakage induction through the proposed method using the preliminary setup and conducts a frequency profiling of the available relay channel. Subsequently, Section 5.3 shows that secret key recovery is possible from reflected waves by injecting EM waves

[8] While execution is possible with online search alone, measurement time becomes enormous in proportion to sweep range, so combined use with advance profiling is practical.

from the external DC power line of the PCB. Then, Section 5.4 demonstrates that in cryptographic devices installed within security boundaries, side-channel information can be leaked outside the security boundaries through filters, adapters, and a shielded box from the primary side power cable of AC/DC adapters, enabling secret key recovery. Finally, Section 5.5 demonstrates that by adjusting the EM wave irradiation intensity, it is possible to control leakage from cryptographic devices, thereby expanding the leakage range and enhancing attack performance.

5.1 Experimental Setup

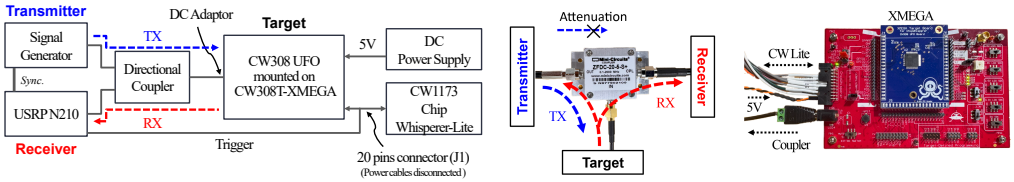
Setup I (Figure 5) is a preliminary setup for verifying the feasibility of Active EMA and for profiling the relay channel. **Setup II** (Figure 6) is reminiscent of a real environment with physical security measures applied through shielding and filtering. First, we describe the common elements of each setup.

We use a CW308T-XMEGA (NewAE Technology) target board with an Atmel 8-bit microcontroller mounted on a CW308 UFO board (NewAE Technology). The power switches on the CW308 UFO were set to `S1:Auto` and `S2:LDO`, converting the 5 V supply voltage to 3.3 V through the off-chip LDO regulator for the cryptographic core power supply. The cryptographic device's clock frequency was set to 12 MHz. The CW308 base and target boards include decoupling MLCCs placed according to the chip vendor's reference design—at the LDO input and output, as well as on the high side of the shunt resistor on the target board. We did not modify this decoupling network in our experiments. A CW1173 ChipWhisperer-Lite (NewAE Technology) [OC14] was used for AES plaintext/ciphertext transmission and reception, with only the communication cable connected to CW308 UFO to ensure power isolation. A signal generator (Rohde & Schwarz, SMA100B) was used as the transmitter, and a software-defined radio (SDR) (Ettus Research, USRP N210, UBX Board) as the receiver. Transmission and reception were synchronized by supplying a reference clock from the transmitter to the receiver, and trigger signals were input to the Pulse-Per-Second (PPS) port to control measurement timing. The ChipWhisperer-Lite, signal generator, and SDR were all connected to a PC that controls the execution of cryptographic operations, EM wave irradiation control, and waveform acquisition/analysis.

We used an unprotected AES-128[9] implementation, and measurements were conducted targeting the 1st round. All experiments used a single fixed 128-bit AES key `2b7e151628aed2a6abf7158809cf4f3c` as per NIST SP 800-38A. The SDR sampling rate was set to 25 MSa/s, with a measurement duration of 125 µs (3125 samples). The SDR gain was set to the maximum gain within the range where the received signal would not saturate.

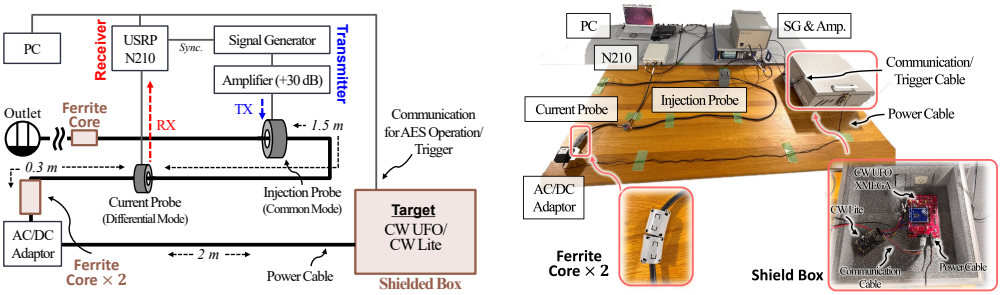
Setup I: This setup verifies the basic feasibility of Active EMA and profiles the relay channel on the same device model as the target. While it does not emulate a protected environment, an attacker can use such a setup to identify favorable parameters prior to attacking a device within a security boundary. To inject EM waves from power lines connected to the cryptographic device and observe reflected waves, a coaxial cable was connected to the DC adapter. This cable was connected to a directional coupler (Mini-Circuits: ZFDC-20-5-S+) to separate incident and reflected waves (Figure 5(b)). Specifically, the transmitter was connected to the coupler's `IN Port`, and the `OUT Port` was connected to the cryptographic device's power line. EM waves propagating from `IN Port` to `OUT Port` were observed by connecting the `CPL Port` to the receiver. Power was supplied from different pins[10].

[9] https://github.com/newaetech/chipwhisperer/tree/develop/firmware/mcu/simpleserial-aes
[10] Similar results were obtained when power was supplied from the DC adapter using a bias tee.



(a) Overview (Block diagram) (b) Directional Coupler (c) Target Board

Figure 5: Setup I. (a) Block diagram of the preliminary setup for verifying the feasibility of Active EMA. (b) Reflected waves are observed separately using a coupler. (c) EM waves are irradiated from the DC adapter of the target cryptographic device to generate reflected waves.

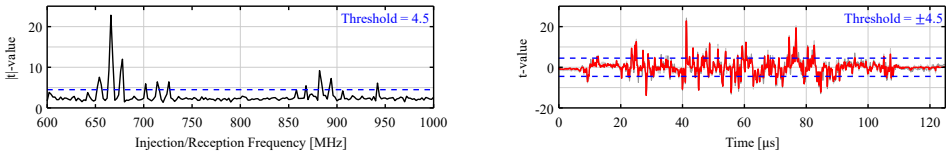


(a) Overview (Block diagram) (b) Photo

Figure 6: Setup II. Block diagram and photo of setup for verifying whether Active EMA is feasible against cryptographic devices installed within security boundaries. The cryptographic device was installed inside a shielded box. Power cables were connected to the device, and assuming an attacker can only access the primary side of the AC/DC adapter, injection probes and current probes were installed there. Additionally, the power cables were clamped with two ferrite cores.

Setup II: This setup instantiates the threat model of Section 3. The cryptographic device was installed inside a shielded box (Micronix, MY1510), with only the power and communication cables exposed, mimicking the inevitable apertures of a security boundary. To suppress leakage through these apertures, two high-frequency ferrite cores (TDK: ZCAT3035-1330) were clamped on the power cable, and a 5 V AC/DC adapter was used to further attenuate coupling toward the primary side. Due to enclosure size limits, the AC/DC adapter and ferrites were placed outside; to avoid unintentionally simplifying the scenario, the injection probe was positioned $\approx$ 1 m away on the AC/DC adapter. Under this configuration, the attacker cannot physically access the inside of the boundary, and passive EMA from outside the boundary fails (Section 5.4). Therefore, it was assumed that the attacker could only access the power cable exposed outside the boundary and execute Active EMA from there.

An Injection Probe (Fischer Custom Communications: F-140) was used to inject EM waves into the AC power cable, clamping the power lines to apply CM current. A Current Probe (Fischer Custom Communications: F-2000) was used to measure the reflected waves, clamping the power lines to observe DM current, thereby suppressing self-interference of EM waves injected from the transmitter. The probes were positioned 3.8 meters and 2.3 meters away from the cryptographic device, respectively. A signal amplifier (R&K: A030k102-3040R) with a 30 dB gain was used to increase irradiation intensity.



(a) Leakage Channel search results

(b) TVLA results at 664 MHz

Figure 7: (a) Results of relay channel search conducted on CW308T-XMEGA mounted on CW308 UFO using **Setup I**. TVLA was performed with $2N = 100,000$ traces at each frequency. Several frequency bands exceeding the t-value threshold of 4.5 were observed, (b) with the highest value of 22.8 observed at 664 MHz.

5.2 Relay Channel Search

Assuming a scenario where attackers can obtain the same device as the target device to perform profiling, we performed a frequency characterization of the relay channel, as shown in algorithm 1, using **Setup I**. Search parameters were: the intensity of signal generator $P_{\mathrm{TX}} = 5$ dBm, search frequency range $(f_{\mathrm{start}}, f_{\mathrm{end}}, f_{\mathrm{step}}) = (600\,\mathrm{MHz}, 1000\,\mathrm{MHz}, 2\,\mathrm{MHz})$. Measurements were conducted with $2N$ = 100,000 traces for TVLA, using fixed vs. random plaintext. Amplitude demodulation was applied as preprocessing, with HPF and LPF applied with cutoff frequencies $f_{\mathrm{cutoff,HPF}} = 30\,\mathrm{kHz}$, $f_{\mathrm{cutoff,LPF}} = 3\,\mathrm{MHz}$. Outlier removal was not performed due to the minimal influence of external noise in close-range measurements via a coaxial cable.

Figure 7 shows the relay channel leakage characterization results. In Figure 7(a), the vertical axis t-value is shown in absolute value notation to confirm the presence or absence of leakage. Frequency bands exceeding the t-value of $|t| > 4.5$ were observed, confirming the existence of frequency bands where side-channel information can be observed through Active EMA. Specifically, leakage was confirmed in the ranges of 650 MHz to 670 MHz and 850 MHz to 900 MHz, with the highest t-value (22.8) obtained at 664 MHz. Figure 7(b) shows the TVLA results with a 664 MHz irradiation and reception frequency. The horizontal axis represents the time index, the vertical axis represents the t-value, and multiple points where $|t| > 4.5$ were observed. Furthermore, to assess reproducibility, we repeated the profiling experiment (**Setup I**) on two CW308T-XMEGA target boards and two CW308 UFO base boards from the same manufacturer (four boards in total). The frequency bands with strong relay-channel characteristics, including the peak near 664 MHz, were consistent across these boards, demonstrating reproducibility and feasibility of the profiling procedure. The security-boundary experiment (**Setup II**) was performed on one board combination, yielding consistent results under shielded and filtered conditions.

5.3 Key Recovery from Outside PCB

We examined the possibility of AES key recovery through Active EMA using **Setup I**. Based on the relay channel search results from Section 5.2, the irradiation and reception frequency were set to $f_{\mathrm{c}} = 664\,\mathrm{MHz}$. The intensity of the signal generator was set to $P_{\mathrm{TX}} = 5$ dBm. As in the previous experiment, amplitude demodulation was applied as preprocessing to the acquired traces, without applying outlier removal, and HPF and LPF were applied with cutoff frequencies $f_{\mathrm{cutoff,HPF}} = 30\,\mathrm{kHz}$, $f_{\mathrm{cutoff,LPF}} = 3\,\mathrm{MHz}$. Acquired traces are shown in Figure 8. Time variations in impedance accompanying AES computational processing were observed.

Next, we collected $N = 500,000$ traces and performed CPA; all 16 bytes of the AES secret keys were recovered. CPA results for each byte are summarized in Appendix B. Figure 9 shows CPA results targeting the 5th byte. Figure 9(a) shows correlation values

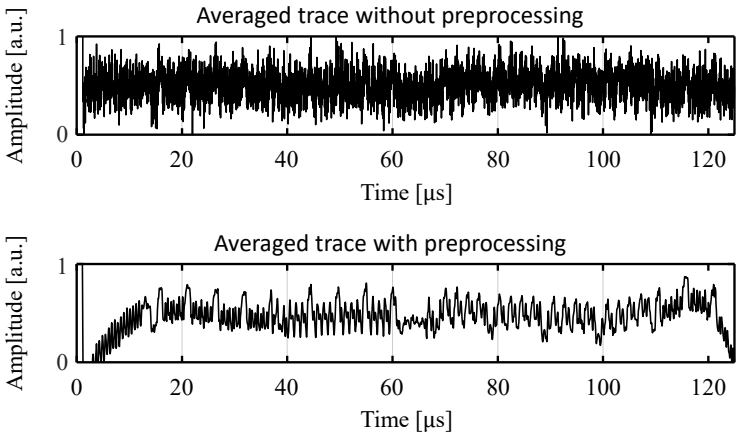
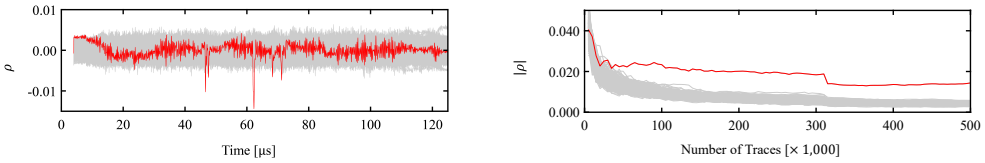


Figure 8: Traces measured with irradiation and reception frequency $f_c = 664\,\text{MHz}$ with **Setup I**. Averaged over 2,000 traces to clarify the waveform outline. Averaged waveforms were not used in CPA. (top) Waveform without preprocessing applied, (bottom) Waveform with HPF and LPF applied.



(a) Time vs Correlation Coefficient

(b) Number of Trace vs Correlation Coefficient

Figure 9: CPA attack results when executing Active EMA with **Setup I** (5th byte). All 16 bytes of AES secret keys were recovered. Irradiation and reception frequency is $f_c = 664\,\text{MHz}$, number of traces is $N = 500,000$ traces. The red line shows the correlation value of the correct key.

for 256 key candidates against the time index, and Figure 9(b) shows correlation values for 256 key candidates against the number of traces used in the analysis. These results demonstrate that leakage can be induced through Active EMA and that secret keys can be recovered.

5.4 CPA Results from the Primary Side

This section demonstrates the possibility of AES key recovery through Active EMA from the primary side of AC/DC adapters under the measurement environment of **Setup II**. This demonstrates that side-channel information can be leaked outside security boundaries through the relay mechanism, crossing boundaries formed by shielded boxes. This setup presents the following challenges arising from physical security boundaries: (1) Because injection probes and current probes are used to inject and observe EM waves non-invasively and without physical contact, EM waves do not propagate efficiently. (2) EM wave propagation to cryptographic devices inside security boundaries formed by shielded boxes. (3) Signal attenuation and multipath reflections introduced by ferrite cores, AC/DC adapters, and long transmission lines. (4) Increased self-interference caused by high-intensity EM-wave irradiation. Due to these factors, the acquisition of side-channel information confined within boundaries becomes more difficult compared to **Setup I**.

Based on the profiling results from Section 5.2, the irradiation and reception frequencies

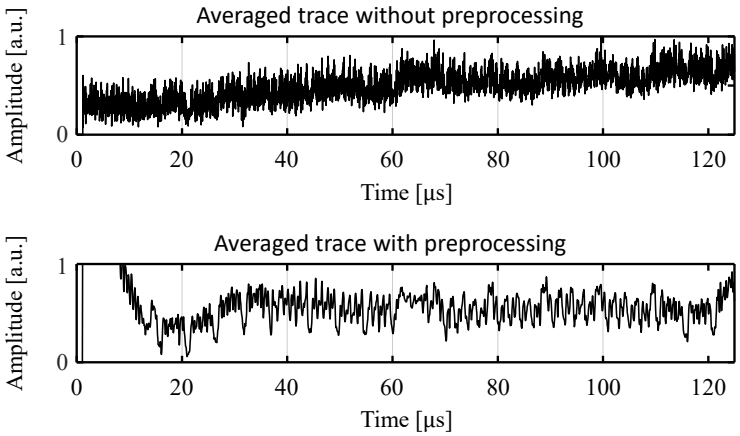


Figure 10: Traces measured from primary side with irradiation and reception frequency $f_c = 664\,\text{MHz}$ with **Setup II**. Averaged over 10,000 traces to clarify the waveform outline. Averaged waveforms were not used in CPA. (top) Waveform without preprocessing applied, (bottom) Waveform with outlier removal, HPF, and LPF applied.

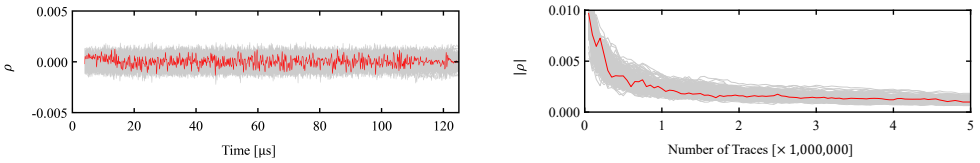
were set to $f_c = 664\,\text{MHz}$. The intensity of the signal generator output was set to $P_{TX} = 17$ dBm and amplified to approximately 47 dBm by the amplifier. The acquired traces were preprocessed using amplitude demodulation, and traces containing surge noise were removed by outlier removal with threshold $k = 1.2$. Afterwards, HPF and LPF with cutoff frequencies $f_{\text{cutoff,HPF}} = 30\,\text{kHz}$, $f_{\text{cutoff,LPF}} = 3\,\text{MHz}$ were applied. A total of $N = 5,000,000$ traces were collected.

To establish the effectiveness of our active attack, we start by performing a passive attack under the same measurement conditions. In this scenario, we do not irradiate EM waves, but only passively capture EM emanations (with the receiver gain maximized) from the device. In this scenario, we were unable to recover any AES key bytes. For example, Figure 11 shows attack results targeting the 5th byte. Notably, even when the number of traces used for the attack is increased to 5,000,000, the correlation value of the correct key indicates that there is no prospect of extracting the key (Figure 11(b)). This shows that the side-channel information is confined within the physical security boundaries achieved by measures such as ferrite cores and a shielded enclosure. Detailed results are shown in Appendix C.

Next, we conducted our proposed active attack. 5.42% (270,873 traces) of all traces were detected as abnormal traces by outlier removal. In subsequent analysis, the remaining 94.58% (4,729,127) of traces were used. Abnormal traces showed surge-like noise with rapid amplitude changes at specific timings, likely caused by unintended modulation from surrounding electronic device operations or external noise superimposition on power lines. Figure 10 shows traces before and after the preprocessing. Time variations in impedance accompanying AES computational processing were observed outside security boundaries through the relay channel.

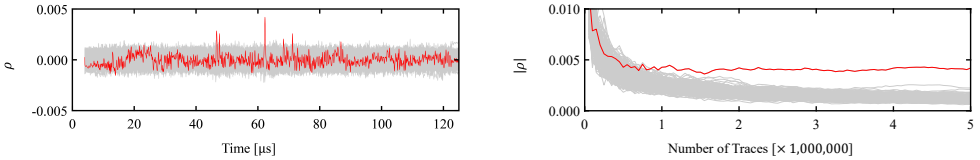
We performed CPA using $N = 5,000,000$ traces[11], and were able to recover all 16 bytes of the AES secret key. CPA attack results for each byte are shown in Appendix C. Figure 12 shows CPA attack results targeting the 5th byte. Figure 12(a) shows correlation values of 256 key candidates against the time index, and Figure 12(b) shows correlation values of 256 key candidates against the number of traces. In contrast to the passive EMA

[11] Here, $N = 5,000,000$ traces is the total number of observations, including abnormal traces removed by outlier removal. For fair evaluation of attack performance, we use "number of traces observed" by the attacker as the evaluation criterion. Actually, $N = 4{,}729{,}127$ traces were used for CPA.



(a) Time vs Correlation Coefficient (b) Number of Trace vs Correlation Coefficient

Figure 11: CPA attack results when executing conventional passive EMA in **Setup II** (5th byte). We cannot extract even one subkey using 5,000,000 traces. Therefore, physical security measures could suppress leakage across the boundary.



(a) Time vs Correlation Coefficient (b) Number of Trace vs Correlation Coefficient

Figure 12: CPA attack results when executing Active EMA in **Setup II** (5th byte). We recovered all 16 bytes of the AES secret key. Irradiation and reception frequency were $f_c = 664\,\text{MHz}$, the number of traces was 5,000,000 traces. The red line shows the correlation value of the correct key.

results, the correlation value of the correct subkey is highest when using approximately 1,000,000 traces or more for CPA. Although the measurement took several days, key recovery was achieved without being affected by temperature changes or environmental changes, even in long-term measurements.

5.5 Controllability of Leakage Intensity

The experiments up to the previous section demonstrated that Active EMA can leak side-channel information beyond security boundaries. This section verifies another important characteristic of Active EMA: controllability of leakage intensity. In conventional passive measurement, the intensity of leaking EM waves depends on the implementation and design of cryptographic devices and cannot be controlled by attackers. In contrast, Active EMA enables attackers to actively control leakage by adjusting the intensity and frequency of irradiated EM waves.

In this experiment, we used **Setup I**, which uses coaxial cables and couplers to accurately separate incident and reflected waves, allowing pure evaluation of reflected wave effects with less external noise influence for high reproducibility and more quantitative evaluation of Active EMA attack accuracy. In the experiment, the signal generator irradiation intensity was varied as $P_{\text{TX}} = 0\,\text{dBm}$, $5\,\text{dBm}$, $10\,\text{dBm}$, $12\,\text{dBm}$, and CPA attacks were performed under each condition. The receiver gain was adjusted to avoid saturation at each irradiation intensity, with gains set to 17.0, 12.5, 7.0, and 5.0, respectively, for each irradiation intensity within the USRP N210 gain setting range (0∼32). This systematic gain adjustment ensures optimal measurement conditions at each irradiation intensity for fair comparison.

Figure 13 shows key recovery rates when varying irradiation intensity. The horizontal axis represents the number of traces, and the vertical axis represents the number of correctly recovered key bytes (maximum 16 bytes). Results confirmed that key estimation accuracy significantly improved with increased irradiation intensity. Specifically, comparing the

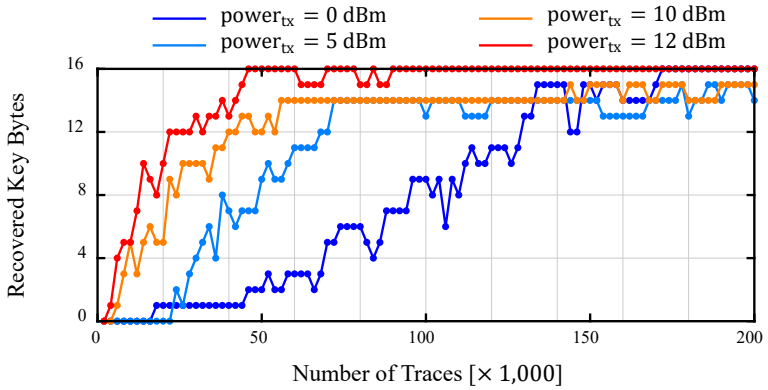


Figure 13: Number of traces required to recover the secret key for multiple irradiation intensities. An increasing irradiation intensity enables key recovery using fewer traces. This is because higher irradiation intensity improves reflected wave intensity, enabling acquisition of higher signal-to-noise ratio traces.

number of traces required to recover full 16 bytes of keys, approximately 50,000 traces were needed at 12 dBm irradiation intensity, while approximately 175,000 traces were required at 0 dBm, a 3.5-fold difference.

In contrast to traditional passive measurements, Active EMA allows control of the leaked signal intensity. Attackers can obtain higher signal-to-noise ratio traces by increasing the radiation intensity. This lets them extend the distance over which the attack can be performed [KFKH23, PLHD25, KFH19]. We use this control feature when we discuss extending attack distance by increasing the irradiation intensity in Section 6.2. On the other hand, practical constraints also exist on irradiation intensity. Excessive irradiation may cause interference or disturbance to cryptographic devices, so attackers need to set the irradiation intensity within the range where the target devices maintain regular operation. In this experimental environment, no communication errors or cryptographic operation errors were observed even when increasing irradiation intensity to 15 dBm in **Setup I**. Still, this upper limit is expected to vary depending on device implementation and environmental conditions.

In Section 5, the experimental results demonstrated that even against cryptographic devices where security boundaries are formed by physical security measures such as shielded enclosures and filters, making attacks difficult with conventional passive measurement, Active EMA based on the relay mechanism can actively leak side-channel information beyond security boundaries, enabling secret key recovery. Furthermore, as shown in Section 5.5, Active EMA enables attackers to intentionally control the leakage intensity by adjusting the irradiation intensity, allowing for the optimization of attack efficiency. This controllability and reproducibility demonstrate that Active EMA is not merely a theoretical threat, but an attack method that can be systematically executed in real-world environments, emphasizing its importance as a new threat model to consider in physical security evaluations.

6 Countermeasures and Future Challenges

In this section, we discuss countermeasures against Active EMA (Section 6.1) and then outline future research directions, including spatial radiative attacks, extended attack distance, and improvements in measurement and analysis performance (Section 6.2).

6.1 Countermeasures against Active EMA

This section discusses physical security measures against Active EMA. Active EMA is established through a relay mechanism, and since impedance variations of nonlinear elements in the First Relay Channel are difficult to suppress, countermeasures against active EM measurement in the Second Relay Channel seem more promising. As shown in Section 5.4, physical security measures designed to suppress leakage can be bypassed. On the other hand, monitoring systems to detect irradiation of EM waves might be effective.

EM fault sensors implement voltage and EM field sensors within cryptographic ICs to detect external EM waves [MNH+16, FHB+18, ZDT+14]. They can detect continuous waves in the hundreds of MHz band and high-intensity EM waves of 47 dBm used in Active EMA, preventing information leakage by stopping cryptographic processing or switching to dummy operations. However, technical extensions from conventional EM pulse wave assumptions to continuous wave support are necessary.

Intentional Electromagnetic Interference (IEMI) detectors have broadband monitoring and direction-of-arrival estimation capabilities [GT04, BRS22, KRS25], and can detect Active EMA-specific patterns such as frequency searches from 600 MHz to 1 GHz and long-duration continuous irradiation. They can learn environmental noise levels and identify low-power continuous waves that do not damage equipment.

Tamper detection using radio frequencies continuously monitors the EM environment within protected areas [STZP22, TKS+25], detecting environmental changes and changes in reflection characteristics caused by injected EM waves. Combination with on-chip impedance measurement [MST22] can also be effective. By combining these countermeasures, a multi-layered defense that effectively detects and prevents channel creation by active EM measurement can be established.

6.2 Future Research Directions

While our experiments demonstrate Active EMA through conductive paths, extending to spatial radiative paths is a natural next step. In through-wall or through-enclosure scenarios, barrier attenuation and multipath interference are key challenges; they may be mitigated by appropriate frequency selection for penetration and by using directional antennas to suppress unintentional reflections. Prior studies also demonstrated that power and interface cables outside the boundary can act as unintentional antennas that receive and re-radiate injected EM waves, enabling radiative leakage channels [KFKH23, PLHD25].

Extending attack distance is also a significant challenge. Based on the relationship between irradiation intensity and key recovery rate shown in Section 5.5, attacks from distances of tens of meters or from adjacent rooms may be possible. However, solving self-interference problems due to increased distance requires complete separation of transmission and reception systems.

Performance improvement is also a challenge. Our attack required 10^3 to 10^5 times more traces than conventional power analysis. Adoption of multi-band measurements [GPNS25] and high-performance receivers is expected to improve the overall measurement quality. For the analysis aspects, using both the amplitude and phase information [AHC+24] and applying deep learning [MPP16] techniques are also expected to improve the results. Similar to the development process of Screaming Channels [CPM+18, CFS20, GPNS25], systematic development of measurement and analysis systems for Active EMA will improve the overall results and will further increase our understanding of an attacker's capabilities.

The decoupling network affects Active EMA in two opposing ways. First, lowering the PDN impedance reduces ground bounce, which disfavors both passive and active measurements. Second, Class II MLCCs can form new Relay Points because their effective capacitance depends on DC/AC bias, which can change the modulation depth and the most favorable carrier band. Disentangling these effects requires a board redesign and

DC/AC-bias characterization as discussed in [NWM+11], which we leave for future work. Our results in Section 5 indicate that, despite decoupling, Active EMA remains effective under the default configuration.

7 Conclusion

This research demonstrates that secret key recovery is possible through active EM side-channel measurements (Active EMA). Our technique uses a relay mechanism that is effective against cryptographic devices with physical security boundaries. The proposed method is based on the principle that ground bounce in cryptographic ICs affects the impedance of peripheral nonlinear elements (First Relay Channel), and EM waves irradiated by attackers are modulated by these impedance variations and leak outside the boundary as reflected waves (Second Relay Channel).

To demonstrate the effectiveness of our technique, we performed an active EM side-channel attack from the primary side of an AC/DC adapter. This was achieved while the target device was placed in a shielded enclosure and protected by ferrite core filters. We showed that attacks can be realized through active EM measurement in environments where SCA was infeasible with conventional passive measurements. Furthermore, we demonstrated that attackers can control the leakage intensity by adjusting the irradiation intensity, demonstrating that Active EMA is a practical attack method that can be systematically executed.

Future challenges include realizing attacks through spatial emission paths, extending to attacks from long distances, and improving performance through multi-band measurement and deep learning-based analysis.

As countermeasures, a multi-layered defense is effective, including the implementation of EM fault sensors and IEMI detectors with continuous wave detection capabilities, and prevention of relay channel generation by monitoring impedance variations.

This research suggests the necessity of considering active EM measurement in addition to conventional passive threat models in physical security evaluation. Particularly in mission-critical systems such as ATMs, infrastructure control systems, and HSMs, countermeasures against new attack paths through inevitable apertures in security boundaries are needed. Active EMA is not merely a theoretical threat, but an attack method that can be executed in real-world environments, calling for the establishment of new security evaluation standards.

Acknowledgments

This work was supported by JSPS KAKENHI (Grant Numbers JP23H00472 and JP23K28087), the JST FOREST Program (Grant Number JPMJFR206L), the JSPS Grant-in-Aid for JSPS Fellows (Grant Number JP23KJ1593), the Flemish Government through the Cybersecurity Research Program (Grant Number VOEWICS02), and the European Commission through the Horizon 2020 research and innovation program under grant agreement Belfort ERC Advanced Grant 101020005 695305. This work was also conducted as part of the JSPS Overseas Challenge Program for Young Researchers, and the authors are grateful for its support.

References

[AARR03] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The EM side—channel(s). In *Cryptographic Hardware and Embedded Systems*

- *CHES 2002*, Lecture notes in computer science, pages 29–45. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[AGR24] Md Sadik Awal, Buddhipriya Gayanath, and Md Tauhidur Rahman. Impedance vs. power side-channel vulnerabilities: A comparative study. *arXiv preprint arXiv:2405.06242*, 2024.

[AHC+24] Pierre Ayoub, Aurélien Hernandez, Romain Cayre, Aurélien Francillon, and Clémentine Maurice. PhaseSCA: Exploiting phase-modulated emanations in side channels. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(1):392–419, dec 2024.

[AJCZ19] Sinan Adibelli, Prateek Juyal, Chia-Lin Cheng, and Alenka Zajic. Terahertz near-field focusing using a 3-D printed cassegrain configuration for backscattered side-channel detection. *IEEE Trans. Antennas Propag.*, 67(10):6627–6638, October 2019.

[BRS22] Ajay Kumar Bellamkonda, Patnam Hanumantha Rao, and Saurabh Saxena. Intentional electromagnetic interference reception in 0.5–2.0 GHz. *IEEE Trans. Electromagn. Compat.*, 64(6):2163–2169, December 2022.

[CFS20] Giovanni Camurati, Aurélien Francillon, and François-Xavier Standaert. Understanding screaming channels: From a detailed analysis to improved attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 358–401, jun 2020.

[Com22] Common Criteria Recognition Arrangement. Common criteria for information technology security evaluation – part 2: Security functional components (CC:2022 revision 1). Technical report, Common Criteria Recognition Arrangement (CCRA), November 2022.

[CPM+18] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 163–177, New York, NY, USA, 2018. ACM.

[dMSV20] Pieterjan de Meulemeester, Bart Scheers, and Guy A E Vandenbosch. Eavesdropping a (ultra-)high-definition video display from an 80 meter distance under realistic circumstances. In *2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)*, pages 517–522. IEEE, July 2020.

[FHB+18] Daisuke Fujimoto, Yu-Ichi Hayashi, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede. Detection of IEMI fault injection using voltage monitor constructed with fully digital circuit. In *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*. IEEE, May 2018.

[GJJR11] Gilbert Goodwill, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi. A testing methodology for side-channel resistance validation. In *NIST Non-Invasive Attack Testing (NIAT) Workshop*. csrc.nist.gov, 2011.

[GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems — CHES 2001*, volume 2162 of *Lecture notes in computer science*, pages 251–261. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.

[GPNS25] Jeremy Guillaume, Maxime Pelcat, Amor Nafkha, and Rubén Salvador. Multi-screaming-channel attacks: Frequency diversity for enhanced attacks. *arXiv [cs.CR]*, apr 2025.

[GPT15] Daniel Genkin, Itamar Pipman, and Eran Tromer. Get your hands off my laptop: physical side-channel key-extraction attacks on PCs: Extended version. *J. Cryptogr. Eng.*, 5(2):95–112, June 2015.

[GS22] Jan Sebastian Götte and Björn Scheuermann. Can't touch this: Inertial hsms thwart advanced physical attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 69–93, 2022.

[GT04] D V Giri and F M Tesche. Classification of intentional electromagnetic environments (IEME). *IEEE Trans. Electromagn. Compat.*, 46(3):322–328, August 2004.

[HB25] Vedad Hadžic and Roderick Bloem. Efficient and composable masked aes s-box designs using optimized inverters. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(1):656–683, 2025.

[HHM+13] Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. *IEEE Trans. Electromagn. Compat.*, 55(3):571–580, June 2013.

[HMF07] Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and EM attacks on passive 13.56 MHz RFID devices. In *Cryptographic Hardware and Embedded Systems - CHES 2007*, Lecture notes in computer science, pages 320–333. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[HSK+10] Yu-Ichi Hayashi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, Takaaki Mizuki, Akashi Satoh, Takafumi Aoki, Shigeki Minegishi, Hideaki Sone, and Hiroshi Inoue. Information leakage from cryptographic hardware via common-mode current. In *2010 IEEE International Symposium on Electromagnetic Compatibility*, pages 109–114. IEEE, July 2010.

[IMK+25] Hayato Ide, Shohei Matsumoto, Taiki Kitazawa, Shugo Kaji, Daisuke Fujimoto, Takashi Kasuga, and Yuichi Hayashi. Amplifying electromagnetic leakage by hardware trojans through cable geometry manipulation. In *2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 261–267. IEEE, may 2025.

[Int15] International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). K.115: Mitigation methods against electromagnetic security threats, 2015.

[ION+18] Vincent Immler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke, Jinyu Lee, Yak Peng Lim, Wei Koon Oh, Keng Hoong Wee, and Georg Sigl. Secure physical enclosures from covers with tamper-resistance. *TCHES*, pages 51–96, 2018.

[KAK+22] Taiki Kitazawa, Kimihiro Arai, Youngwoo Kim, Daisuke Fujimoto, and Yuichi Hayashi. A novel remote visualization of screen images against high-resolution display with divided screens focusing on the difference of transfer function of multiple emanations. *IEEE Trans. Electromagn. Compat.*, 64(6):1941–1948, December 2022.

[KFH19] Masahiro Kinugawa, Daisuke Fujimoto, and Yuichi Hayashi. Electromagnetic information extortion from electronic devices using interceptor and its countermeasure. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 62–90, aug 2019.

[KFH24] Taiki Kitazawa, Daisuke Fujimoto, and Yuichi Hayashi. Fundamental study on simple power analysis using backscattering from switching regulators. In *2024 International Symposium on Electromagnetic Compatibility – EMC Europe*, pages 22–26. IEEE, sep 2024.

[KFKH23] Shugo Kaji, Daisuke Fujimoto, Masahiro Kinugawa, and Yuichi Hayashi. Echo TEMPEST: EM information leakage induced by IEMI for electronic devices. *IEEE Trans. Electromagn. Compat.*, 65(3):655–666, June 2023.

[KJJ99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology — CRYPTO' 99*, Lecture notes in computer science, pages 388–397. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[KOP09] Timo Kasper, David Oswald, and Christof Paar. EM side-channel attacks on commercial contactless smartcards using low-cost equipment. In *Information Security Applications*, Lecture notes in computer science, pages 79–93. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[KRS25] Pallepogu Prasanna Kumar, Patnam Hanumantha Rao, and Saurabh Saxena. Design and analysis of 0.5–2.0 GHz RF frontend subsystems for IEMI applications. *IEEE Trans. Electromagn. Compat.*, 67(1):237–246, February 2025.

[Kuh05] Markus G Kuhn. Security limits for compromising emanations. In *Cryptographic Hardware and Embedded Systems – CHES 2005*, Lecture notes in computer science, pages 265–279. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[LDMPT15] J Longo, E De Mulder, D Page, and M Tunstall. SoC it to EM: ElectroMagnetic side-channel attacks on a complex system-on-chip. In *Lecture Notes in Computer Science*, Lecture notes in computer science, pages 620–640. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[MMT23] Saleh Khalaj Monfared, Tahoura Mosavirik, and Shahin Tajik. Leakyohm: Secret bits extraction using impedance analysis. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 1675–1689, 2023.

[MNH+16] Noriyuki Miura, Zakaria Najm, Wei He, Shivam Bhasin, Xuan Thuy Ngo, Makoto Nagata, and Jean-Luc Danger. PLL to the rescue: a novel EM fault countermeasure. In *Proceedings of the 53rd Annual Design Automation Conference*, New York, NY, USA, jun 2016. ACM.

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Springer, New York, NY, 2007 edition, mar 2007.

[MPP16] Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff. Breaking cryptographic implementations using deep learning techniques. In *Security, Privacy, and Applied Cryptography Engineering*, Lecture notes in computer science, pages 3–26. Springer International Publishing, Cham, 2016.

[MST22] Tahoura Mosavirik, Patrick Schaumont, and Shahin Tajik. ImpedanceVerif: On-chip impedance sensing for system-level tampering detection. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 301–325, nov 2022.

[Nat01] National Institute of Standards and Technology. Security requirements for cryptographic modules (FIPS PUB 140-2). Technical report, U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, May 2001.

[Nat19] National Institute of Standards and Technology. Security Requirements for Cryptographic Modules (FIPS PUB 140-3). Technical Report FIPS PUB 140-3, U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 2019.

[NWM+11] Istvan Novak, Kendrick Barry Williams, Jason R. Miller, Gustavo Blando, and Nathaniel Shannon. Dc and ac bias dependence of capacitors including temperature dependence. In *Proceedings of DesignCon East 2011*, Santa Clara, CA, 2011. DesignCon.

[OC14] Colin O'Flynn and Zhizhang Chen. ChipWhisperer: An open-source platform for hardware embedded security research. In *Constructive Side-Channel Analysis and Secure Design*, Lecture notes in computer science, pages 243–260. Springer International Publishing, Cham, 2014.

[O'F24] Colin O'Flynn. Phase modulation side channels: Jittery JTAG for on-chip voltage measurements. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024(4):382–424, sep 2024.

[OI18] Johannes Obermaier and Vincent Immler. The past, present, and future of physical security enclosures: From battery-backed monitoring to PUF-based inherent security and beyond. *J. Hardw. Syst. Secur.*, 2(4):289–296, December 2018.

[PLHD25] Lina Pu, Yu Luo, Song Han, and Junming Diao. Your cable, my antenna: Eavesdropping serial communication via backscatter signals. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 3710–3726, 2025.

[Poz21] David M Pozar. *Microwave engineering: theory and techniques*. John Wiley & Sons, New York, NY, 2021.

[PSQ07] Eric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Power and electromagnetic analysis: Improved model, consequences and comparisons. *Integration (Amst.)*, 40(1):52–60, 1 2007.

[PSS22] Clayton R Paul, Robert C Scully, and Mark A Steffka. *Introduction to electromagnetic compatibility*. John Wiley & Sons, Nashville, TN, 3 edition, 7 November 2022.

[QS01] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic analysis (EMA): Measures and counter-measures for smart cards. In *Smart Card Programming and Security*, Lecture notes in computer science, pages 200–210. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.

[SB15] B. G. Streetman and Sanjay Banerjee. *Solid State Electronic Devices*. Pearson, Upper Saddle River, NJ, 7 edition, 2015.

[SBO+15] Daehyun Strobel, Florian Bache, David Oswald, Falk Schellenberg, and Christof Paar. Scandalee: a side-channel-based disassembler using local electromagnetic emanations. pages 139–144, 9 March 2015.

[SE07] M Swaminathan and E Engin. Power integrity modeling and design for semiconductors and systems. 2007.

[SHH+09] Takeshi Sugawara, Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, and Akashi Satoh. Mechanism behind information leakage in electromagnetic analysis of cryptographic modules. In *Information Security Applications*, Lecture notes in computer science, pages 66–78. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[SJL+21] Yin Sun, Junho Joo, Jongjoo Lee, Keeyoung Kwon, and Chulsoon Hwang. Analysis of power supply induced jitter of high speed output buffer with on-die low-dropout voltage regulator. In *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, pages 318–322. IEEE, 26 July 2021.

[SLT16] Sami Saab, Andrew Leiserson, and Michael Tunstall. Key extraction from the primary side of a switched-mode power supply. In *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pages 1–7. IEEE, December 2016.

[SMTG23] Kai Schoos, Sergej Meschkov, Mehdi B Tahoori, and Dennis R E Gnad. JitSCA: Jitter-based side-channel analysis in picoscale resolution. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 294–320, jun 2023.

[SSS+13] Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, and Takeshi Fujino. On measurable side-channel leaks inside ASIC design primitives. In *Cryptographic Hardware and Embedded Systems - CHES 2013*, Lecture notes in computer science, pages 159–178. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[STZP22] Paul Staat, Johannes Tobisch, Christian Zenger, and Christof Paar. Anti-tamper radio: System-level tamper detection for computing systems. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1722–1736. IEEE, May 2022.

[TG07] Stefan Tillich and Johann Großschädl. Power analysis resistant aes implementation with instruction set extensions. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 303–319. Springer, 2007.

[TKS+25] Maryam Shaygan Tabar, Johannes Kortz, Paul Staat, Harald Elders-Boll, Christof Paar, and Christian Zenger. Anti-tamper radio meets reconfigurable intelligent surface for system-level tamper detection. *arXiv [cs.CR]*, mar 2025.

[vE85] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Comput. Secur.*, 4(4):269–286, December 1985.

[Wei00] Steve H Weingart. Physical security devices for computer subsystems: A survey of attacks and defenses. In *Cryptographic Hardware and Embedded Systems — CHES 2000*, Lecture notes in computer science, pages 302–317. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[WPZ22] Frank T Werner, Milos Prvulovic, and Alenka Zajić. Detection of recycled ics using backscattering side-channel analysis. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 30(9):1244–1255, 2022.

[ZDT+14] Loic Zussa, Amine Dehbaoui, Karim Tobich, Jean-Max Dutertre, Philippe Maurine, Ludovic Guillaume-Sage, Jessy Clediere, and Assia Tria. Efficiency of a glitch detector against electromagnetic fault injection. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014*, New Jersey, 2014. IEEE Conference Publications.

Appendix

A Outlier Removal

Using the variance value of each trace as an indicator, anomaly detection and removal of traces are performed using the IQR. Let traces be $L_i = (l_{i1}, l_{i2}, \ldots, l_{iN})$, $i = 1, 2, \ldots, M$, and the variance value of each trace be σ_i^2. The quartiles and their IQR are calculated as follows, and outlier thresholds are set.

$$Q_1 = \mathrm{Percentile}_{25}\left(\{\sigma_i^2\}_{i=1}^{M}\right), \quad Q_3 = \mathrm{Percentile}_{75}\left(\{\sigma_i^2\}_{i=1}^{M}\right), \quad \mathrm{IQR} = Q_3 - Q_1. \tag{7}$$

$$Lower_{\mathrm{th}} = Q_1 - k \cdot \mathrm{IQR}, \qquad Upper_{\mathrm{th}} = Q_3 + k \cdot \mathrm{IQR}, \tag{8}$$

where k is an arbitrary constant. Using these thresholds, only normal traces L_{normal} are extracted.

$$L_{\mathrm{normal}} = \{\, X_i \mid i \in \mathcal{N}\}, \quad \mathcal{N} = \{\, i \mid Lower_{\mathrm{th}} \leq \sigma_i^2 \leq Upper_{\mathrm{th}}\} \tag{9}$$

B CPA from outside PCB (Setup I)

Figure 14 shows the analysis results for all subbytes in the CPA attack through Active EMA in Section 5.3. The display area of results is set to 300 indices (12 μs) before and after the Point of Interest (POI) calculated by performing Known Answer Test (KAT) using Active EMA traces executed with $P_{\mathrm{TX}} = 12$ dBm in Section 5.5.

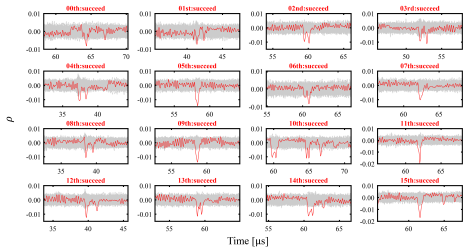
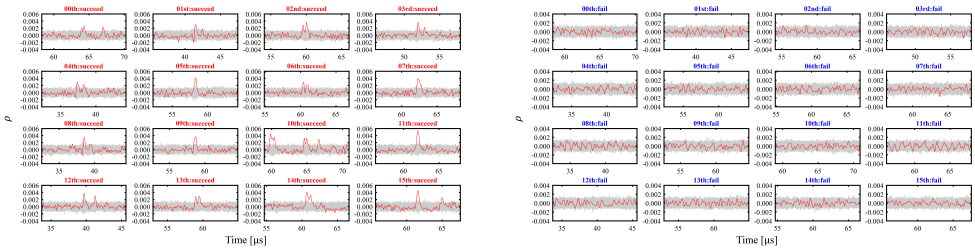


Figure 14: CPA results when executing Active EMA in **Setup I**. Irradiation and reception frequency is $f_{\mathrm{c}} = 664\,\mathrm{MHz}$, number of traces is $N = 500\,\mathrm{k}$. The red line shows the correlation value of the correct key.

C CPA from Primary Side (Setup II)

Figure 15(a) shows the analysis results for all subbytes in the CPA attack through Active EMA in Section 5.4. The display area of results is set to 300 indices (12 μs) before and after the PoI calculated by performing KAT using Active EMA traces executed with $P_{\mathrm{TX}} = 12$ dBm in Section 5.5.

Additionally, to demonstrate that the above CPA attack results were achieved through active EM measurement, EM wave measurement was conducted with the signal generator irradiation stopped and SDR gain maximized. After measuring $5,000,000$ traces, the same signal processing as in Section 5.4 was applied, and a CPA attack was performed. As a result, passive measurement could not extract even one byte of the secret key. Figure 15(b) shows the analysis results when the CPA attack is performed.



(a) Active EMA (Proposed Method)

(b) Passive EMA (Conventional Method)

Figure 15: CPA attack results when executing EMA in **Setup II**. Frequency is $f_{\mathrm{c}} = 664\,\mathrm{MHz}$, number of traces is $N = 5,000,000$ traces. The red line shows the correlation value of the correct key.