Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers

Giovanni Camurati
EURECOM
camurati@eurecom.fr

Sebastian Poeplau
EURECOM
poeplau@eurecom.fr

Marius Muench
EURECOM
muench@eurecom.fr

Tom Hayes
EURECOM
hayes@eurecom.fr

Aurélien Francillon
EURECOM
aurelien.francillon@eurecom.fr

ABSTRACT

This paper presents a new side channel that affects mixed-signal chips used in widespread wireless communication protocols, such as Bluetooth and WiFi. This increasingly common type of chip includes the radio transceiver along with digital logic on the same integrated circuit. In such systems, the radio transmitter may unintentionally broadcast sensitive information from hardware cryptographic components or software executing on the CPU. The well-known electromagnetic (EM) leakage from digital logic is inadvertently mixed with the radio carrier, which is amplified and then transmitted by the antenna. We call the resulting leak "screaming channels". Attacks exploiting such a side channel may succeed over a much longer distance than attacks exploiting usual EM side channels.

The root of the problem is that mixed-signal chips include both digital circuits and analog circuits on the same silicon die in close physical proximity. While processing data, the digital circuits on these chips generate noise, which can be picked up by noise-sensitive analog radio components, ultimately leading to leakage of sensitive information. We investigate the physical reasons behind the channel, we measure it on several popular devices from different vendors (including Nordic Semiconductor nRF52832, and Qualcomm Atheros AR9271), and we demonstrate a complete key recovery attack against the nRF52832 chip. In particular, we retrieve the full key from the AES-128 implementation in `tinyAES` at a distance of 10 m using template attacks. Additionally, we recover the key used by the AES-128 implementation in `mbedTLS` at a distance of 1 m with a correlation attack.

Screaming channel attacks change the threat models of devices with mixed-signal chips, as those devices are now vulnerable from a distance. More specifically, we argue that protections against side channels (such as masking or hiding) need to be used on this class of devices. Finally, chips implementing other widespread protocols (e.g., 4G/LTE, RFID) need to be inspected to determine whether they are vulnerable to screaming channel attacks.

CCS '18, October 15–19, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-5693-0/18/10…$15.00
https://doi.org/10.1145/3243734.3243802

KEYWORDS

Electromagnetic side channels; Mixed-signal chips

ACM Reference Format:
Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. 2018. Screaming Channels:, When Electromagnetic Side Channels Meet Radio Transceivers. In *2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), October 15–19, 2018, Toronto, ON, Canada.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3243734.3243802

1 INTRODUCTION

The drive for ever smaller and cheaper components in microelectronics has popularized so-called *mixed-signal circuits* (i.e., circuits in which analog and digital circuitry reside on the same piece of silicon, called a *die*). A typical example is a WiFi chip featuring a (digital) microcontroller as well as the (analog) radio. The special challenge of such designs is to separate the "noisy" digital circuits from the sensitive analog side of the system. In this paper we show that improper separation of digital and analog components leads to novel side-channel attacks that can break cryptography implemented in mixed-signal chips over at least 10 meters.

Modern cryptographic algorithms have been designed with a wide range of attacks in mind and are thus hardened against the more traditional ways of breaking the secrecy that cryptography is meant to provide. More recently, a lot of research attention has therefore been focused on side-channel attacks. In a side-channel scenario, attackers do not break the algorithm directly, but instead gain knowledge of the algorithm's internal state by means of observing its physical implementation; whenever such knowledge is not meant to be public, it can be used to undermine the algorithm's integrity. For example, Kocher et al. showed in 1999 that observing the power consumption of a smart card running an unprotected implementation of DES allows an attacker to guess the key, effectively breaking the cryptosystem [33]. Those results and related work spawned a long line of work on side-channel attacks against the implementations of all common cryptographic algorithms.

Measuring a system's power consumption usually requires direct physical access and potentially invasive application of probes on the power supply. A more discreet avenue of attack that has since been proved feasible are Electromagnetic (EM) attacks. Such attacks use inadvertent electromagnetic emissions that are common in digital circuitry—the key observation is that the emanations correlate with certain computations [5]. EM attacks often use specialized magnetic-field antennas in close proximity of the target chip, typically within

millimeters. In particular, the emissions of low-power devices are very weak and do not allow for attacks over larger distances.

The key observation of this paper is that in mixed-design radio chips the processor's activity leaks into the analog portion of the chip, where it is upconverted, amplified, and broadcast as part of the regular radio output. This leakage is not due to the design error of an individual vendor, but to a fundamental difficulty in designing mixed-signal chips. We show that it is possible to recover the original leaked signal and apply variations of known side-channel analysis techniques; we call our variations *Correlation Radio Analysis (CRA)* and *Template Radio Analysis (TRA)*, inspired by the corresponding classes of power and EM analysis attacks. Using the example of a commercial off-the-shelf Bluetooth device, we demonstrate that cryptographic keys can be recovered by observing the device's radio emissions in the 2.4 GHz band from a distance.

Note that our attack does not depend on the actual data that the device sends—all we need is the fact that the radio is transmitting while the processor carries out cryptographic operations. Indeed, in the context of this attack the transmitted data is considered noise that we effectively remove, whereas the side channel leak (i.e., signals correlated with the circuit's computations) is the signal we aim to recover.

In summary, our contributions are the following:

- We present a novel side channel on devices that handle sensitive information and include a radio transceiver.
- We demonstrate full key recovery up to 10 meters, a much larger distance than conventional EM side channels.
- We conduct a thorough analysis of the channel's properties and explain its origin, allowing chip designers to take the issue into consideration for future designs.
- We suggest countermeasures to protect current designs.

After examining necessary background information (Section 2) we give an overview of screaming channels (Section 3) and present our full example attack (Section 4). We then conduct a detailed analysis of the channel (Section 5) and perform additional experiments (Section 6). Finally, we discuss the implications of our work (Section 7), we place it in the context of current research (Section 8), and we conclude (Section 9).

2 BACKGROUND

In this section we provide required background information, in particular focusing on EM side-channel attacks and the challenges associated with mixed-signal circuits. We defer the detailed review of the electronic effects explaining our new side channel to Section 5.

2.1 Side channels

Cryptographic algorithms are generally subject to extensive analysis. Before an algorithm is deployed, care has to be taken that the security properties it claims actually hold. While there is rarely an unconditional proof that a given system is secure, the algorithms in mainstream use today are considered sound under certain assumptions, one of which being that potential attackers might be able to observe inputs and outputs of an algorithm but not its internal state. It is this very assumption that does not hold in the case of side-channel attacks, which can compromise a cryptosystem's integrity.

Consider the example of a symmetric cipher using an unknown key, implemented in software. An attacker may send arbitrary plaintexts to the system and observe the corresponding ciphertexts; the goal of the attack is to reveal the key. A secure system should be designed to thwart such attacks. However, suppose that the attacker gains some degree of insight into the execution of the cryptosystem's *implementation*, for example, the ability to observe the data used by the processor when executing machine code. Under such conditions it is trivial for the attacker to recover the key simply by observing the operands of the computation at the right moments. While the example is rather contrived and grants the attacker an unreasonable degree of power, it exemplifies the general principle of side-channel attacks: when the implementation of a system inadvertently leaks information about its internal state, attackers who recover such information may be able to break the system's security guarantees.

Research on the topic of side channels has revealed a variety of ways for system internals to leak to the outside. The ones most relevant to our work analyze the correlation of electromagnetic emanations with computational activity. Quisquater et al. [46] have shown that electrical switching in digital circuits induces electromagnetic emanations correlated with the data processed in the circuits. Several techniques have been developed for recovering secrets on the basis of such correlation, notably Differential EM Analysis (DEMA) and Template EM Analysis (TEMA) [5].

EM emissions are very weak in general, and exploiting them requires close proximity to the target circuit. While high-power chips (e.g., PC-class CPUs) allow side-channel attacks from distances of less than a meter [14, 25, 27, 48] this is not the case for low-power devices because the leakage is too weak. Typically, probes must be placed within millimeters of an exposed chip to capture exploitable information. The side channels we describe are very similar to EM side channels (see Section 5), but more powerful; the great advantage of screaming-channel attacks is that weak leakages are re-transmitted by the device's own transmitter and can therefore be detected and exploited from much larger distances.

2.2 Mixed-signal circuits

Though modern electronic systems rely on digital components and software to process information, they also employ analog circuitry for power and communication with the outside world. With the growth of the mobile and telecommunication markets, and with the more recent development of automotive and Internet of Things (IoT) applications, radio communications are an increasingly vital application field of analog circuitry. Though modern protocols are digital, and most of their layers are implemented in the digital domain, the generation, amplification, and radiation of radio signals are inherently analog operations. Moreover, these signals are at Radio Frequency (RF) and have particular physical properties.

Market pressure for cheaper, smaller devices and advances in microelectronics have popularized so-called mixed-signal chips, which combine the digital and analog/RF domain on a single chip (also called Radio Frequency Integrated Circuits (RFICs)). Many commercial devices use this technology, ranging from WiFi, 3G,

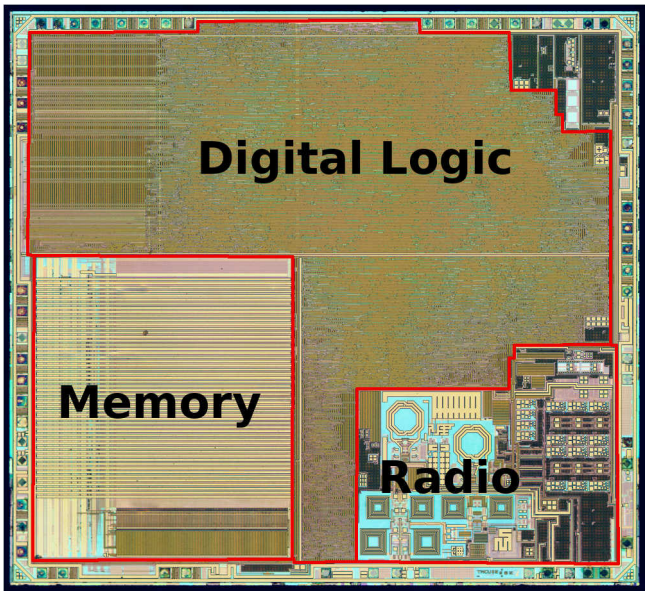


Figure 1: Labeled die picture from an nRF51822 Bluetooth LE 2.4GHz mixed-signal design chip. Digital and Analog parts of the chip can be easily distinguished (Original picture CC BY 3.0 by zeptobars [60]). This chip is very similar to the chip we use in our experiments.

and Bluetooth transceivers to GPS and TV receivers. Figure 1 shows a labeled die picture of a typical mixed-design Bluetooth chip, the nRF51822 from Nordic Semiconductor.

Integrating digital and analog microelectronic components on the same silicon die introduces design and validation challenges at multiple layers. For the purpose of this paper, the most important one is dealing with noise. Digital circuits are characterized by an intense switching activity (i.e., logic gates taking "0" and "1" values). As a consequence, sharp current variations generate noise in a wide range of frequencies. Analog/RF circuits, which operate with continuous signals, are extremely sensitive to noise. The physical proximity of digital and analog/RF components in mixed-signal circuits naturally leads to noise issues, with the digital part that acts as an aggressor of the analog one (the victim), strongly impacting its performance.[1] One of the main reasons for noise propagation is substrate coupling, where the substrate is the "bulk" silicon on which both digital and analog components are built. Designing mixed-signal chips is therefore difficult and, as a consequence, the literature on the topic is broad (see Section 8).

The side-channel attack we introduce here is based on the idea that noise coupling propagates sensitive information from the digital domain to the radio transmission chain, which broadcasts it at a much larger distance than normal EM leaks. It is interesting to note that in a mixed-signal design, the transmitter is often more exposed to noise than other analog/RF components. The reason is that radio receiver chains are very sensitive to noise and are therefore typically placed in a corner of the silicon chip, as far as possible from digital noise[52]; on the other hand, the transmit chain deals with more powerful signals that are strong enough to present a good signal-to-noise ratio (SNR) even in the presence of digital noise. However, we will show that this noise leaks sensitive information and is powerful enough to make remote side channel attacks possible.

[1] *Aggressor/victim* is the terminology commonly used in the field of Electromagnetic Compability (EMC) [43].

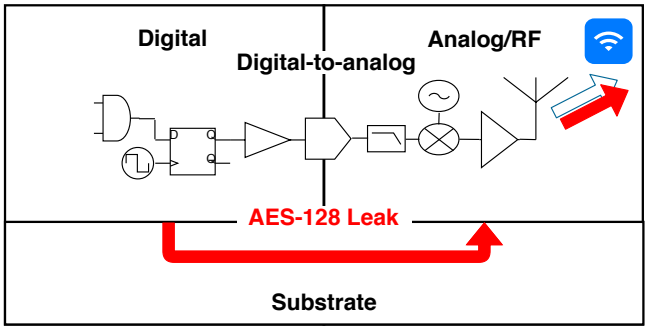


Figure 2: The noise produced by the digital circuit when executing AES-128 (red arrow) is picked up and transmitted by the analog part. It becomes part of the legitimate radio signal (blue arrow).

3 SCREAMING CHANNELS

We now introduce screaming channels by presenting the high-level concept and our observations before showing a concrete exploit in Section 4 and explaining the mechanisms underlying the channel in Section 5.

The basic intuition of screaming channels is that, when an RF circuit is placed in close proximity to digital circuitry, information on the digital circuit's operation leaks into the RF part and is broadcast along with regular transmissions. If the digital component carries out sensitive computations (e.g., cryptographic operations) the leaking information that is transmitted by the analog radio component can be sufficient to render the system vulnerable to side-channel attacks, as visualized in Figure 2.

We use a simple experiment to demonstrate the presence of the leak: While capturing the radio output of a mixed-signal chip we first configure the radio to transmit an arbitrary Bluetooth packet repeatedly; the digital part of the device is idle in this first step of the experiment. Then we start running AES, again on arbitrary data, on the microprocessor. The software-defined radio (SDR) that we use to capture the radio emissions is tuned to $f_{\text{chan}} + 2 \cdot f_{\text{clock}}$, where f_{chan} is the Bluetooth channel's center frequency (2.4 GHz) and f_{clock} the frequency of the microprocessor's clock (64 MHz). Figure 3 shows the resulting spectrogram. Even while the microprocessor is idle and only the radio is active (i.e., in the first step of the experiment) we see an "echo" of the data transmitted by the radio. (Note that the frequency we are tuned to is offset from the actual Bluetooth channel by 128 MHz.) Moreover, as soon as we run AES on the microprocessor, the spectrogram changes significantly, even allowing us to detect individual executions of the algorithm. Further analysis of those additional signal components reveals that details of the AES computations are amplitude-modulated onto the Bluetooth carrier signal, and that the leaked information is observable even

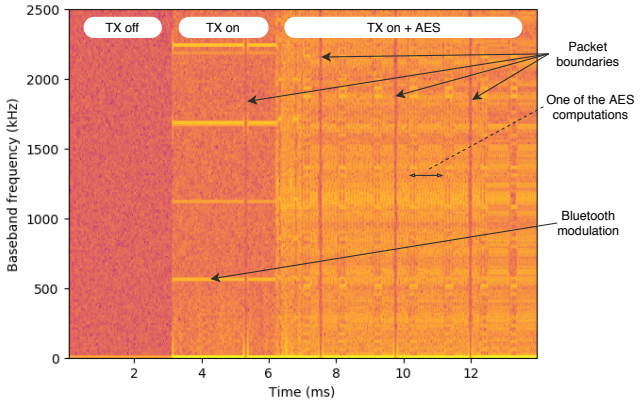


Figure 3: Spectrogram of the radio emissions from a Nordic Semiconductor nRF52832 over time, captured at 2.528 GHz with Ettus Research USRP B200 mini via cable, sampling at 5 MHz (brighter colors indicate higher signal amplitude).

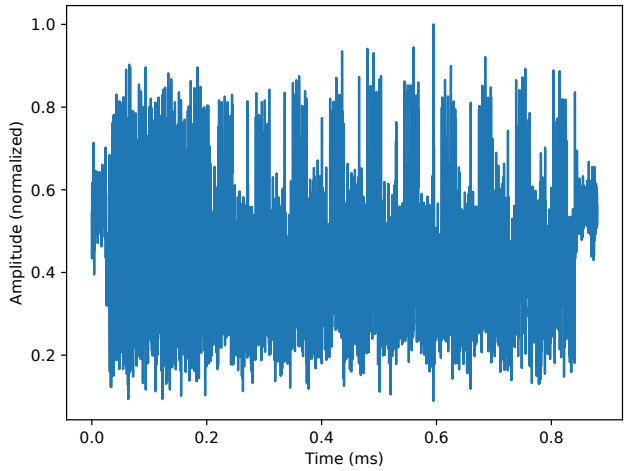


Figure 4: Time-domain signal from our target; the ten rounds of AES-128 are clearly visible.

from a distance; in the time domain, we can clearly distinguish the ten rounds of the `tinyAES` implementation of AES-128 (see Figure 4).

In order to show the sensitivity of the leaked information we demonstrate a key recovery attack in the next section; afterwards, we characterize the channel and explain the microelectronic characteristics that cause the leak.

4 COMPLETE KEY RECOVERY ATTACK

In this section we describe a full key recovery attack against AES on Nordic Semiconductor nRF52832, a commercial Bluetooth chip. The chip is used in many systems, for instance in the Rigado BDM301[2] or the RedBear BLE Nano v2[3]. The nRF52832 is commonly used in IoT

[2]FCC ID 2AA9B04, https://fccid.io/2AA9B04
[3]FCC ID 2AKGS-MBN2, https://fccid.io/2AKGS-MBN2

Figure 5: Experimental setup for a long-distance screaming-channel attack (10 m).

applications and embeds a Cortex-M4 microcontroller allowing for single chip solutions. Note, however, that our attack is not specific to this particular chip: in Section 6 we discuss other devices that are possibly vulnerable.

The goal of the attack is to recover the key of an AES computation carried out by the processor of the target chip, using only the radio signal that the chip emits and knowledge of the plaintexts. (An analogous attack can be carried out against the ciphertexts.) We first describe the experimental setup, then detail trace collection and processing, and finally show how to recover the key.

4.1 Experimental setup

The physical setup consists of two main components: the target chip and an SDR to collect the traces, placed in an anechoic test chamber at a distance of 10 m from each other, as shown in Figure 5. The chip runs periodic AES encryptions with a fixed key and random plaintexts, using the `tinyAES` implementation included in the Nordic Semiconductor SDK[4]. Moreover, the chip is configured to modulate and transmit random data according to the Bluetooth standard on a fixed channel without Adaptive Frequency Hopping (AFH).

On the receiving side, we use an antenna with a gain of 24 dB (TP-Link TL-ANT2424B) and two low noise amplifiers with a gain of 20 dB (Minicircuits ZEL 1724 LNA), followed by a DC Block to stop any direct current components after the amplifiers. The signals are then received by an Ettus Research USRP N210 populated with an SBX daughter board. The radio is tuned to frequency $f_{\text{chan}} + 2f_{\text{clk}}$, i.e., the frequency of the Bluetooth channel as per the Bluetooth standard increased by two times the clock frequency of the target device's CPU. The choice of frequency is based on considerations that we present in Section 5; it is essentially a consequence of how the leaked information from the CPU is modulated onto the output signal of the radio. We sample at 5 MHz; we found this bandwidth to be sufficient for the attack.

The result of running the first step of the attack in this setup is a capture of the emitted signal's in-phase and quadrature (I/Q) components over time, spanning many AES computations of the chip's CPU.

[4]Available at https://www.nordicsemi.com/eng/Products/Bluetooth-low-energy/nRF5-SDK.

4.2 Trace separation and alignment

Well-known side-channel techniques such as correlation or template attacks are based on aligned traces of the leaking signal, each covering a single execution of the computation under attack. Concretely, in order to apply such attacks to our signal, we need to partition it into individual traces, each spanning a single AES computation, and align the traces.

In a first step, we use a coarse-grained trigger mechanism to recognize individual computations, partially inspired by [11]. By manual analysis we identified a frequency component in the signal of our target device that is only present just before AES runs (related to a specific piece of code present in the program). Therefore, amplitude demodulation of the trigger component yields a rough trigger signal from the received emissions, which we square to amplify the triggering effect. We cut the original capture accordingly, obtaining traces that each correspond more or less to a single run of AES. However, for a successful attack we need precisely aligned traces, so the next step is to fine-tune trace alignment.

To this end, we iteratively shift each trace in time, maximizing correlation with a "prototype trace". The prototype is the point-wise mean of all traces aligned so far. Intuitively, averaging aligned traces removes random noise, so aligning new traces with the prototype becomes easier as we average over more and more traces.

The result of partition and alignment is a set of precisely aligned traces, i.e., time-domain signals emitted by the target device at $f_{\text{chan}} + 2f_{\text{clk}}$, each covering the time of a single AES computation. This dataset is suitable for known key-recovery techniques, such as correlation and template attacks.

4.3 Key recovery

The final step of the attack is to use the collected traces to recover the AES key. At this point our data is sufficiently similar to the traces employed in power and EM attacks, so that we can use the same algorithms with only small modifications. In fact, the novelty of our attack is the process of deriving traces from mere radio signals. This forms the basis for CRA and TRA attacks, whereas existing algorithms can be used for key recovery. However, in order to demonstrate a full attack from start to finish we briefly discuss the application of well-known techniques for key recovery from our traces.

Our implementation is a slightly modified version of the attack code from the ChipWhisperer project [42], originally designed for analyzing power traces. We have successfully executed a template attack on our traces, achieving full key recovery. Specifically, we attack the first round of the SubBytes step in AES. The attack needs around 70 000 traces for (offline) template creation, enabling the actual attack to succeed with only 428 traces. A single trace contains the average of 500 measurements of the same encryption.

5 ANALYSIS

We have introduced the concept of screaming channels and demonstrated their exploitability. In this section we focus on explaining the physical effects underlying the channel before showing additional experiments in the next section.

5.1 Overview

Screaming channels originate from the interplay of different factors at the physical level in complex mixed-signal circuits. Figure 6 provides an overview of the main steps that lead to a leak via radio; we briefly describe each of the factors before discussing them in detail.

When software runs on a processor, or a specialized hardware block carries out its function, the underlying digital electronic components are very active. As logic entities take 0 and 1 values, transistors switch from low to high voltage values and vice versa. The intense switching activity leads to sharp voltage and current variations that are correlated with the logic data being processed by the system. This correlation lays the ground for many side-channel attacks, as unintended effects can be measured (typically indirectly) and analyzed: for example, power side channels [33], conventional EM side channels [5] or Simple Photonic Emission Analysis (SPEA) [50] are based on such measurements. More generally, the effects on current and voltage are unintended outcomes of the digital circuit's normal operation, and are therefore called *digital noise*. The clock signal is a particularly strong source of digital noise: since it is responsible for synchronizing the circuit at a given frequency it is one of the fastest switching signals in the circuit. Moreover, it is a non-ideal square wave that exhibits many harmonics at multiples of the fundamental frequency.

The digital noise propagates inside and outside the circuit. This process is strongly dependent its characteristics in the frequency domain. Propagation channels typically only allow a certain band of frequencies to pass. The information leak that we are interested in is present in several copies at different frequencies. As a consequence, it is very likely to be admitted through at least one noise propagation path in the circuit. We refer to this effect as *spectrum spraying*.

Among the different ways of noise propagation the most relevant to mixed-signal circuits is substrate coupling [12]. The substrate is the "bulk" silicon on which the chip is manufactured. Depending on the frequency, the noise flows through a mainly resistive, capacitive, or inductive path to the analog transistors. EMC literature usually calls the digital circuit the *aggressor* and the analog part the *victim*.

As previously explained, information about the digital circuit's activity leaks into other parts of the circuit, and components of the leak are likely to reach the analog portion of the chip. In particular, they reach the radio transmission chain, and they contain frequencies in the range of the radio's baseband signal. The leak thus couples with the baseband signal, with the mixer, amplifier, or with the Voltage Controlled Oscillator (VCO) that is part of the carrier-frequency synthesizer. In any case the result is unintended amplitude/frequency modulation of the carrier. Literature discusses different kinds of substrate coupling and their effects on different transmitters [12]. Capacitive coupling with the VCO, which leads to amplitude modulation of its output, is a model that fits our experimental results on the Nordic Semiconductors nRF52832. We leave the in-depth investigation of substrate coupling in this chip as future work. The leak (i.e., the modulated carrier) is then amplified by a power amplifier and radiated by the antenna over a potentially very long distance.

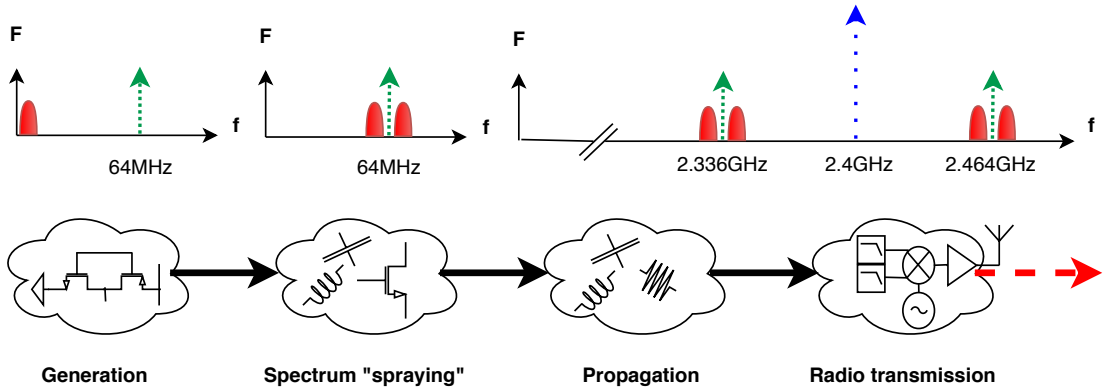


Figure 6: Steps that lead to the radio transmission of the digital circuit's switching activity, assuming a clock frequency of 64 MHz and a radio channel centered at 2.4 GHz. The Fourier transforms illustrate the process in the frequency domain.

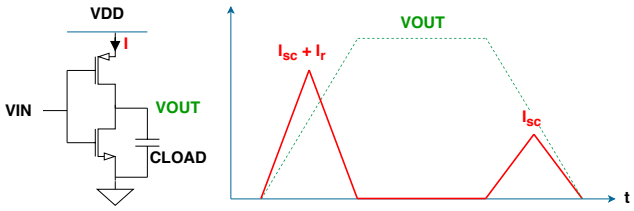


Figure 7: Current sourced by the power supply during the switching of a CMOS inverter.

We now discuss each of the steps in detail: the generation of digital noise, its frequency characteristics, its propagation into other parts of the circuit, and finally its emanation via the radio.

5.2 Noise generation

Logic gates are built with the Complementary Metal Oxide Semiconductor (CMOS) technology.[5] CMOS transistors are used in their non-linear region and act as switches that connect the output either to the power supply (high) or to the ground (low). Since the output is a parasitic capacitive load, it consumes a spike I_r from the supply when rising to high, and it sinks a spike I_f to the ground when falling to low. Moreover, for a short time window during the transition, the transistors connect the supply to the ground, consuming a spike I_{sc} of short-circuit current over their parasitic resistance. The current consumption is therefore correlated with the value of the output: At the power supply, the consumption is $I_{sc} + I_r$ in the case of a rising transition and I_{sc} in the case of a falling transition; ideally, there is no consumption if the value does not switch. Figure 7 summarizes the effect. Building on these observations, the *Hamming weight* and *Hamming distance* models correlate the power consumption with the current value of a register or its transition, respectively; they are widely used in the side-channel literature.

[5]While BJT technology is often used for analog chips, mixed-design chips almost exclusively rely on CMOS [7].

5.3 Spectrum spraying

It is interesting to analyze the noise in the frequency domain, as it helps explaining its propagation through the circuit.

Intuitively, the idea behind frequency analysis is that a time-domain signal can be seen as the composition of many pure sine waves at different frequencies (i.e., frequency components), and the Fourier transform is a way to switch between the time and frequency domains. One of the most important sources of noise in a digital circuit is the clock signal, which (ideally) is a square periodic signal. The Fourier transform of a periodic signal is composed of a component at the fundamental frequency, plus several harmonics at its multiples which depend on the shape of the base period. The "sharper" the changes in the time domain, as it is the case for a square wave, the higher the frequencies of the individual components. For example, the Fourier transform of the idealized clock (i.e., a square wave) is:

$$X(f) = \sum_{n=-\infty}^{\infty} \frac{2\sin(n2\pi f_0 T)}{n} \delta(f - nf_0), \tag{1}$$

where $f_0 = \frac{1}{T}$ is the fundamental frequency and $\delta(f - nf_0)$ is a harmonic component at frequency nf_0 with amplitude $\frac{2\sin(n2\pi f_0 T)}{n}$. Thus, a square wave is composed of an infinite number of sine wave components.

If such a signal is amplitude modulated, then each of the harmonics is, so that the modulation is "spread" over the spectrum. In other words, each sine wave component acts as a distinct carrier for the modulating signal. Recall that, if a modulating signal $x(t)$ modulates a carrier $e^{-i2\pi f_0 T}$ with frequency f_0, then its spectrum $X(f)$ is shifted to $X(f - f_0)$ (i.e., at the carrier's frequency).

We will now describe the precise mechanics of how data signals behave as modulating signals, spreading their sensitive information over the spectrum. Suppose that a data signal is coupled with a harmonic of the clock (e.g., through parasitic capacitance), and the sum of the two enters the input of a Metal Oxide Semiconductor (MOS) transistor in some logic gate. When such a transistor is in the saturation region, the current that flows through it is quadratic

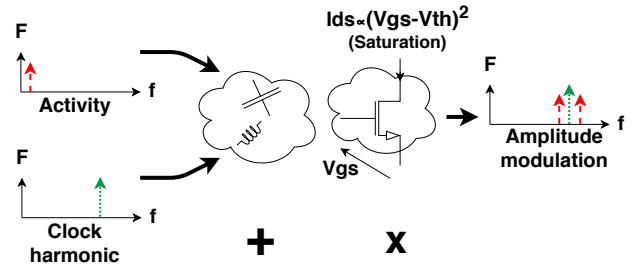


Figure 8: Amplitude modulation of a clock harmonic.

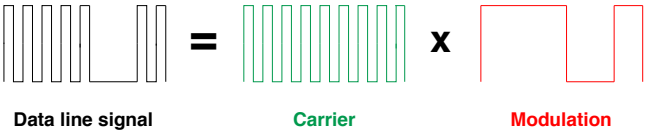


Figure 9: Interpretation of a data line as a modulated carrier.

in the input voltage:

$$I_{ds} = \alpha(V_{gs} - V_{th})^2 \tag{2}$$

where g,s,d represent the gate, source, and drain terminals, α and V_{th} are constants that depend on physical parameters, and $V_{ds} > V_{gs} - V_{th}$ is the condition for being in the saturation region. Because of its quadratic behavior, the transistor acts as a mixer that produces a current at the harmonic of the clock, amplitude modulated by the data signal [36], as shown in Figure 8. The following development demonstrates that, in general, squaring the sum of two sine waves is indeed equivalent to mixing:

$$\begin{gathered}(\sin(2\pi f_1 t) + \sin(2\pi f_2 t))^2 = \\ 2\sin(2\pi f_1 t)\sin(2\pi f_2 t) + \sin^2(2\pi f_1 t) + \sin^2(2\pi f_2 t) = \\ \cos(2\pi(f_1 - f_2)t) - \cos(2\pi(f_1 + f_2)t) + \ldots\end{gathered} \tag{3}$$

In deep-submicron technologies (i.e., gate length of the MOS transistors smaller than 0.35 µm), the transistor is rather linear in saturation. However, the activity itself can be seen as a modulated carrier [36] (Figure 9). In both cases, the modulating activity is replicated at each of the harmonics of the clock, which act as separate carriers. Alternatively, a data signal can couple with the input of a VCO, leading to frequency modulation of its output (e.g., the clock) [5, 36].

It has been shown that malicious software can deliberately generate a carrier and modulate it as described above to transmit data, thus creating a covert channel. For example, crafted memory accesses can produce a square wave modulation and broadcast music [21], and more complex protocols can be used to furtively send data from air-gapped computers over cellular frequencies [29]. While these covert channels are based on the same principles of modulation, they invoke the modulating effects on purpose, whereas the leak we analyze in this paper is an unintended modulation.

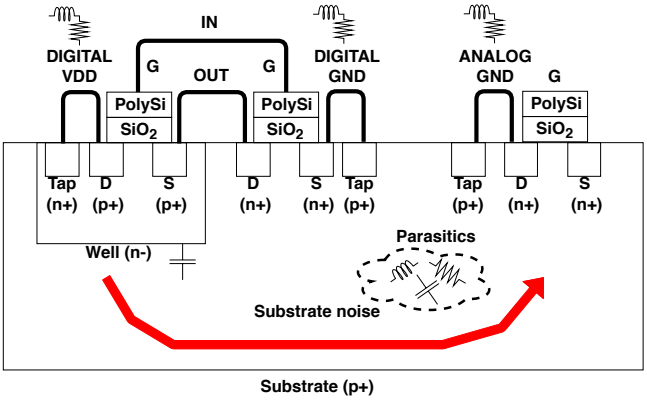


Figure 10: Schematic illustration of substrate noise coupling (inspired by [4]).

5.4 Noise propagation and initial emission

In this part we further detail substrate coupling as the main channel between the digital and analog domains. We also review how signals may radiate even before reaching the radio transmitter.

Figure 10 shows a simplified schema of a mixed-signal circuit's silicon die. On the left, a digital gate—a CMOS inverter—is the aggressor. On the right, an analog transistor (e.g., part of an amplifier) is the victim. A few examples of parasitic capacitance, inductance and resistance are shown as discrete elements over the image.

The main reasons for substrate coupling are impact ionization currents at the device level, capacitive coupling (junction and interconnect parasitic capacitances) at the circuit level, and inductive/resistive coupling at the chip level [4]. Resistive coupling dominates at low frequency, whereas capacitive and then inductive coupling appear at higher frequencies [12].

Sharp variations of current in some components lead to direct electromagnetic emissions, which can be measured with suitable antennas: H-probes (magnetic field) and E-probes (electric field). In general, direct emissions are small and localized, and measuring them requires close proximity or even decapsulation of the chip [36]. Moreover, some of the modulated harmonics of the clock that we previously described may excite the resonance of some components, such as data lines, that will act as antennas and radiate. This last case is commonly referred to in literature as *indirect emissions*.

Near-field emissions are the basis of EM side channels. The short range of EM attacks is a direct consequence of the low signal intensity of such emissions.

5.5 Radio transmission

Screaming channels, as opposed to EM side channels, can be attacked over long distances. This is because the noise propagates to mixed-signal circuits that compose the radio, where it is mixed, amplified and broadcast. Modern radio transmitters are typically composed of:

(1) a *digital baseband* which converts the data to transmit into digitally modulated data (I/Q signals),
(2) a digital-to-analog converter (DAC) which converts modulated I/Q data to analog I/Q signals (the *baseband* signals),

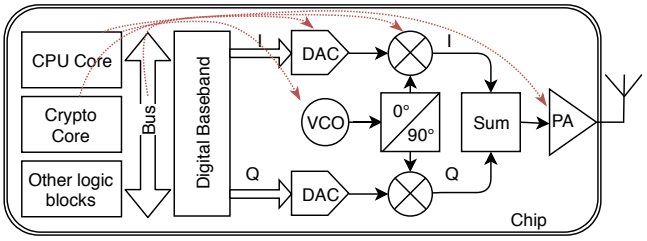


Figure 11: System on Chip including radio using a direct radio transmitter architecture. Possible noise coupling is indicated with red dashed lines.

(3) an analog transmitter which will bring baseband signals to the right frequency and amplifies them.

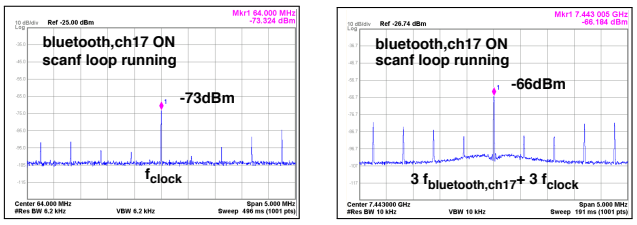
The way noise couples to the radio transmitter will depend on the transmitter architecture. There are multiple possible architectures, and the choice will depend on several factors, such as the semiconductor technology used, the difficulty to create a stable high frequency local oscillator, the acceptable noise levels or simply the cost. For example, a superheterodyne transmitter performs the conversion in two stages, first to an intermediate frequency then to the final frequency, while in a direct transmitter the VCO will be tuned to the exact frequency at which the signal needs to be transmitted. Direct transmitters are the most compact and common ones in modern integrated radio circuits [7]. Figure 11 shows such a direct radio transmitter and the possible locations where noise can couple.

The noise propagation mechanics described above, a replica of the digital noise reaches the analog domain. Here it can couple in various ways and places, in particular with the VCO that is part of the frequency synthesizer for the carrier [12]. As explained before, we are mainly interested in the capacitive coupling that leads to amplitude modulation. In this case, we have two cascaded modulations. First, the leak modulates the clock harmonics. Second, the resulting signal propagates to the radio and modulates the carrier (and its harmonics). The frequencies of the resulting signals can be predicted as follows:

$$f_{\text{radio\_leak}(p,q,r)} = p \cdot f_{\text{carrier}} \pm q \cdot f_{\text{clock}} \pm r \cdot f_{\text{leak}} \qquad (4)$$

where p, q, r are positive integers. Not all multiples are present, depending on the actual shape of the signals and/or the presence of components that act as filters. The "noise modulated" carrier is further mixed with the legitimate baseband signal of the radio protocol. Then it enters a power amplifier, a balun, and finally reaches the antenna, where it is broadcast.

Figure 12 shows two measurements that illustrate the prediction of Equation 4: "copies" of an EM leak can be observed at various frequencies. In this example, we see an EM leak at the clock frequency, and a radio leak at the third harmonic of the Bluetooth carrier. The leaks are visible only when the power amplifier of the transmitter is on, confirming that the digital noise flows through a screaming channel from the digital to the analog/RF part of the circuit. Measurements were taken with an off-the-shelf WiFi antenna, two low noise amplifiers (ZEL 1724LN), and a spectrum analyzer (Agilent Technologies MXA N9020A) with 6 dB attenuation.



(a) EM leak (b) Radio leak

Figure 12: Leaks resulting from executing `printf` on a Nordic Semiconductor nRF52840. Note the central frequency is 64 MHz in (a) and of 7.443 GHz in (b).

6 ADDITIONAL EXPERIMENTS

While we demonstrated the exploitability of screaming channels in Section 4, we conducted several experiments to further evaluate their impact. The main objective in conducting those experiments is to understand the applicability of screaming-channel attacks in different scenarios, including different experimental setups, cryptographic implementations, and target devices.

6.1 Key Recovery in different environments

While in Section 4 the experiments are performed in optimal conditions for an attacker, it is important to also evaluate such attacks under more realistic assumptions. We therefore tested attacks over several distances, and also in a normal office environment with a large amount of noise, using commercial of-the-shelf antennas. The noise in the office environment is caused by different sources, such as phone calls, WiFi access points, or Bluetooth communications. Table 1 highlights some cases in which we were able to successfully recover the *full* encryption key with a template attack and shows the number of traces we used for generation of the template and for the actual attack. A single trace contains the average of 500 measurements of the same encryption. Although these numbers are specific to our attack implementation and may be improved by various optimizations, we believe that this data gives a first intuition about the performance of screaming-channel attacks in different settings.

Quite naturally, screaming-channel attacks perform very well in a low-noise environment. The number of traces to perform an actual attack differs by more than an order of magnitude in the different settings with templates of similar size. The creation of these templates required us to conduct measurements for approximately 20 h, while the collection of an attack set with less than 1000 traces barely took 15 min.

Table 1: Configurations for attacks with full key recovery

Distance	Environment	#Attack Traces	#Template Traces
1 m	Office	52 589	70 000
3 m	Laboratory	718	70 000
10 m	Laboratory	1428	130 000

6.2 Attacking other AES implementations

In all our previous experiments, we attacked `tinyAES`, as this is a simple, straight-forward textbook AES implementation. However, commodity devices often use more sophisticated cryptographic implementations, which are also likely to be vulnerable against screaming channel attacks.

We choose to demonstrate this on `mbedTLS`, a widely used TLS implementation which has some counter-measures against remote timing side-channel attacks [51]. Since the EM attacks are considered as local attacks, and thus outside the threat model, there are no countermeasures against them. However, this leaves this implementation vulnerable to screaming channel attacks as well, which instead may succeed remotely.[6]

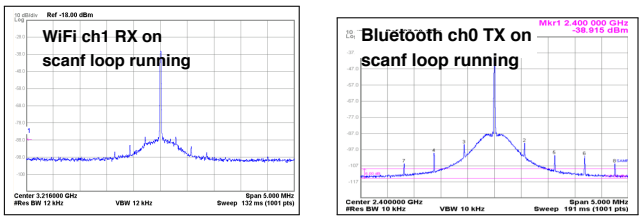
To ease the creation of a proof of concept attack, we slightly modified our attack scenario in this case. Instead of sending modulated data with the device under attack, we were just transmitting a continuous wave while encrypting, as this allows correlation attacks to succeed easily. We want to stress that, while this seems less realistic, a successful correlation attack is an important first step to demonstrate the feasibility of the exploitation of screaming channels. In fact, during the initial development of screaming channel attacks, we used exactly this methodology and improved on it. Using this setup, we were able to recover the full key with less than 40000 traces over a distance of 1m, which is essentially showing that even well maintained implementations are vulnerable to screaming channels attacks.

Additionally, besides software implementations for cryptographic primitives, a majority of chips also come with hardware implementations to enable efficient link-layer encryption of the communication. While we applied screaming channel attacks so far only to software implementations likely to be present in application logic, we also measured their applicability to the hardware AES implementation of the nRF52832. While we were not able to mount a successful attack over the air, we were able to obtain some encouraging results over a direct coaxial connection. While this doesn't effectively break link-layer encryption, we believe that the presence of screaming channels even for hardware implementations poses a significant threat.

6.3 Screaming Channels on other devices

We observed the same leak, in a Rigado BDM301 Bluetooth module (which, like the RedBear BLE Nano v2 module, is based on a nRF52832) and on a Nordic Semiconductor nRF52840 Bluetooth device, indicating that the problem is not only due to one chip or one module. The BDM301 is interesting because it has a connector to an external antenna, which may perform better than the compact antenna directly soldered on the PCB of the BLE Nano v2, leading to stronger signal. The latter also has a stronger available power output, and an ARM cryptocell cryptographic module. It would be interesting to evaluate the potential leakage from this dedicated security hardware block. We leave the in-depth evaluation and attack of these devices for future work.

[6]See for example this questions on the `mbedTLS` discussion forum and the response by the main `mbedTLS` developer: https://tls.mbed.org/discussions/crypto-and-ssl/aes-implementation-resistant-to-side-channel-analysis-attacks



(a) Possible Atheros leak (b) Confirmed nRF52832 leak

Figure 13: A possible screaming channel carrier on a Qualcomm Atheros AR9721, with spurs which change depending on the code being executed. Besides, a confirmed leak on the nRF52832.

We have also performed some experiments on an ExpressIF `ESP32` Bluetooth and WiFi chip. We were able to observe some classic EM leaks at low frequency that are correlated with code execution, and indications of a possible screaming channel leak on Bluetooth transmissions. However, this leak was weak and not confirmed with full AES-128 key extraction.

Though we mainly investigated Bluetooth chips, mixed-signal designs are very common also for WiFi devices. Like Bluetooth the most commonly used WiFi radio band is at 2.4 GHz. We conducted some preliminary studies on a Qualcomm Atheros AR9271 WiFi dongle. We observed the presence of what could be a variation of the screaming channels described before for the nRF52832 chips. When the device is on, some components appear around 3 GHz, whose frequency depends on the receiving channel, and that are most likely modulated by code execution. More precisely, the frequency changes regularly when changing the channel, and it appears amplitude modulated by code execution, as different loops show different components, similarly to what we observed on the nRF52832. Interestingly, this signal is impacted neither by the transmission nor by the reception of WiFi data. As a consequence, we conjecture that it is an harmonic of the frequency synthesizer for reception that leaks into the transmission path (*LO reradiation* [7, 16, 55]). In general, this highlights how any carrier modulated by a leak could be picked by the transmission chain and broadcast, leading to different flavors of screaming channels. We leave the detailed exploration of this effect and possibly the extraction of AES-128 traces for future work. Figure 13 summarizes the measurements.

7 DISCUSSION

In this section we discuss the results reported so far. In particular, we focus on the attack's applicability in real-world scenarios, countermeasures, and directions for future work.

7.1 Real world applicability

The hardware requirements for carrying out radio attacks outside lab environments are very moderate: successful attacks from shorter distances are possible using a commodity WiFi antenna and a hobbyist SDR like the HackRF [28]. Attacking from greater distances will require more equipment, such as a highly directional antenna, a low noise amplifier and a good SDR for collecting traces.

We have experimented under several radio propagation conditions: cable only, radio propagation in home or office environment and finally in an anechoic room designed for testing radio transmissions at 2.4 GHz. Clearly an anechoic room provides ideal collection conditions and allows to demonstrate the best environment conditions for the attacker. The tests over a cable do not correspond to any realistic threat model and are therefore mostly relevant for development of the attacks. Finally, the results we presented in a home/office environment show that attacks are possible in a non controlled environment with an important volume of non controlled interfering communications. Those interfering communications slow down the attack, increasing the amount of samples that needs to be collected, and reducing the achievable distance, yet the attack remains possible. It is likely that the results we present in this paper can be improved, by applying more advanced attacks, and by additional engineering optimizations regarding the collection on both the measurement and processing sides, for example, to increase accuracy and speed.

Some knowledge of the target chip is required in order to determine the right attack parameters. In particular, the attacker needs to know or guess the clock frequency of the target's CPU to determine the radio frequency to listen on. We found in practice that because the clock signal is transmitted by the radio, the clock frequency can be reliably guessed from the spectrum of the target's radio emissions. Furthermore, the attack requires a trigger for cutting a signal into individual traces; in the case of our example target nRF52832, manual inspection of the signal yielded suitable trigger components.

Finally, the target device needs to use its radio in transmission mode while running the computation of interest. The destination or contents of the transmission are irrelevant as long as the attacker can observe the signal. Since the transmitted data does not matter for the attack, any communication is suitable. For targets that do not communicate enough on their own, it would be possible, for example, to periodically query for identifiers, beacons, echo replies or similar facilities provided by the respective protocol stack.

7.2 Impact on the threat model

Devices that need to protect a secret and can be physically accessed by an adversary will typically consider EM or power side-channels in their threat model. This is the case for example for smart cards used in applications such as credit cards, pay TV or ID documents. Therefore, such devices typically use multiple countermeasures against physical attacks, including masked cryptographic implementations which render EM and power side channels attacks more difficult to mount. However, EM or power side-channels attacks are usually considered out of scope for devices with lower level of security and without tamper resistance requirements, such as IoT devices, wearables, and Bluetooth and WiFi chips included in smartphones and computers.

The reason for ignoring EM side-channels in these devices is that if an attacker can get close enough to mount a side-channel attack, then the system can be compromised in many other ways. As such, those attacks are often considered as physical attacks. However, our results show that this security model is not sufficient, and that for data to be really protected from attackers the chip must avoid leaks through the radio channel. As a consequence we believe that, in the light of radio side channels, affected devices will require additional protection mechanisms.

7.3 Countermeasures

Generic countermeasures against side-channel attacks are an active field of research.

7.3.1 Cryptographic countermeasures. We refer to the relevant literature, in particular on *hiding* and *masking* [31, 39]. Hiding is the process of changing the design such that intermediate values of sensitive computations do not leak into observable channels, such as power, EM emissions and, as we have shown, radio transmissions. Masking tries to make leaked intermediate values less useful, for example by randomizing them. Both techniques can likely be used to defeat the primary leaks and therefore render screaming channel attacks more difficult. Rapidly re-keying is also an efficient way to prevent the adversary to collect enough samples to mount a complete attack and can be performed already in many protocols [40].

7.3.2 Avoiding leakage. Another class of possible protection mechanisms are dedicated techniques to prevent information from leaking into radio signals. Since the general issue is a direct consequence of the physical proximity of analog and digital components in affected chips, countermeasures can only indirectly protect such systems.

A simple approach is to avoid sensitive computations in digital circuitry close to radio components. For example, a WiFi chip attached to a computer could use the PC's CPU for cryptographic operations instead of carrying them out internally. Naturally, such protections harm performance and require the availability of a separate processor in the first place. Moreover, while leakage should be significantly reduced, some side-channel information may still be observable.

Barring the presence of an alternative processor, countermeasures have to ensure that the radio is never active in transmit mode during sensitive computations. For example, the firmware could serialize corresponding operations instead of executing them in parallel. In many cases this will require extensive redesign of the firmware and have a strong impact on performance.

7.3.3 Countermeasures during chip design. System in Package (or System in a Package) (SiP) technologies integrate multiple dies inside one package, this allows to avoid substrate coupling and to use different semiconductor technologies [35]. SiP devices have the advantage of being almost as compact as single chip solutions but providing more room for isolating sensitive operations from radio transmitter (e.g., creating filters using passive components).

Unlike conventional transmitters (including SDRs) fully digital radios perform the complete modulation of the signal in digital circuits [44]. The final stage of the radio is typically a *Differential-like Digital Power Amplifier* which directly converts the modulated digital signal to amplified radio signals. As those designs are made with significantly less analog radio components, it would be interesting to estimate their susceptibility to the screaming channels.

While shielding the whole device is effective for classic EM emanations, in the radio side channel it cannot be applied on the whole system because the radio transmitter has to transmit data.

I.e., shielding the antenna goes against the purpose of the antenna. However, isolation can be used to reduce the coupling inside the chip using for example guard rings, various substrate modifications techniques or even active noise cancellation techniques [4].

New designs will be able to avoid the core issue by moving cryptography to protected hardware blocks or by incorporating strong shielding between digital and analog components. However, the required changes are likely to run counter to market demands: low cost and ever reduced chip size.

In any case it appears difficult to address the core problem without compromising on other requirements. Moreover, experience shows that protection mechanisms usually increase the difficulty of attacks but do not prevent them entirely. We therefore expect radio side-channel attacks to be possible for the foreseeable future; they should thus be considered in the threat model of sensitive applications.

7.4 Future Work

In this work, we demonstrated the existence of a novel side-channel, conducted an analysis of the underlying physical problems and showed the feasibility of an attack against them. Quite naturally, this initial investigation by far does not exhaust the capabilities of screaming channel attacks, and a variety of directions can be explored in future work.

7.4.1 Improving screaming channel attacks. In this paper, we focused on attacking single chip, the nRF52832. While we show the presence of screaming channel leaks on other devices, full attacks against them still have to be implemented. Moreover Bluetooth and WiFi chips may not be the only vulnerable devices, as mixed-signal designs are also present in other domains, such as GSM baseband chips or IoT devices communicating on other frequencies. Similarly, there is no reason to consider that screaming channels are limited to mixed-signal designs on a single integrated chip. Any system that is processing sensitive data and contains a radio transmitter is potentially vulnerable if proper isolation of both domains is insufficient.

Furthermore, the attack itself can be further refined. While we base our code on implementations for conventional EM attacks, dedicated implementations coping with the unique environment of screaming channels could probably improve the effectiveness of an attack. For instance, as the leak is spread over a wide spectrum, it could be collected and analyzed on different bands at the same time. This could be performed by tuning on multiple frequencies with multiple radio receivers. In the current attacks we only use the amplitude of the signal, but noise coupling could lead to phase noise and exploiting phase noise can likely improve the attack. Using SDRs with more bandwidth may capture more frequency components and improve effectiveness. Likewise, using multiple radios from different locations may help to reduce impact of background noise. Finally, a systematic study of the influence of noise, distances, and measurement equipment for screaming channel attacks could give new insights on how to improve practical attacks.

7.4.2 Impact on wireless protocols security and hardware cryptographic blocks. In this paper we show that we can recover key material from cryptographic operations conducted in software on the CPU core integrated in a mixed-signal chip. This is very relevant to IoT devices, which often rely on a single chip solution and rely, e.g., on `mbedTLS` for protecting their communication to an online service. On the other hand, for most devices the wireless link is protected by AES-CCM (e.g., Bluetooth [10] or WiFi [3]). Because those devices are aiming at low power and the standards are well established, they often include a hardware cryptographic block to protect wireless communication. However, hardware cryptographic implementations are generally more power efficient than software ones, which leads to less EM side-channel leakage. Hence, CRA and TRA attacks on hardware cryptographic blocks are more challenging, and while the analysis of the channel and some preliminary results seem to show the general feasibility, complete attacks are left for future work.

8 RELATED WORK

Our work mainly touches upon two areas of research: on the one hand, we build on previous work around side-channel attacks, and on the other hand, we draw inspiration from research in circuit design, particularly concerning noise in mixed-signal circuits.

8.1 EM side-channel attacks

Kocher et al. were the first to show non-timing side-channel attacks against cryptography in 1999 [33]. They used power measurements on a smartcard to attack its DES implementation. Since then, a long line of work has found attacks against various algorithms, including AES, RSA and the Diffie-Hellman key exchange, using a variety of side channels. The more common channels are power measurements, as initially suggested by Kocher et al., cache-timings, as demonstrated by Bernstein [8], and electromagnetic emanations. In particular this last category has inspired our work; one of our goals was to extend the rather limited range of EM attacks on low-power devices. In parallel with the research on side-channel attacks, countermeasures have been proposed [31, 39].

EM eavesdropping attacks on general computing hardware have existed for decades, the TEMPEST specification [2] partially declassified in 2001. In 1985 [20] van Eck described a method to infer the output of a CRT monitor from hundreds of meters away, using cheap off-the-shelf equipment. Kuhn [34] applied similar principles to flat-panel displays in 2004 and was able to reproduce text from laptop screens at distance of 10 meters. Another TEMPEST document from 1982 (declassified in 2000) [41] mentions 4 mechanisms for propagation of compromising emanations, one of them is "modulation of an intended signal" but the details are redacted (reproduced in Appendix A). One could speculate that those redacted lines discuss some effect similar to the screaming channel.

The power of EM side-channel attacks against secure systems was concretely demonstrated in 2001 [23], when Gandolfi et al. used small EM probes to fully recover key material from three different types of microcontrollers. More recently, EM side-channel attacks have extracted cryptographic keys from PCs [25] and FPGAs [48, 61]. In [54] Shamir et al. exploit the fact that power is delivered wirelessly to RFID devices to measure energy consumption patterns and infer sensitive information. Radio receivers can under some conditions reradiate the local oscillator [7] and this can be used for detecting radio receivers [16, 55]. The closest related work to ours

is by Esteves et al. [22] which investigates the feasibility of digital logic to interfere with a radio transmitter to create a covert channel as transmission noise.

Trojan circuits inserted by a malicious foundry are an important concern [37], this type of attack was more recently implemented in the context of FPGAs which are shared among different users. In this scenario, an attacker implements circuitry to measure power consumption (either directly with ring-oscillators [61], or indirectly through delay sensors [49]) to infer secret information from a privileged portion of the device, shared routing resources, or "long wires" [26, 47].

FPGAs are becoming very popular in data centers and where hardware logic from independent tenants is sharing resources which make such vulnerabilities even more important. While these works mention attacks which can be mounted remotely [61], the attacker is assumed to control part of the FPGA design. In contrast, screaming channels do not require this assumption and are applicable with relatively loose constraints on physical proximity.

Our work builds on previous studies which observed information leaks transmitted by unintentional carrier signals. Agrawal et al. [5] mounted EM-based attacks in 2003 against DES on smart cards, and noted an important distinction between two types of EM emanations: direct (intentional) current flows from rapid transitions between digital states, and unintentional emanations due to coupling between different components on a chip. They observed that unintentional emanations can modulate a "carrier" signal generated by a chip (either by changing its amplitude or phase), and that this information can be recovered at a larger distance, with less precise probe placement, when compared to the attempted recovery of direct emanations. Many subsequent attacks [24, 32, 58] relied on this principle. In this type of attack, the carrier usually comes from an oscillator or digital clock signal on a device, while a screaming channel will use the carrier wave created by a frequency synthesizer in an RF transmitter.

8.2 Modern tools and applications

Besides discovering and exploiting side-channels, methods for targeting collection parameters and inferring processor state information have also become more sophisticated in recent years. This includes highlighting the most promising sources of unintentional emanations [15], measuring the power consumption of individual instructions [56], measuring an attacker's advantage when an instruction is changed in a program [14], and modeling the range of viability for EM side-channel attacks [59].

Remote device fingerprinting based on intercepted signals include measuring artifacts such as modulation errors [18], seed sequences [57], and characteristic defects in the manufacturing process that are expressed in a device's modulated signal [17]. It has also been suggested as a way to profile a program's performance [13, 53] or detect anomalies in program execution [38] (such as malware injection).

Software provided by GNURadio [9], rsa-sdr [11], and the ChipWhisperer project [42] have simplified the tasks of trace collection and analysis, and in some cases inspired the trace processing code written for this study.

8.3 Noise in mixed-signal designs

A lot of work has been dedicated to observing and explaining the various interactions in electronic circuits that lead to inadvertent signal emission in Printed Circuit Boards (PCBs) [6, 19, 30, 45]. Much of this research, however, is targeted at aiding circuit design with respect to EM compliance; security is never considered focus.

The challenges and countermeasures of mixed-signal IC design are conceptually similar to PCB design. Bronckers et al. [12] performed a detailed study of substrate noise coupling mechanisms in SoCs that incorporated digital and analog components. Their work demonstrated that the extent of undesirable noise in ICs is highly dependent on layout, and provided recommendations for how designers could effectively use guard rings and other isolation structures to properly shield analog components.

9 CONCLUSIONS

Unintentional EM leaks have plagued designers and users of secure systems since they were discovered. In this paper, we introduce and analyze a novel side channel on mixed-signal chips, where EM leaks from digital circuits propagate to nearby analog radio components and, as a result, are broadcast in the air along with the intended radio communications. We demonstrated full key recovery against popular AES implementations over such "screaming channels" for distances up to 10 m for `tinyAES` and 1 m for `mbedTLS` using novel TRA and CRA attacks.

We believe that our attack requires to re-think the way in which mixed-signal chips, or cryptographic implementations for them, are designed. Hence, besides showing the attack, we also propose several directions for countermeasures in the hope to allow better protection for affected devices in the future.

While those attacks are on specific Bluetooth chips, the fact that the effects involved are very generic implies that it is likely that "screaming channels" affect many systems which process sensitive data and include a radio transmitter. Future work will therefore have to discover which other systems are affected.

CODE AVAILABILITY

All code required to replicate our attack is available at http://s3.eurecom.fr/tools/screaming_channels/, together with the data we have collected and a precise description of the hardware setup.

ACKNOWLEDGMENTS

The authors acknowledge the support of SeCiF project within the French-German Academy for the Industry of the future as well as the support by the DAPCODS/IOTics ANR 2016 project (ANR-16-CE25-0015). We would like to thank the FIT R2lab team from Inria, Sophia Antipolis, for their help in using the R2lab [1] testbed.

REFERENCES

[1] [n. d.]. R2lab, an open tested located in an anechoic chamber for reproducible research in wireless networks. http://fit-r2lab.inria.fr/. Accessed: 2018-05-07.
[2] 1972. *TEMPEST: A Signal Problem.* Technical Report. NSA. Available at:https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf.
[3] 2004. IEEE Std 802.11i-2004 Medium Access Control (MAC) Security EnhancementsWireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification.

[4] A. Afzali-Kusha, M. Nagata, N. K. Verghese, and D. J. Allstot. 2006. Substrate Noise Coupling in SoC Design: Modeling, Avoidance, and Validation. *Proc. IEEE* 94, 12 (Dec 2006), 2109–2138. https://doi.org/10.1109/JPROC.2006.886029

[5] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. 2003. The EM Side—Channel(s). In *Cryptographic Hardware and Embedded Systems - CHES 2002*, Burton S. Kaliski, çetin K. Koç, and Christof Paar (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 29–45.

[6] Michael Bailey. 2011. General Layout Guidelines for RF and Mixed-Signal PCBs. APP 5100, https://www.maximintegrated.com/en/app-notes/index.mvp/id/5100.

[7] Arya Behzad. 2008. *Wireless LAN Radios: System Definition to Transistor Design (IEEE Press Series on Microelectronic Systems)*. John Wiley & Sons, Inc., Hoboken, NJ, USA.

[8] Daniel J. Bernstein. 2005. *Cache-timing attacks on AES*. Technical Report.

[9] Eric Blossom. 2004. GNU radio: tools for exploring the radio frequency spectrum. *Linux journal* 2004, 122 (2004), 4.

[10] Bluetooth SIG. 2016. Core Specification. https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=421043.

[11] bolek42. 2017. bolek42/rsa-sdr. https://github.com/bolek42/rsa-sdr

[12] Stephane Bronckers, Geert Van der Plas, Gerd Vandersteen, and Yves Rolain. 2009. *Substrate Noise Coupling in Analog/RF Circuits*. ARTECH HOUSE, Norwood, MA, USA.

[13] Robert Callan, Farnaz Behrang, Alenka Zajic, Milos Prvulovic, and Alessandro Orso. 2016. Zero-overhead profiling via EM emanations. In *Proceedings of the 25th International Symposium on Software Testing and Analysis*. ACM, 401–412.

[14] Robert Callan, Alenka Zajic, and Milos Prvulovic. 2014. A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events. In *Microarchitecture (MICRO), 2014 47th Annual IEEE/ACM International Symposium on*. IEEE, 242–254.

[15] Robert Callan, Alenka Zajić, and Milos Prvulovic. 2015. FASE: finding amplitude-modulated side-channel emanations. In *Computer Architecture (ISCA), 2015 ACM/IEEE 42nd Annual International Symposium on*. IEEE, 592–603.

[16] Anadi Chaman, Jiaming Wang, Jiachen Sun, Haitham Hassanieh, and Romit Roy Choudhury. 2018. Ghostbuster: Detecting the Presence of Hidden Eavesdroppers. In *The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*.

[17] B. Chatterjee, D. Das, S. Maity, and S. Sen. 2018. RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-situ Machine Learning. *ArXiv e-prints* (May 2018). arXiv:cs.CR/1805.01374

[18] Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On Physical-layer Identification of Wireless Devices. *ACM Comput. Surv.* 45, 1, Article 6 (Dec. 2012), 29 pages. https://doi.org/10.1145/2379776.2379782

[19] ANALOG DEVICES. (undated). Mixed Signal Circuit Techniques. AN-280, http://www.analog.com/media/en/technical-documentation/application-notes/29454258225611477795969399246177120 5AN280.pdf.

[20] Wim Van Eck. 1985. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security* 4, 4 (1985), 269–286. https://doi.org/10.1016/0167-4048(85)90046-x

[21] William Entriken. 2013. System Bus Radio. https://github.com/fulldecent/system-bus-radio

[22] José Esteves, Emmanuel Cottais, and Chaouki Kasmi. 2018. Second Order Soft-TEMPEST in RF Front-Ends: Design and Detection of Polyglot Modulations.

[23] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. 2001. Electromagnetic Analysis: Concrete Results. *Cryptographic Hardware and Embedded Systems (CHES 2001)* 2162 (2001).

[24] Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. 2015. Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 207–228.

[25] Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. 2016. ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs. In *Cryptographers' Track at the RSA Conference*. Springer, 219–235.

[26] Ilias Giechaskiel, Kasper B Rasmussen, and Ken Eguro. 2018. Leaky Wires: Information Leakage and Covert Communication Between FPGA Long Wires. (2018).

[27] Gabriel Goller and Georg Sigl. 2015. Side Channel Attacks on Smartphones and Embedded Devices Using Standard Radio Equipment. *Lecture Notes in Computer Science* (2015), 255–270. https://doi.org/10.1007/978-3-319-21476-4_17

[28] Great Scott Gadgets. 2017. HackRF one. https://greatscottgadgets.com/hackrf/.

[29] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, 849–864.

[30] Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. 2013. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. *IEEE Transactions on Electromagnetic Compatibility* 55, 3 (2013), 571–580.

[31] Philip Hodgers, Francesco Regazzoni, Richard Gilmore, Ciara Moore, and Tobias Oder. 2016. Secure Architectures of Future Emerging cryptography: State-of-the-Art in Physical Side-Channel Attacks and Resistant Technologies. (2016). http://www.safecrypto.eu/wp-content/uploads/2015/02/SAFEcrypto_D7.1-Approved.pdf

[32] Tae Hyun Kim, Changkyun Kim, and Ilhwan Park. 2012. Side Channel Analysis Attacks Using AM Demodulation on Commercial Smart Cards with SEED. *J. Syst. Softw.* 85, 12 (Dec. 2012), 2899–2908. https://doi.org/10.1016/j.jss.2012.06.063

[33] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential Power Analysis. In *Advances in Cryptology — CRYPTO' 99*, Michael Wiener (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 388–397.

[34] Markus G Kuhn. 2004. Electromagnetic eavesdropping risks of flat-panel displays. In *International Workshop on Privacy Enhancing Technologies*. Springer, 88–107.

[35] Joy Laskar, Babak Matinpour, and Sudipto Chakraborty. 2004. Modern Receiver Front-Ends. Chapter 7: Design and Integration of Passive Components. (Feb 2004), 143–190. https://doi.org/10.1002/0471474851.ch7

[36] Huiyun Li, A. Theodore Markettos, and Simon Moore. 2005. Security Evaluation Against Electromagnetic Analysis at Design Time. In *Cryptographic Hardware and Embedded Systems – CHES 2005*. Springer, 280–292.

[37] Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson. 2009. Trojan side-channels: lightweight hardware trojans through side-channel engineering. In *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, 382–395.

[38] Yannan Liu, Lingxiao Wei, Zhe Zhou, Kehuan Zhang, Wenyuan Xu, and Qiang Xu. 2016. On Code Execution Tracking via Power Side-Channel. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 1019–1031. https://doi.org/10.1145/2976749.2978299

[39] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. 2008. *Power analysis attacks: Revealing the secrets of smart cards*. Vol. 31. Springer Science & Business Media.

[40] Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni. 2010. Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. *Lecture Notes in Computer Science* (2010), 279–296. https://doi.org/10.1007/978-3-642-12678-9_17

[41] NSA. 1982. *NACSIM 5000, Tempest fundamentals*. Technical Report. Document declassified in 2000 and available at https://cryptome.org/jya/nacsim-5000/nacsim-5000.htm.

[42] Colin O'Flynn and Zhizhang David Chen. 2014. Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 243–260.

[43] Henry W Ott. 2011. *Electromagnetic compatibility engineering*. John Wiley & Sons.

[44] Viral K. Parikh, Poras T. Balsara, and Oren E. Eliezer. 2008. A fully digital architecture for wideband wireless transmitters. *2008 IEEE Radio and Wireless Symposium* (Jan 2008). https://doi.org/10.1109/rws.2008.4463450

[45] Sanjay Pithadia and Shridhar More. [n. d.]. Grounding in mixed-signal systems demystified, Part 1. Analog Applications Journal 2013, http://www.ti.com/lit/an/slyt499/slyt499.pdf.

[46] Jean-Jacques Quisquater and David Samyde. 2001. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. *Lecture Notes in Computer Science* (2001), 200–210. https://doi.org/10.1007/3-540-45418-7_17

[47] Chethan Ramesh, Shivukumar B. Patil, Siva Nishok Dhanuskodi, George Provelengios, Sébastien Pillement, Daniel Holcomb, and Russell Tessier. 2018. FPGA Side Channel Attacks without Physical Access. In *Field-Programmable Custom Computing Machines (FCCM), 2018 IEEE 26th Annual International Symposium on*. IEEE.

[48] Craig Ramsay and Jasper Lohuis. 2017. TEMPEST attacks against AES. Fox-IT whitepaper. Available at: https://www.fox-it.com/en/insights/blogs/blog/tempest-attacks-aes/.

[49] Falk Schellenberg, Dennis R.E. Gnad, Amir Moradi, and Mehdi B. Tahoori. 2018. An Inside Job: Remote Power Analysis Attacks on FPGAs. DATE 2018. Cryptology ePrint Archive, Report 2018/012 available at https://eprint.iacr.org/2018/012.

[50] Alexander Schlösser, Dmitry Nedospasov, Juliane Krämer, Susanna Orlic, and Jean-Pierre Seifert. 2013. Simple photonic emission analysis of AES. *Journal of Cryptographic Engineering* 3, 1 (01 Apr 2013), 3–15. https://doi.org/10.1007/s13389-013-0053-7

[51] Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard. 2017. Malware Guard Extension: Using SGX to Conceal Cache Attacks. *CoRR* abs/1702.08719 (2017). arXiv:1702.08719 http://arxiv.org/abs/1702.08719

[52] R.M. Secareanu, S. Warner, S. Seabridge, C. Burke, T.E. Watrobski, C. Morton, W. Staub, T. Teilier, and E.G. Friendman. [n. d.]. Physical design to improve the noise immunity of digital circuits in a mixed-signal smart-power system. *2000 IEEE International Symposium on Circuits and Systems. Emerging Technologies for the 21st Century. Proceedings (IEEE Cat No.00CH36353)* ([n. d.]). https://doi.org/10.1109/iscas.2000.858742

[53] Nader Sehatbakhsh, Alireza Nazari, Alenka Zajic, and Milos Prvulovic. 2016. Spectral profiling: Observer-effect-free profiling by monitoring EM emanations. In *Microarchitecture (MICRO), 2016 49th Annual IEEE/ACM International Symposium on*. IEEE, 1–11.

[54] A. Shamir and Y. Oren. 2007. Remote Password Extraction from RFID Tags. *IEEE Trans. Comput.* 56 (06 2007), 1292–1296. https://doi.org/10.1109/TC.2007.1050

[55] Colin Stagner. 2013. *Detecting and locating electronic devices using their unintended electromagnetic emissions.* Ph.D. Dissertation. Missouri University of Science and Technology.

[56] Evangelos Vasilakis. 2015. *An instruction level energy characterization of arm processors.* Technical Report FORTHICS/TR-450. Institute of Computer Science (ICS), Foundation of Research and Technology Hellas (FORTH).

[57] Tien Dang Vo-Huu, Triet Dang Vo-Huu, and Guevara Noubir. 2016. Fingerprinting Wi-Fi devices using software defined radios. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 3–14.

[58] Martin Vuagnoux and Sylvain Pasini. 2009. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In *Proceedings of the 18th Conference on USENIX Security Symposium (SSYM'09)*. USENIX Association, Berkeley, CA, USA, 1–16. http://dl.acm.org/citation.cfm?id=1855768.1855769

[59] Alenka Zajic, Milos Prvulovic, and Derrick Chu. 2017. Path loss prediction for electromagnetic side-channel signals. In *Antennas and Propagation (EUCAP), 2017 11th European Conference on*. IEEE, 3877–3881.

[60] Zeptobars. 2014. nRF51822 - Bluetooth LE SoC : weekend die-shot. https://zeptobars.com/en/read/nRF51822-Bluetooth-LE-SoC-Cortex-M0.

[61] M. Zhao and G. E. Suh. [n. d.]. FPGA-Based Remote Power Side-Channel Attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*, Vol. 00. 805–820. https://doi.org/10.1109/SP.2018.00049

A EXCERPT FROM NACSIM 5000

1-5. (~~C~~) Propagation of TEMPEST Signals (U). - There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (~~C~~) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (~~C~~) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (~~C~~) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (~~C~~) [Six lines redacted.]

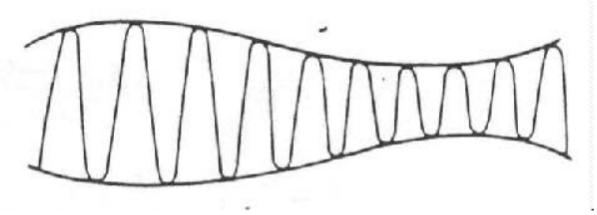


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

e. (~~C~~) Acoustics (U) - Characteristically plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays -- these produce sound. and consequently can be sources of compromise.

Appendix A: Excerpt from [41], discussing four propagation mechanisms of compromising emanations. Details about the third, "modulation of an intended signal", are redacted. Could the redacted text describe an effect similar to screaming channels?