Side-Channel Propagation Measurements and Modeling for Hardware Security in IoT Devices

Seun Sangodoyin, *Member, IEEE*, Frank Werner, *Student Member, IEEE*, Baki B. Yilmaz, *Student Member, IEEE*, Chia-Lin Cheng, *Student Member, IEEE*, Elvan M. Ugurlu, *Student Member, IEEE*, Nader Sehatbakhsh, *Student Member, IEEE*, Milos Prvulovic, *Senior Member, IEEE* and Alenka Zajić, *Senior Member, IEEE*

***Abstract*—The ubiquitous inter-connectivity of electronic devices offered by Internet-of-Things (IoT) networks has been increasingly embraced in a wide range of applications. In IoT networks, threats to hardware security are often not perceived as serious, with the assumption that an attack could only be carried out at close proximity. However, in this paper, we show that through Electromagnetic (EM) side-channel signal leakage, operational information and program activities of IoT devices and Field Programmable Gate Array (FPGA) modules can be garnered from approximately 200 m away in an outdoor Line-of-Sight (LOS) environment. We describe an extensive measurement campaign conducted to investigate the aforementioned leakage and provide propagation models that can be used to predict the power (and corresponding variation i.e., shadowing gain) of the EM side-channel signal emanation at various distances, scenarios and environments. With a circularly polarized receiver antenna, our results show that the received power of the emanated EM side-channel (carrier) signal varies from about -61 dBm at 1 m to about -112 dBm at 200 m in the outdoor LOS environment. Furthermore, a received signal power of about -73 dBm was observed at 1 m and -88 dBm was recorded at 10 m in an indoor LOS environment. Power variation (shadowing gain) of about 3.6 dB and 2.0 dB were observed in the outdoor and indoor environments, respectively. This work is relevant for EM side-channel leakage countermeasure development and provides pertinent information to embedded systems and wireless network security engineers.**

***Index Terms*—Electromagnetic wave propagation, Side-channel attacks, Internet of Things, statistical channel model.**

I. Introduction

THE emergence of Internet-of-Things (IoT) has led to advancements in personalized medical care, interaction between home (or office) appliances, and the promise of autonomous automobile, airline and smart grid systems. IoT can be described as a networked system of nodes/*smart* devices with sensing, computing and communication (often wireless) capabilities. These nodes range from smartphones to embedded sensor modules. The seamless inter-connectivity in IoT networks has also made them invaluable in a number of small-, large-scale tasks and critical infrastructure operations that affect people's daily lives.

There are, however, concerns about security vulnerabilities to embedded devices in IoT networks that could prove devastating or *at least* disruptive to people's lives. Recent demonstrations of security attacks on commercial products, e.g., pacemakers and insulin pumps [1], [2], have elevated the security of wireless medical devices from the realm of theoretical possibility to an immediate concern [3], while attacks on air-traffic control [4] have also shown potential vulnerabilities to large-scale IoT networks. Currently, security measures have been extensively explored in different layers of wireless network architecture [5], including the communication between devices [6], encryption [7], and user authentication [8]. However, side-channel security still lags behinds those of the upper layers since most concerns are often about software manipulations in wireless and cyber-physical networks.

EM side-channel attacks are analog-signal attacks that primiarily stem from unintentionally leaked EM radiation from electronic devices. EM side-channel attacks exploit sub-channels (at different frequencies and modulations) and use information gained or leaked from the physical implementation of a system to extract sensitive information such as cryptographic keys [9]. Some of the strongest EM side-channel signals are created when a periodic signal (such as an *on-board* clock signal) becomes amplitude or frequency modulated based on processor or memory activity. Algorithms such as "FASE" presented in [10] and the frequency-modulation detection procedure in [11] have been used to detect EM side-channel signals and can, in-turn, be used to predict operational activities of the device.

An essential step in the design of any wireless system is the measurement and modeling of the propagation channel in which this system is to operate. Currently, there are no propagation models to predict the range and conditions at which these emanated signals can be intercepted. To aid security vulnerability assessment in IoT networks, it is of utmost importance that a comprehensive and realistic characterization of EM side-channel signal propagation be conducted. The aforementioned characterization should be done with respect to distance, frequency, scenarios (Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS)) and environment as it will facilitate the development of necessary countermeasures to EM

Part of this work was presented at the 14^{th} European Conference on Antennas and Propagation (EuCAP) 2020, in Copenhagen, Denmark, $15-20$ March 2020. This work is supported, in part, by DARPA LADS contract FA8650-16-C-7620. The views and findings in this paper are those of the authors and do not necessarily reflect the views of DARPA.

S. Sangodoyin, F. Werner, B. B. Yilmaz, Chia-Lin Cheng, Elvan M. Ugurlu, and A. Zajić are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332-0250 USA (email: {seun.sangodoyin; fwerner6; b.berkayyilmaz; cheng; ugurlu}@gatech.edu, alenka.zajic@ece.gatech.edu).

Nader Sehatbakhsh and Milos Prvulovic are with the School of Computer Science, Georgia Institute of Technology, Atlanta, Georgia 30332-0250 USA (email: nader.sb@gatech; milos@cc.gatech.edu)

side-channel attacks.

A. Related Works

Several publications [9], [12]–[25] have investigated the concept of side-channel attacks and defenses over the years. Existing publications on side-channel attacks include works from [12], which studied acoustic side-channel emanation from printers and presented an attack that recovers what a dot matrix printer processing alphanumeric text is printing based on the sound made by the printer. The concept of using power consumption measurements to find secret keys from tamper resistance devices was explored in [13], while power analysis attacks against smart cards implementation of modular exponentiation algorithms were explored in [14]. Work in [18] presented a new metric called *Signal Available to Attacker* (SAVAT), which explores the EM side-channel signal generated as a consequence of the difference in the execution of two program activities in a computer system. Near-field measurement (with the receiver probe placed at 10 cm above the device-under-test) of EM side-channel signals generated from different computer systems was measured and compared in [19]. Spectral profiling was used to monitor EM side-channel signal emanation in [20]. Work in [9] presented the use of EM side-channel attacks to retrieve the secret exponent from a single decryption on arbitrary ciphertext in an RSA cryptosystem. Work in [21] investigated the propagation mechanisms of EM side-channel signals at different frequencies and proposed models for near-field and far-field propagation; however this was done for a small sample of distances (≤ 3 m) and frequency points. Work in [22] introduced the concept of *screaming channels*, which occurs when EM leakage from digital logic in a mixed-signals chip is inadvertently combined with the radio carrier and is then amplified and transmitted by the antenna in a transceiver module. Their work showed that improper separation of digital and analog components leads to novel side-channel attacks that can break cryptography implementation in mixed-signal chips over at least 10 m. In our conference paper [25], we provided preliminary results for the measurement campaign that underlies the current paper, in particular, EM side-channel signal propagation in an indoor environment. However, we did not provide results from EM side-channel propagation in an outdoor environment; unique spectral signature given off by various instructions sets running on the IoT devices; also a more comprehensive indoor model has been provided in this paper – with the inclusion of the environment-dependent shadowing gain and board (angular) orientation dependent shadowing gain.

Existing work on defense (countermeasures) includes [15], which introduced a systematic methodology for automatic application of software countermeasures to thwart power analysis attacks. Cache based side-channel attacks were analyzed in [17] with the introduction of new security aware cache designs. A technique for preventing timing attacks used by adversaries in finding fixed Diffie-Hellman exponents and factor RSA keys was presented in [23]. Work in [13] and [24] both presented countermeasures to preventing the use of power measurements to find secret keys in electronic devices.

B. Contributions

To the best of our knowledge, no work details measurements and modeling of EM side-channels signals in a long-distance (excess of 10 m) outdoor or indoor environment for LOS and NLOS scenarios. In an effort to fill this gap, we have conducted extensive measurements in the aforementioned scenarios and are able to show that operational information and program activities of IoT devices can be monitored from long distances. Contributions of this paper can be summarized as follows:

1) We detail an extensive channel measurement campaign conducted using different measurement setups in various scenarios and environments.
2) We find that EM side-channel signals can be garnered at approximately 200 m away in an outdoor LOS environment.
3) We find that the received power of the EM side-channel signal exhibits a monotonically decreasing relationship with distance. We provide a detailed statistical model that can be used to predict the aforementioned received power (along with subsequent variations (i.e., shadowing gain)) at different distances, scenarios and environments.
4) We provide details about the EM side-channel signal generation procedure for the SAVAT microbenchmark. The signal was used as propagation channel excitation waveform in our work.
5) We find that instruction sets that run on IoT devices lead to EM side-channel emanations with unique spectral signatures, which can be used to track the electronic device's operation.
6) We remotely monitored segments of two regular programs, *bitcount* and *basicmath*, running on an IoT device. We find that the operation sequence of these programs can be detected and monitored from long distances in both outdoor and indoor environments.

C. Organization

The rest of this paper is organized as follows. Section II describes the generation of EM emanation and the various benchmark (and microbenchmark) programs running on the IoT and FPGA devices. The channel measurement campaigns conducted are discussed in section III. Section IV describes the data processing procedure and the obtained results while summary and conclusions are inferred in section V.

II. EM Emanation and Channel excitation waveform

The EM side-channel signal propagation characterization proposed in this work will require a *controlled* emanation of the signal from the IoT device. This signal will serve as the channel excitation waveform. In this section, we discuss the procedure for generating the aforementioned EM side-channel signal using a microbenchmark SAVAT [18]. Furthermore we discuss the signal emanation as a result of two realistic applications, *bitcount* and *basicmath*, running on the IoT device.

A. Excitation Procedure

Using SAVAT [18], controlled emanations were generated by executing two types of program activities repeatedly on the IoT device. Typical program activities include simple instructions such as addition, subtraction, multiplication, division, load, and store. Sequential invocation of a pair of instructions leads to electric current being drawn repeatedly from the device's power supply. Any difference in the magnitude of the current drawn when executing the two activities results in a periodic current being superimposed onto the traces on the device, thereby emanating an EM field–an excitation signal.

```
for(j=0;j< n_out; i++){
  // Invoke instances of the X instruction
  for(i=0;i< n_X; i++){
    ptr1=(ptr1&~mask1)|((ptr1+offset)&mask1);
    // The X-instruction, e.g. a load
    value=*ptr1;
  }
  // Invoke instances of the Y instruction
  for(i=0;i< n_Y; i++){
    ptr2=(ptr2&~mask2)|((ptr2+offset)&mask2);
    // The Y-instruction, e.g. a store
    *ptr2=value;
  }
}
```

Fig. 1: Microbenchmark pseudo-code for generating the excitation signal [18].

An example of the microbenchmark used to generate the excitation signal is shown in Fig. 1. In this example, the first program activity is the X instruction (indicated in the code) and the second activity is the Y instruction. The program is comprised of two smaller for-loops contained in an outer for-loop. The first inner for-loop repeatedly executes the X instruction while the second inner for-loop repeatedly executes the Y instruction. The variables n_{X} and n_{Y} define the number of times X and Y are executed in their respective for-loops. The variable n_{out} represents the number of times the pattern of X/Y is executed by the outer for-loop. One iteration of the outer for-loop is equal to one period, T_{alt}, of the excitation signal. Hence, we will define an alternation frequency, f_{alt} as $\frac{1}{T_{\mathrm{alt}}}$.

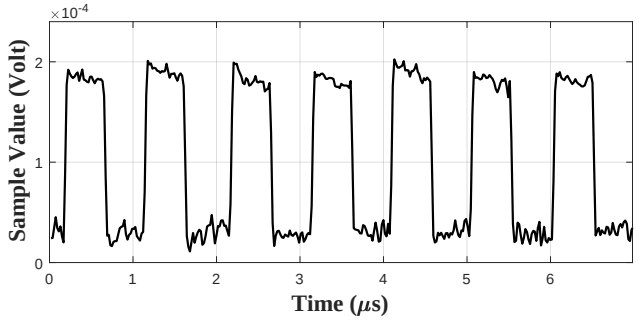


Fig. 2: Example of the waveform generated by the X/Y alternation activity.

An example of the waveform generated by the microbenchmark is shown in Fig. 2. Although the execution of each program activity should take an equal length of time [18], realistically this is hardly the case as there are usually some variations. If we define the amount of time it takes to execute X as t_{X} and the time it takes to execute Y as t_{Y}, then the total execution time for the instructions can be calculated as

$$T_{\mathrm{alt}} = t_{\mathrm{X}} \times n_{\mathrm{X}} + t_{\mathrm{Y}} \times n_{\mathrm{Y}}. \quad (1)$$

Given that manipulating the values of n_{X} and n_{Y} changes T_{alt} (see (1)), it is therefore possible to tune f_{alt} to a part of the frequency spectrum with little interference. If both activities are executed for the same amount of time during one period, the generated waveform is considered to have a 50% duty cycle. For this work, the excitation signals were set to a duty cycle of 50%.

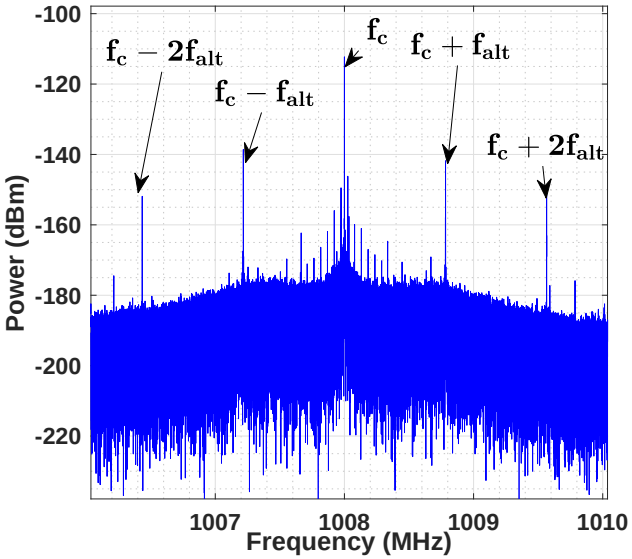
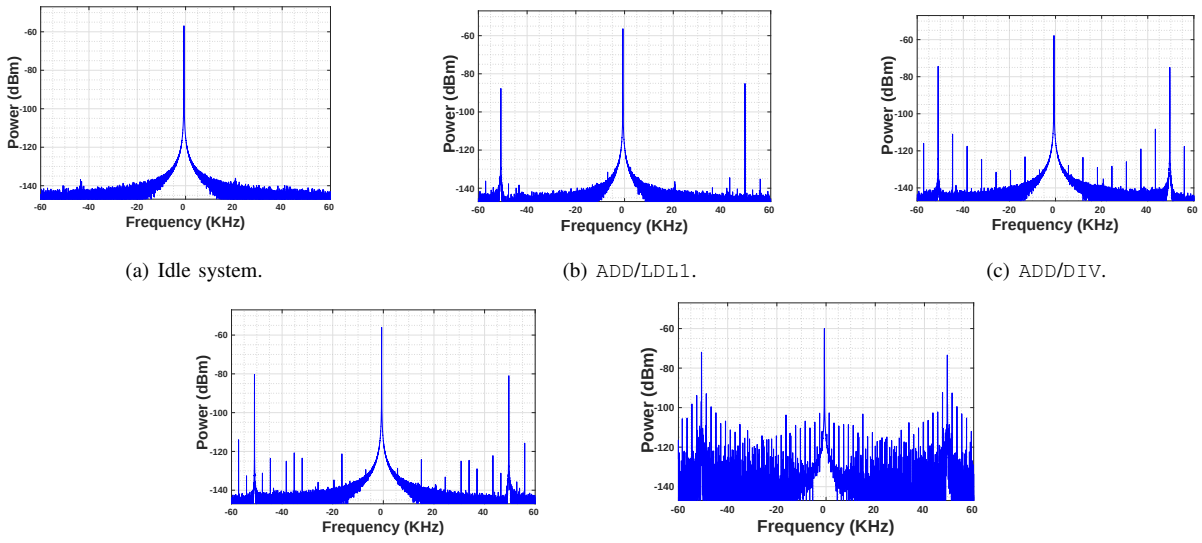


Fig. 3: Example of the processor clock being modulated by a 1 MHz excitation signal.

	Instruction	Description
LDM	mov eax, [esi]	Load from main memory
LDL1	mov eax, [esi]	Load from L1 cache
ADD	add eax, 173	Add imm to reg
DIV	idiv eax	Integer division
NOP		No instruction

TABLE I: x86 instructions for our X/Y ESE measurements.

In theory, generating signals with any desired alternation frequency is possible. However, this becomes difficult with increasing values of f_{alt} as clock timing of the device limits the flexibility by introducing constraints on the total execution time of any inner for-loop. The excitation signal also amplitude modulates other periodic signals generated by the device. In this situation, the clocks of the components (such as the processor and memory) used for executing the alternating program activity act as carriers for the modulating waveform. During normal operations, the clocks produce periodic currents



(a) Idle system. (b) ADD/LDL1. (c) ADD/DIV.

(d) ADD/STR. (e) ADD/LDM.

Fig. 4: The spectrum of the emanated signal for different instruction pairs with the frequency normalized relative to f_c.

at the clock frequency, f_c, along the device's traces, thereby generating an EM field. When the alternating program activity is executed, the periodic current from the clock is then modulated. Fig. 3 shows an example of the power spectrum generated when a device's 1.008 GHz processor clock is modulated by a 1 MHz excitation signal. The figure confirms modulating program activities, which results in sidebands at $f_c \pm f_{alt}$ and its harmonics. In this work, we will refer to f_c as Carrier, while $f_c + f_{alt}$ and $f_c - f_{alt}$ will be referred to as Upper-Sideband (USB) and Lower-Sideband (LSB) frequencies respectively. Note that the distinct peaks of the power spectrum at the Carrier, USB and LSB frequencies correspond to the received power at the these frequencies.

B. Spectral Signature of Emanated Signals

Emanated EM side-channel signals stemming from a pair of instruction sets (see Table I) have unique spectral signatures. This can be attributed to factors ranging from instruction[1] processing order to the use of different computational parts of a processor [26]. In this paper, the instruction sets (given in Table I) range from load(s) that can access different levels of the cache/memory hierarchy to simple addition, which represents the arithmetic logic unit (ALU) and integer division (DIV), and the "No Instruction" case where Line 6 or Line 12 in Fig. 1 are simply left empty.

To show the different spectral signature of various instruction pairs, we conducted tests in which the alternation frequency was kept constant while changing the instruction pairs. The outcome of our tests is summarized below.

- The power spectrum in Fig. 4(a) was obtained with an idle processor i.e., without any activity running. However, the power spectrum of the clock signal of the device was still visible. This figure serves as a *baseline* for comparing other activities running on the processor.
- With the alternating frequency set to 50 kHz the power spectrum given in Fig. 4(b) was measured while running the LDL1/ADD instruction pair. The two peaks representing the sidebands are clearly observable at both sides of the normalized center frequency.
- Using instruction pair ADD/DIV results in the power spectrum shown in Fig. 4(c). From this figure, in addition to the observed sidebands, several low-powered components spread are also visible.
- The power spectrum of the other instruction pairs such as ADD/STR and ADD/LDM are shown in Fig 4(d) and 4(e) with distinct spectral signatures.

It is clearly observable that if an eavesdropper can associate the unique features of the spectral shape to an instruction pairs, this can result in the leakage of operational information – a security vulnerability, which can be explored to nefarious ends.

C. Benchmark Programs

Benchmarks are applications commonly used for performance evaluation of embedded processors. A publicly available suite for characterizing ARM-based processors is the MiBENCH embedded benchmark suite [27]. *Bitcount* and *basicmath* are two out of several applications provided by MiBENCH and will be used to study EM side-channel leakage in this work. Unlike the excitation program used for SAVAT, *bitcount* and *basicmath* are not designed to maximize the amount of EM emanation from a device. Instead, *bitcount* and *basicmath* are a better representation of more complex programs since they are comprised of multiple segments of program activity instead of just one. These benchmarks are described below:

1) ***Bitcount****: Bitcount* program tests the bit manipulation abilities of a processor by counting the number of bits in an array of integers [27]. The *bitcount* was implemented in our IoT device by running seven segments of distinct tasks within

[1]Here, *instructions* refer to the commands that a processor can execute.

the *bitcount* operation. The tasks performed in each segment are itemized below:

- Segment 1 - Optimized 1-bit per loop count.
- Segment 2 - Ratko's mystery algorithm.
- Segment 3 - Recursive bit count by nibbles.
- Segment 4 - Non-recursive bit count by nibbles.
- Segment 5 - Non-recursive bit count by bytes (BW).
- Segment 6 - Non-recursive bit count by bytes (AR).
- Segment 7 - Shift and count bits.

2) ***Basicmath****:* The *basicmath* program performs simple mathematical calculations that often do not have dedicated hardware support in the embedded processor [27]. In our work, *basicmath* was implemented by running four segments with distinct tasks itemized below:

- Segment 1 - Cubic function solution.
- Segment 2 - Integer square root calculations.
- Segment 3 - Angular conversion from degrees to radians.
- Segment 4 - Angular conversion from radians to degrees.

Note that a fixed set of constants were used as input data for these programs.

Bitcount and *basicmath* generates peaks at distinct frequencies during each segment of the execution. It will be shown that these peaks can be remotely monitored at long proximity ranges as a result of EM side-channel leakage.

III. Measurement Campaign

In this section, detailed descriptions of the measurements conducted in various environments using different experimental setups are presented.

A. Outdoor Measurements

1) ***Measurement Environment****:* The outdoor measurements were conducted on a walkway adjacent to a quadrangle on the campus of the Georgia Institute of Technology (Georgia Tech), in Atlanta, GA, USA. The structural layout of the measurement site with TX and RX placements at various locations are shown on the map in Fig. 5. To avoid congestion, only a subset of the measured positions are marked on the map. The measurement site is an open area surrounded by buildings and trees with the ground of the walkway paved with a mixture of brick and concrete slabs while lamp posts are placed alongside its edges. The measurements were conducted between Clough Undergraduate Learning Commons and the Klaus Advanced Computing Building with five other buildings surrounding the measurement area. The aforementioned buildings boast a modern-contemporary architectural facade – a makeup of concrete, bricks, metal sheet and glass window panes.

2) ***Measurement Setup****:* We designed and assembled a task-specific system for this outdoor measurement campaign. The block diagram of the measurement setup is shown in Fig. 6. A list of the equipment used and corresponding parameter settings have been presented in Tables II and III. Note that while all the equipment are either commercially available as over-the-counter (OTC) products or with designs published in the public domain, it is the specific combination thereof that makes the system uniquely suited for our investigation into long-range detection and monitoring of EM side-channel signals.

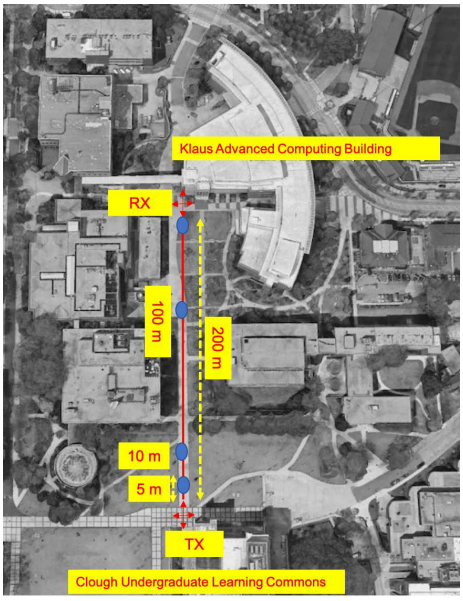


Fig. 5: Map of the measurement area in the outdoor environment.

At the TX end of the measurement setup is an EM source/emitter (IoT) board (Olimex A13-OLinuXino-MICRO) [28] and a Personal Computer (PC). The Olimex[2] is an open-source embedded ARM linux computer with an A13 cortex-A8 processor and an on-board clock frequency of 1.008 GHz. The Olimex was configured to run different programs such as SAVAT and *bitcount*. A PC was connected to the Olimex for control purposes while also providing power. At the RX end is a high gain antenna, which was connected to a Spectrum Analyzer (SA, N9030B). Two types of receiver antennas (with both designed and built in-house) were used for this experiment. The aforementioned antennas include: a high-gain quadrature array of nonuniform helical antennas (abbreviated as QHA) [29] and; a Planar Disc Antenna (PDA) [30]. As stated in [29], the QHA is circularly polarized with a directive gain of approximately 20.5 ± 1.5 dBi in the frequency range 0.9 GHz to 1.1 GHz (and a gain of 21 dBi at 1.008 GHz). The PDA is vertically polarized and was designed to operate over a bandwidth of 50 MHz centered around 1 GHz. The broadside gain of the PDA is approximately 17 dBi at 1.008 GHz with a peak gain of 19 dBi at about 1.012 GHz. Pictures of the measurement setup using QHA and PDA antenna deployments in the outdoor environment are shown in Figs. 7(a) and 7(b).

We ran the instruction set MUL/ADD[3] in SAVAT for this particular experiment while setting f_{alt} to 500 kHz. Measurements were conducted in a LOS scenario with TX and RX separation distances of 5, 10, 20, 50, 100, 130 and 200 meters respectively. In addition to the usage of two types of

[2]For simplification, we will henceforth replace the *term* "EM source/emitter" with the type of board (manufacturer's name e.g., "Olimex") being used for each measurement in this work.

[3]MUL (muli r22, r22,173 – integer multiplication) instruction is supplemental to the instructions sets in Table I discussed in Section II.

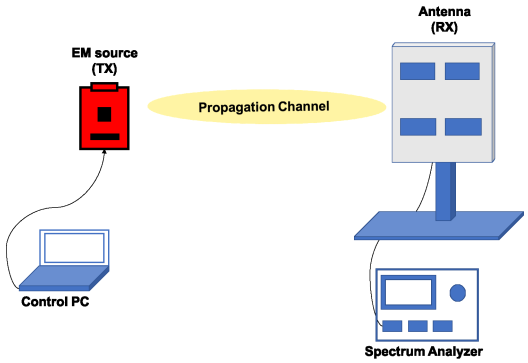
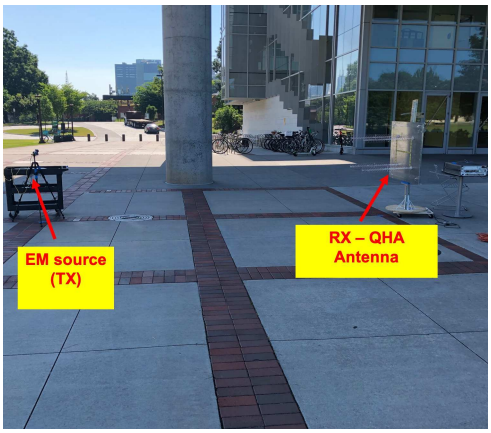
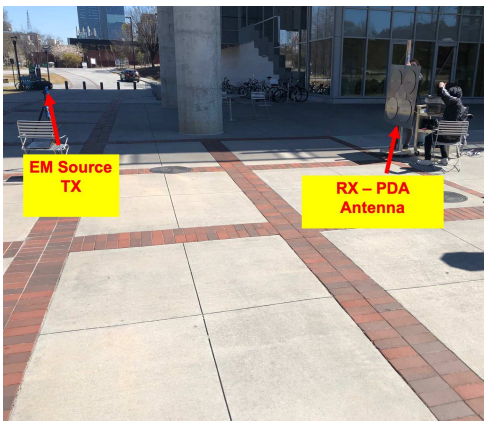


Fig. 6: Measurement setup



(a) QHA



(b) PDA

Fig. 7: LOS measurement setup with QHA and PDA antennas.

receiver antennas, the outdoor measurements were conducted with different Olimex board polarization (as shown in Fig. 8). Note that the exact same locations[4] (with constituents unchanged) were used for all experiments so as to aid assessment and comparability of results. The sequence in which the experiments were conducted is such that all measurements (distance and polarization) were conducted with a particular

[4] At each measured distance, the emitter device's location was marked on the floor as shown in Figs. 5. We strictly adhered to placements at these markings for all the measurements conducted so as not to create different channel realizations.

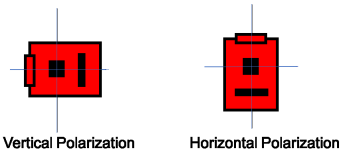


Fig. 8: EM source board polarization.

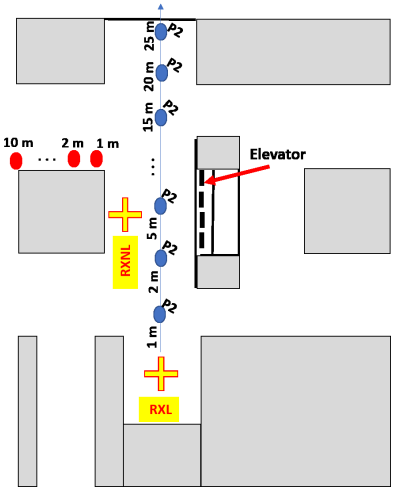


Fig. 9: Floor map of the indoor environment.

antenna before switching to another type of antenna.

To further demonstrate our ability to monitor programs running on IoT devices, the distance measurements were repeated for the Olimex while it executed *bitcount*.

Item	Manufacturer	Model No.
IoT board	Olimex	A13-OLinuXino-MICRO
Spectrum Analyzer	Keysight	N9030B
QHA antenna	Self-fabricated	N/A
PDA antenna	Self-fabricated	N/A
Control PC	Dell	Precision 7720

TABLE II: Equipment used in the outdoor measurement.

Parameters	Settings
Alternating freq. f_{alt}	500 kHz
Spectrum Analyzer center freq.	1.008 GHz
Spectrum Analyzer bandwith	8 MHz
Spectrum Analyzer res. bandwidth	136 Hz
QHA gain at center freq.	21 dBi
QHA bandwidth	200 MHz
QHA freq. range	0.9-1.1 GHz
QHA polarization	Circular
PDA gain at center freq.	17 dBi
PDA bandwidth	50 MHz
PDA freq. range	0.975-1.25 GHz
PDA polarization	Vertical

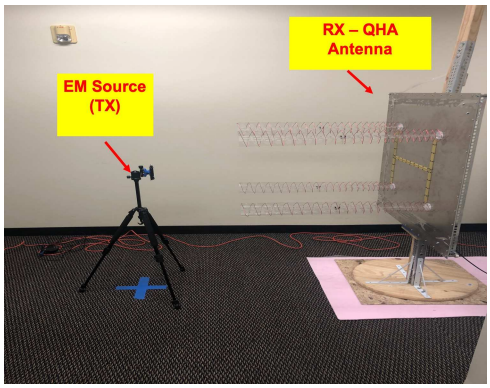
TABLE III: Parameters and settings of the equipment used in the outdoor measurement.

It is important to note that the TX and RX ends were operated in a distributed setup fashion i.e., without synchronization. Such a configuration is similar to how an eavesdropper's setup would most likely be deployed. The duration (including setup

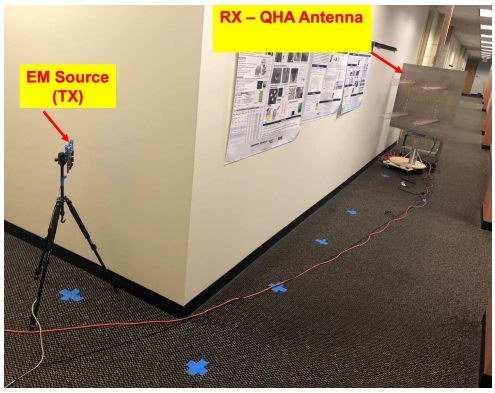
time) of the outdoor measurement was approximately 2 hours. We made sure that there were no moving objects or personnel in the channel during the measurements.

B. Indoor Measurements

*1) **Measurement Environment**:* The indoor measurements were conducted at the Technology Square Research Building (TSRB) – a building adjacent to the campus of Georgia Tech. TSRB is five-storied comprising of office spaces and large open hallways. The ceiling and walls surrounding each large open hallway are made of concrete, wood and steel framed glass panes (used for office space demarcations) while plastic covered lighting fixtures hang down from the ceiling. The hallway floors are carpeted with Olefin fiber rugs and four elevator cars were fitted into the walls. A structural layout of the measurement site is provided in Fig. 9.



(a) LOS



(b) NLOS

Fig. 10: Measurement setup in the indoor LOS and NLOS scenarios.

*2) **Measurement Setup**:* The setup used for the indoor measurements is similar to that described in section III-A (see Fig. 6) with the exception that QHA was the only RX antenna used in the indoor experiments. Measurements were conducted for LOS and NLOS scenarios in and around the large hallways at TX-RX separation distances of 1, 2, 5, 10, 15, 20 and 25 m for the LOS and 1, 2, 3, 5, 8, and 10 m for the NLOS cases respectively. The measurement positions for the LOS and NLOS cases are indicated in Fig. 9 with labels "RXL" and "RXNL" indicating the RX placement for LOS and NLOS cases respectively. With the RX fixed, the Olimex was moved to different locations to create the various TX-RX separation distances. At each distance, the Olimex was then rotated through 90° angular increments i.e., from 0° to 270° (as shown in Fig. 11) with measurements conducted at each angle. The rotation was carried out so as to characterize any power variation, which could stem from radiation dependency on board's angular orientation. Pictures of the measurement setup for both LOS and NLOS scenarios are shown in Figs. 10(a) and 10(b). Note that the measurements were conducted with EM signals emanation as a result of SAVAT, *bitcount* and *basicmath* running on the IoT device. These measurements were conducted with the Olimex set to its vertical polarization orientation.

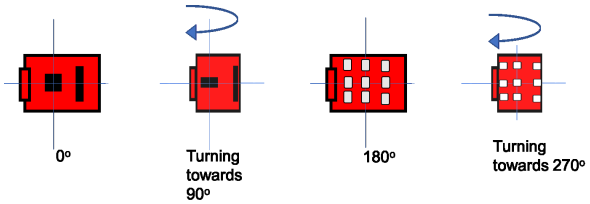


Fig. 11: EM source (clockwise) rotation.

C. Indoor FPGA Measurements

*1) **Measurement Environment**:* Measurements were conducted in a similar environment to that described in section III-B.

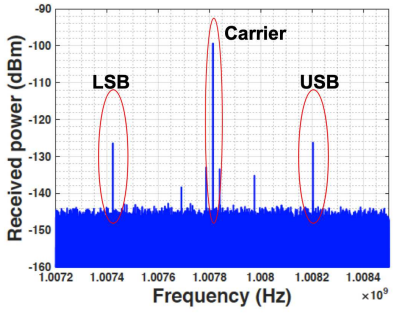
*2) **Measurement Setup**:* The setup used for this indoor experiment is similar to that described in section III-A and B (see Fig. 6) with the exception of the EM source/emitter used. An FPGA (DE0-CV Cyclone V) board [31] was used as the EM source in this experiment. The DE0-CV is a development board using the Altera Cyclone V FPGA with an on-board processor clock frequency of 50 MHz. We ran the instruction set MUL/ADD in SAVAT (with f_{alt} set to 500 kHz) on the FPGA board for this experiment. With the relatively low[5] fundamental frequency of the on-board clock, we were only able to capture the 20^{th} harmonic of the EM side-channel signal within the operation frequency range 0.9 to 1.1 GHz of the RX antenna (QHA). It is important to note that the use of the 20^{th} harmonic of the EM side-channels signals does not preclude the remote monitoring of operational information of the FPGA.

Measurements were conducted for a LOS scenario at P2 (see Fig. 9) in the large hallways at TX-RX separation distances of 1, 2, 5, and 10 m.

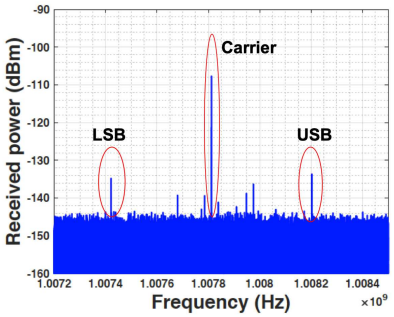
IV. Data Processing and Results

The received power of the Carrier, USB and LSB (created by SAVAT) were recorded at the various distances measured. Sample plots of the received power spectrum for the outdoor measurement at select distances of 20 m and 100 m have been provided in Figs. 12(a) and 12(b). It can be observed from

[5]This is lower than the 1.008 GHz of the Olimex IoT board.



(a) 20 m



(b) 100 m

Fig. 12: Power spectrum of received signal in the outdoor environment for TX-RX separations of (a) 20 m and (b) 100 m.

the figures that the Carrier and accompanying side-bands have significant Signal-to-Noise Ratio[6] (SNR) values at the select distances.

It is important to note that the motivation for using the models proposed in this work is primarily due to its similarity to the conventional power law [32], which is a standard procedure for modeling pathloss and shadowing gain and has been used in [33]–[36]. However, modifications (to the power law) introduced in our models are mainly out of necessity. One of the challenges in predicting propagation loss of EM side-channel signals is that the transmit power and transmit "antenna" gain are unknown [21]; therefore pathloss cannot be computed using the aforementioned (traditional) power law model directly. In this work, we have modeled the received power and corresponding pathloss (at all measured distances) relative to the power received at a reference distance. We have also modified the shadowing gain model to include power variation due to both environment and board angular rotation in certain experiments. Due to differing experimental setup and data storage structures, the evaluation procedure for the various measurements are discussed separately.

A. Results from Outdoor Measurement

For the outdoor measurement, the recorded data structure of the received power can be represented as $M^{\kappa,\psi,\alpha,p}$, where $\kappa \in [1, 2, ..., 7]$ denotes the indexes of the distances measured such that $d_\kappa \in [5, 10, 20, 50, 100, 130, 200]$ m, while $\psi \in [1, ..., \Psi = 3]$ represents the carrier and sidebands such that $\psi = 1, 2, 3$ denotes Carrier, USB and LSB respectively. $\alpha \in [1, ..., A = 2]$ indicates the antenna type used with $\alpha = 1$ representing QHA while $\alpha = 2$ represents PDA. $p \in [1, ..., P = 2]$ indicates the Olimex board polarization where $p = 1$ corresponds to vertical polarization and $p = 2$ represents horizontal polarization. A model for the distance-dependent pathloss and shadowing gain parameters are presented in this section.

*1) **Distance-dependent pathloss**:* With consideration for parameters κ, ψ, α, p, the received power from the empirical data can modeled as:

$$M^{\kappa,\psi,\alpha,p} = M_0^{\psi,\alpha,p} \cdot \left(\frac{d_\kappa}{d_0}\right)^{\eta^{\psi,\alpha,p}} \cdot \xi^{\kappa,\psi,\alpha,p} \tag{2}$$

where M_0 is the power received at the reference distance d_0 (chosen as 1 m), η is the pathloss exponent, and ξ is a random variable describing shadowing gain in the environment. Figs. 13(a)-13(d) show the scatter plot of the received power at distances measured using different antennas and EM source polarization for Carrier, USB and LSB respectively. A linear regression fit for the scatter plot shows a monotonic dependence of the received power on distance. Values of parameters such as M_0 and η were extracted through the linear fit on the empirical data and have been provided in Table IV.

It can be observed from Table IV that M_0 (dBm) values from the carrier are similar in both vertical and horizontal polarizations for measurements conducted using the QHA antenna, while the sidebands (USB and LSB) slightly differed by about 3 dB between both polarizations. The closeness in value between results from both polarizations can be attributed to the fact that QHA is circularly polarized and, therefore, mostly immune to any polarization changes by the EM source. For the PDA, however, a noticeable difference of about 10 dB can be observed in the M_0 (dBm) values from the Carrier while sidebands differed by about 6-7 dB in the vertical and horizontal polarization measurements. This disparity is primarily due to the fact that the PDA is vertically polarized hence the polarization preference. It can also be observed that the pathloss exponent η values are comparable for the carrier, USB and LSB for both antennas at the respective polarizations with the exception of the PDA in the horizontal polarization.

*2) **Shadowing gain**:* Shadowing gain (denoted as ξ in (2)) is obtained by computing the deviation of the received power (M) at each measured location from the linear regression fit. The linear regression fit can be expressed as

$$\Phi^{\kappa,\psi,\alpha,p} = \Phi_0^{\psi,\alpha,p} \cdot \left(\frac{d_\kappa}{d_0}\right)^{\eta^{\psi,\alpha,p}}, \tag{3}$$

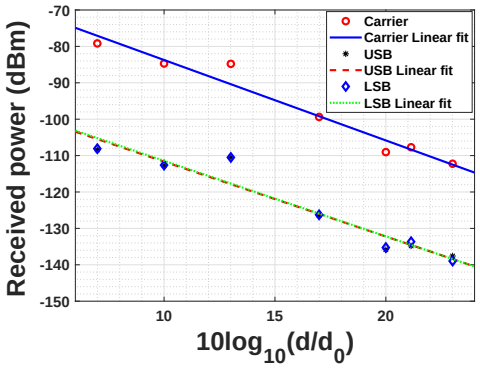
with the shadowing gain computed as

$$\xi^{\kappa,\psi,\alpha,p} = \frac{M^{\kappa,\psi,\alpha,p}}{\Phi_0^{\psi,\alpha,p} \cdot \left(\frac{d_\kappa}{d_0}\right)^{\eta^{\psi,\alpha,p}}}. \tag{4}$$

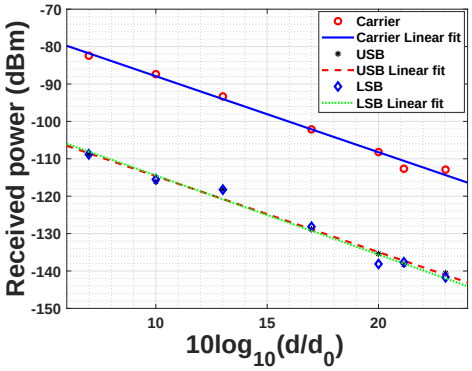
Note that Φ_0 in (3) is equivalent to M_0 in (2).

We modeled the logarithmic equivalent of the extracted shadowing gain as a Gaussian distribution

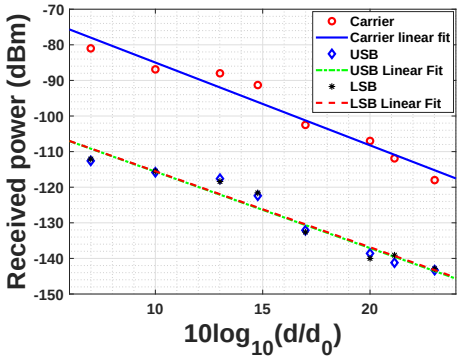
[6]Note that the Signal-to-Noise Ratio of each component (i.e., Carrier, USB, and LSB) is computed by subtracting the noise level (≈ -146 dBm) from the peak of its power spectrum (in dBm) in the spectrum.



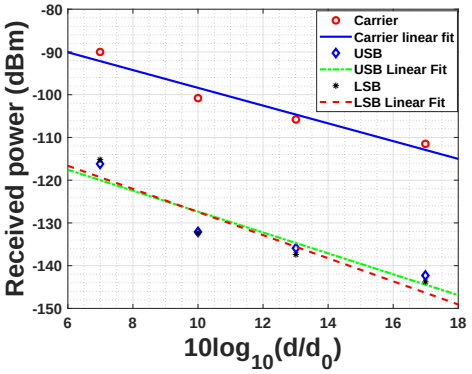
(a) QHA V-pol



(b) PDA V-pol

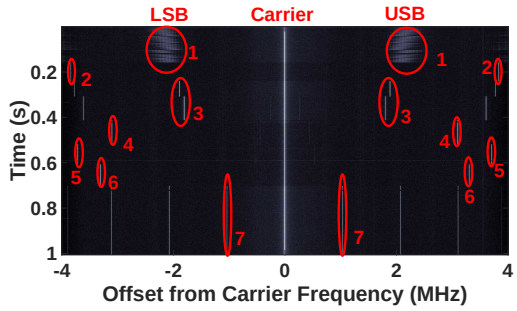


(c) QHA H-pol

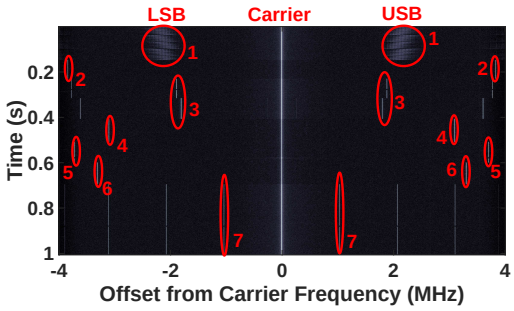


(d) PDA H-pol

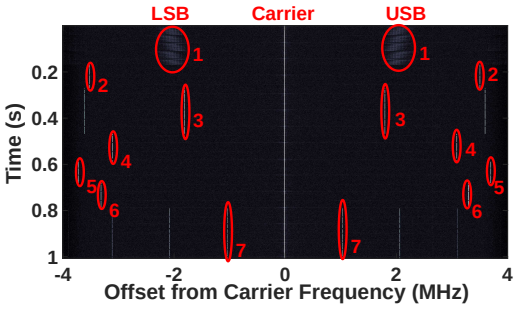
Fig. 13: Linear regression fit for received power over distance in LOS scenario with different antennas and polarization in the outdoor environment.



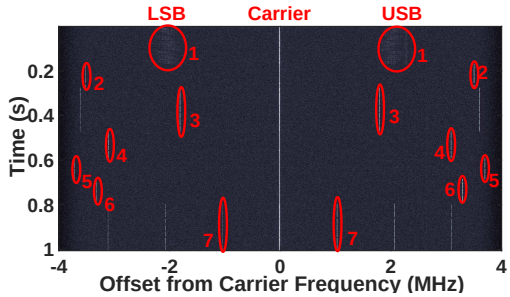
(a) 5 m



(b) 10 m



(c) 20 m



(d) 50 m

Fig. 14: *Bitcount* results at various measured distances in the outdoor environment.

$\mathcal{N}(\mu_\xi(\text{dB}), \sigma_\xi(\text{dB}))$, with the first and second moment parameters computed as

$$\mu_\xi^{\psi,\alpha,p}(\text{dB}) = \mathbb{E}_\kappa \left\{ 10 \cdot \log_{10} \left(\frac{M^{\kappa,\psi,\alpha,p}}{\Phi_0^{\psi,\alpha,p} \cdot \left(\frac{d_\kappa}{d_0}\right)^{\eta^{\psi,\alpha,p}}} \right) \right\} \quad (5)$$

$$\sigma_\xi^{\psi,\alpha,p}(\text{dB}) = \mathbb{D}_\kappa \left\{ 10 \cdot \log_{10} \left(\frac{M^{\kappa,\psi,\alpha,p}}{\Phi_0^{\psi,\alpha,p} \cdot \left(\frac{d_\kappa}{d_0}\right)^{\eta^{\psi,\alpha,p}}} \right) \right\} \quad (6)$$

where $\mathbb{E}_{\hat{r}}\{\cdot\}$ and $\mathbb{D}_{\hat{r}}\{\cdot\}$ are the expected value and standard deviation operators over an ensemble of the parameter $\hat{r}$ respectively. This is a standard modeling procedure for the shadowing gain and has been reported in [32] and [33]. The mean value of the logarithmic equivalent of the shadowing gain i.e., (μ_ξ(dB)) was found to be zero in our work while the computed standard deviation values (σ_ξ(dB)) has been provided in Table IV. Although the values of $\sigma_\xi(\text{dB})$ are similar for measurements conducted with same antenna, it is, however, noticeably different for measurements conducted using the different antennas.

It is important to note that the discrepancies in the results between the QHA and PDA can be attributed to the characteristics of the antennas and how they influence propagation in the channel. For example, the (approximately) 6 dB difference in M_0 (for the carrier) between QHA and PDA can be accounted for by the difference in antenna gain values at the carrier frequency of 1.008 GHz. In addition to this, the larger beamwidth of the QHA affords the aggregation of more multipath components therefore leading to a high receiver power. The shadowing gain disparity can be attributed to the variation in power of the higher number of multipath components captured by the antenna with the wider beamwidth.

3) ***Bitcount****:* As discussed in Section III-A.2, the program *bitcount* was used to demonstrate how well the IoT device's emanation is received. From our measurement results, using a visual approach, we look to identify the frequency peaks generated by each segment of *bitcount* at each distance measured. Sample spectrogram plots at select distances are displayed in Figs. 14(a) - 14(d). Note that in the spectrogram, all frequency values plotted on the *x-axis* have been normalized to that of the Carrier frequency. The centered line (at 0 MHz) represents the power spectrum of the Carrier over the 1 s measurement duration while the USB and LSB power spectrum are shown on opposite sides of the Carrier respectively. It can be observed from Figs. 14(a)-14(d) that the peaks corresponding to all seven segments of *bitcount* can be easily identified[7]. Note that to aid our discussion (and for clear representation), we have chosen to only provide spectrogram plots at distances of $5, 10, 20$ and 50 m since these sets of plots gave the best color[8] contrast. Each set of "shorter-lines" (circled and numbered on the spectrogram plots) corresponds to the segment of *bitcount* being executed during that period of time. It can be observed that while most of the segments generate sharp, identifiable lines at specific frequencies, segment 1 of *bitcount* consistently generated a "smeared" line on the spectrogram at all distances measured. Furthermore, the frequency of the peak occasionally shifted between two values while the Olimex executes segment 3 of *bitcount* thereby leading to two contiguous lines appearing during its execution. The aforedescribed effects are clearly observable at the 5 m and 10 m measurements shown in Figs. 14(a) and 14(b).

It can be deduced from the results provided in this work that EM side-channel signals emanation stemming from regular programs such as benchmarks running on the IoT devices are in fact identifiable and can be monitored at long distances.

Vertical polarization						
	QHA			**PDA**		
	M_0 (dBm)	η	σ_ξ (dB)	M_0 (dBm)	η	σ_ξ
Carrier	-61.64	-2.21	3.6	-67.59	-2.03	1.1
USB	-91.09	-2.05	3.5	-94.32	-2.03	1.3
LSB	-90.68	-2.08	2.8	-93.30	-2.11	1.6
Horizontal polarization						
	QHA			**PDA**		
	M_0 (dBm)	η	σ_ξ (dB)	M_0 (dBm)	η	σ_ξ
Carrier	-61.70	-2.32	3.0	-77.61	-2.07	2.1
USB	-94.16	-2.14	2.7	-102.89	-2.44	3.7
LSB	-94.20	-2.13	2.8	-100.41	-2.70	4.0

TABLE IV: Extracted propagation channel parameters in the outdoor environment.

B. Result from Indoor Measurements

A model for the distance-dependent pathloss and shadowing gain along with corresponding statistical distribution fits are discussed in this section. Note that this model is an extension of that presented in section IV.A with the shadowing gain defined as the combination of the environment-dependent and board (angular) orientation-dependent shadowing gain (i.e., "board shadowing").

The data structure of the received power in the indoor measurements can be represented as $Q^{\kappa_c,\psi,c,o}$, where $c \in [1, 2]$ denotes the LOS and NLOS scenarios with $c = 1$ indicating LOS and $c = 2$ indicates NLOS. κ_c denotes the index of the scenario distances such that $\kappa_{c=1} \in [1, 2, ..., 7]$ are distance indexes for the LOS scenario while $\kappa_{c=2} \in [1, 2, ..., 6]$ represents distance indexes for the NLOS scenario. Note that $d_{\kappa_{c=1}} \in [1, 2, 5, 10, 15, 20 \text{ and } 25]$ m while $d_{\kappa_{c=2}} \in [1, 2, 3, 5, 8 \text{ and } 10]$ m. $\psi \in [1, ..., \Psi = 3]$ denotes sidebands and carrier indexes such that $\psi = 1, 2, 3$ indicates USB, Carrier and LSB respectively while $o \in [1, ..., O = 4]$ denotes the indexes of the rotation angles ($[0°, 90°, 180°, 270°]$) measured.

[7]Note that the circles in Figs. 14(a) - 14(d) were indiscriminately placed and bears no consequence other than to show that the loop of the benchmark is identifiable at each segment.

[8]We recognized that whenever possible, the use of color as a differentiation metric should be avoided so as to make accommodation for readers who suffer from achromatopsia (color blindness) or those who might choose to print this paper in black and white. With these readers in mind we have used color tones, which would still convey the information intended in this work.

*1) **Distance-dependent pathloss**:* From the empirical data, we model the received power at different distances as:

$$Q^{\kappa_c,\psi,c,o} = Q_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\tilde{\eta}^{\psi,c}} \cdot \tilde{\xi}^{\kappa_c,\psi,c} \cdot \Delta^{\kappa_c,\psi,c,o} \quad (7)$$

where Q_0 is the power received at the reference distance d_0 (1 m). $\tilde{\eta}$, $\tilde{\xi}$ and Δ represent the pathloss exponent, environment-dependent shadowing gain and the board angular orientation-dependent shadowing gain ("board shadowing") in the indoor environment respectively.

$$Q_{\text{tot}}^{\kappa_c,\psi,c} = \mathbb{E}_{\text{o}} \left\{ Q_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\tilde{\eta}^{\psi,c}} \cdot \tilde{\xi}^{\kappa_c,\psi,c} \cdot \Delta^{\kappa_c,\psi,c,o} \right\} \quad (8)$$

To extract the channel parameters Q_0 and $\tilde{\eta}$, (7) was averaged over an ensemble of board orientations as shown in (8) to create a local mean power (Q_{tot}). A linear regression fit (shown in Fig. 15) is then used to derive the relationship between the local mean power and distances measured. The extracted parameters Q_0 and $\tilde{\eta}$ are provided in Table V. Note that in Fig. 15, Q_{tot} was obtained by averaging $Q^{\kappa_c,\psi,c,o}$ on the linear scale while the display is plotted in decibels. From Table V, it can be observed that the extracted parameters for the sidebands are similar – irrespective of the scenario with the exception of $\tilde{\eta}$ in the NLOS case.

LOS scenario					
	Q_0 (dBm)	$\tilde{\eta}$	$\tilde{\sigma}_{\tilde{\xi}}$ (dB)	μ_{σ_Δ} (dB)	σ_{σ_Δ}(dB)
Carrier	-73.55	-1.54	2.0	5.3	1.5
USB	-100.61	-1.57	2.5	5.1	1.9
LSB	-100.99	-1.59	1.9	5.4	1.6
NLOS scenario					
	Q_0 (dBm)	$\tilde{\eta}$	$\tilde{\sigma}_{\tilde{\xi}}$ (dB)	μ_{σ_Δ}(dB)	σ_{σ_Δ}(dB)
Carrier	-88.34	-1.69	3.9	4.6	2.1
USB	-117.11	-1.60	4.1	4.9	1.6
LSB	-116.82	-1.54	3.9	5.1	2.0

TABLE V: Propagation channel parameters for LOS and NLOS indoor measurements.

*2) **Shadowing analysis**:* From (8), the deviation of the local mean power (Q_{tot}) from the linear regression fit stems from the shadowing ($\tilde{\xi}$) caused by the environment, while the variation of Δ around Q_{tot} is caused by the board shadowing effect at different angular orientation. To extract $\tilde{\xi}$, we define the linear fit as

$$\tilde{\Phi}^{\kappa_c,\psi,c} = \tilde{\Phi}_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\tilde{\eta}^{\psi,c}} \quad (9)$$

and then compute

$$\tilde{\xi}^{\kappa_c,\psi,c} = \frac{Q_{\text{tot}}^{\kappa_c,\psi,c}}{\tilde{\Phi}_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\tilde{\eta}^{\psi,c}}}. \quad (10)$$

Note that $\tilde{\Phi}_0$ is equivalent to Q_0 in (7).

In this work, the logarithmic equivalent of $\tilde{\xi}$ has been modeled as a Gaussian distribution $\mathcal{N}(\tilde{\mu}_{\tilde{\xi}}(\text{dB}), \tilde{\sigma}_{\tilde{\xi}}(\text{dB}))$ in the LOS and NLOS scenarios with the first and second moment parameters computed as

$$\tilde{\mu}_{\tilde{\xi}}^{\psi,c}(\text{dB}) = \mathbb{E}_{\kappa_c} \left\{ 10 \cdot \log_{10} \left(\frac{Q_{\text{tot}}^{\kappa_c,\psi,c}}{\tilde{\Phi}_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\tilde{\eta}^{\psi,c}}} \right) \right\} \quad (11)$$

$$\tilde{\sigma}_{\tilde{\xi}}^{\psi,c}(\text{dB}) = \mathbb{D}_{\kappa_c} \left\{ 10 \cdot \log_{10} \left(\frac{Q_{\text{tot}}^{\psi,c}}{\tilde{\Phi}_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\tilde{\eta}^{\psi,c}}} \right) \right\}. \quad (12)$$

We found the logarithmic equivalent of $\tilde{\xi}$ to have a mean value of zero in both LOS and NLOS scenarios and have thus presented the extracted standard deviation ($\tilde{\sigma}_{\tilde{\xi}}$ (dB)) in Table V. The board shadowing gain (Δ) was computed as

$$\Delta^{\kappa_c,\psi,c,o} = \frac{Q^{\kappa_c,\psi,c,o}}{Q_{\text{tot}}^{\kappa_c,\psi,c}}. \quad (13)$$

We have modeled Δ as a zero-mean lognormally distributed variable at different distances in this work. We found that the standard deviation of σ_Δ differed from location to location and hence has been modeled as a random variable. The first and second order moments for the distribution of the standard deviation over an ensemble of distances are derived in (14) and (15) respectively.

$$\mu_{\sigma_\Delta}^{\psi,c}(\text{dB}) = \mathbb{E}_{\kappa_c} \left\{ \mathbb{D}_o \left\{ 10 \cdot \log_{10} \left(\frac{Q^{\kappa_c,\psi,c,o}}{\mathbb{E}_o \{Q^{\kappa_c,\psi,c,o}\}} \right) \right\} \right\} \quad (14)$$

$$\sigma_{\sigma_\Delta}^{\psi,c}(\text{dB}) = \mathbb{D}_{\kappa_c} \left\{ \mathbb{D}_o \left\{ 10 \cdot \log_{10} \left(\frac{Q^{\kappa_c,\psi,c,\text{o}}}{\mathbb{E}_o \{Q^{\kappa_c,\psi,c,\text{o}}\}} \right) \right\} \right\} \quad (15)$$

Empirical CDF plots and corresponding Gaussian fits for the logarithmic equivalent of σ_Δ for the Carrier, USB and LSB are shown in Figs. 16(a) - 16(c). It can be observed from Table V that $\tilde{\xi}$ in the NLOS is greater than that in the LOS scenario while μ_{σ_Δ} and σ_{σ_Δ} are comparable in both scenarios. This agrees with intuition since the board shadowing effect should be similar irrespective of the scenario, while the environment shadowing gain will be more pronounced in the NLOS than the LOS scenario.

C. Results from Indoor Bitcount and Basicmath Measurements

The results from the indoor *bitcount* and *basicmath* measurements reveals that peaks generated (at each frequency) by the seven segments of the *bitcount* and four segments of the *basicmath* programs are identifiable in both LOS and NLOS scenarios as shown in sample spectrogram plots at select LOS distances (1 m and 25 m) in Figs.17(a) - 18(b). Note that each set of "shorter-lines" (numbered on the spectrogram plots) corresponds to the segments of programs being executed.

These results confirm the possibility of remote monitoring of EM side-channel leakage from IoT devices at long proximity ranges in an indoor environment.

D. Results from FPGA Measurements

The data structure for measurements conducted in a LOS scenario using the FPGA board can be represented as $\Gamma^{\vartheta,\psi}$,

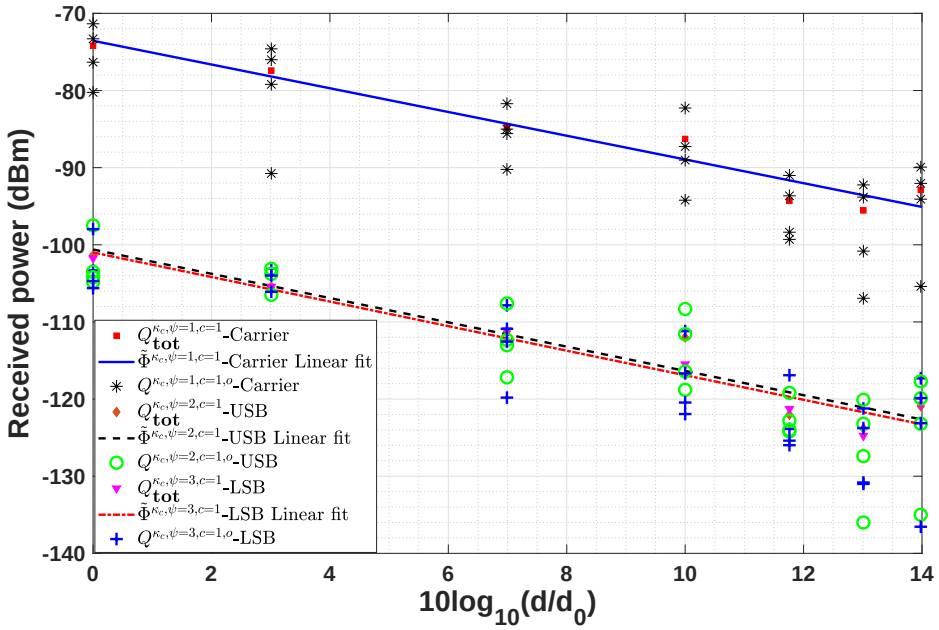
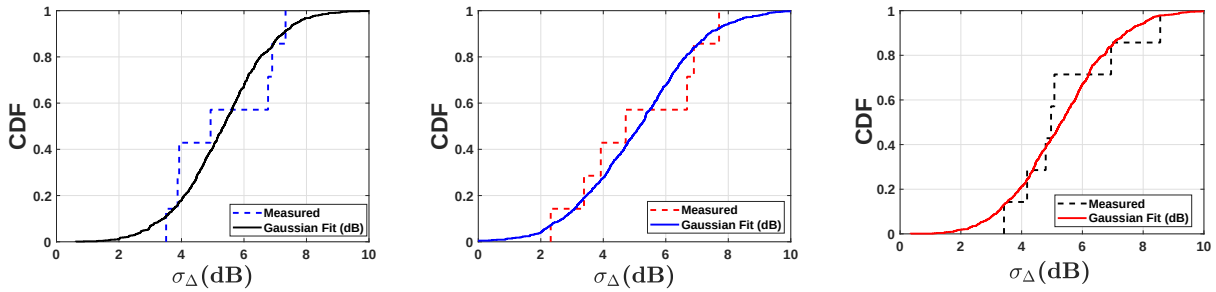
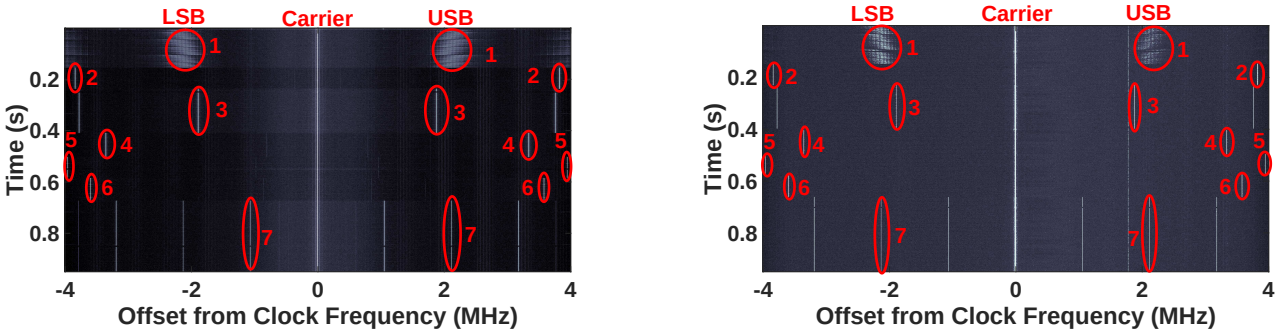


Fig. 15: Linear regression fit for received power over rotation and distances in an indoor LOS scenario.



(a) Carrier (b) USB (c) LSB

Fig. 16: Empirical CDF and corresponding Gaussian fit for Carrier, USB and LSB board shadowing in an indoor LOS scenario.



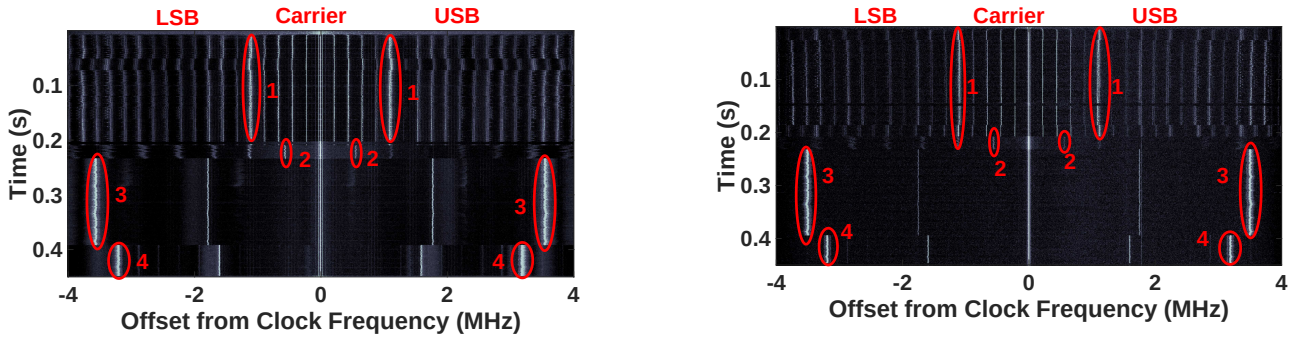
(a) 1 m (b) 25 m

Fig. 17: *Bitcount* results at measured LOS distances in the indoor environment.

where $\vartheta \in [1, 2, ..., 4]$ denotes the index of distances measured with $d_\vartheta \in [1, 2, 5, 10]$ m. $\psi \in [1, ..., \Psi = 3]$ represents carrier and sidebands such that $\psi = 1, 2, 3$ denotes the Carrier, USB and LSB respectively.

*1) **Distance-dependent pathloss**:* From the empirical data, the received power at different distances was modeled as

$$\Gamma^{\vartheta,\psi} = \Gamma_0^{\psi} \cdot \left(\frac{d_\vartheta}{d_0}\right)^{\varrho^{\psi}} \cdot \chi^{\vartheta,\psi}, \tag{16}$$



(a) 1 m

(b) 25 m

Fig. 18: *Basicmath* results at measured LOS distances in the indoor environment.

where Γ_0 is the power received at the reference distance d_0 (1 m), with ϱ and χ representing the pathloss exponent and shadowing gain due to this indoor environment.

Similarly to previous sections, a linear regression fit was used to derive a monotonically decreasing relationship between the received power and the measured distances with the extracted propagation channel parameters Γ_0 and ϱ presented in Table VI.

LOS scenario			
	Γ_0 (dBm)	ϱ	σ_χ (dB)
Carrier	-90.69	-1.91	2.4
USB	-125.65	-1.54	3.2
LSB	-126.42	-1.61	3.0

TABLE VI: Propagation channel parameters for LOS indoor FPGA measurements.

It can be observed from the results in Table VI that propagation channel parameters such as Γ_0 i.e., the received power at the reference distance (1 m) is considerably less (with differences of about 17-19 dB for Carrier, 25-28 dB for sidebands) than those presented in section IV. B even though the measurements were conducted in the same environment. This not only reflects the impact of the type of EM source board but also the fact that the 20$^{\text{th}}$ harmonic[9] was used in characterizing the propagation.

*2) **Shadowing gain**:* The shadowing gain was computed as the deviation of the received power from the linear regression fit expressed as

$$\overline{\Phi}^{\vartheta,\psi} = \overline{\Phi}_0^{\psi} \cdot \left(\frac{d_\vartheta}{d_0}\right)^{\varrho^{\psi}}, \tag{17}$$

with the shadowing gain derived as

$$\chi^{\vartheta,\psi} = \frac{\Gamma^{\vartheta,\psi}}{\overline{\Phi}_0^{\psi} \cdot \left(\frac{d_\vartheta}{d_0}\right)^{\varrho^{\psi}}}. \tag{18}$$

Note that $\overline{\Phi}_0$ is equivalent to Γ_0 in (16).

The logarithmic equivalent of χ has been modeled as a Gaussian distribution $\mathcal{N}(\mu_\chi(\text{dB}), \sigma_\chi(\text{dB}))$. We found χ (dB) to have a mean value of zero with standard deviation (σ_χ (dB)) presented in Table VI. Although the parameters in Table VI were extracted using the 20$^{\text{th}}$ harmonic of the carrier and sideband signals, nevertheless the values are useful for EM side-channel signal detection within a 10 m range in a LOS indoor environment. A system capable of reception at 50 MHz frequency range will afford an improved performance leading to longer range measurements.

[9]Note that the fundamental frequency of the FPGA board is 50 MHz while that of Olimex (IoT) board is 1.008 GHz.

V. Summary and Conclusion

We have successfully conducted EM side-channel propagation experiments in various environments using self-developed measurement setups. This research is the first to demonstrate the possibility of receiving side-channel signals at distances greater than 10 m and to statistically model the propagation of EM side-channel signals. We have extracted propagation channel parameters and provided statistical models that can be used in predicting the received power of the EM side-channel signals in various scenarios. A summary of our key findings is as follows:

1) Our results (using both SAVAT and bitcount) indicate that EM side-channel signals can be received at approximately 200 m away from the EM source in a LOS outdoor environment.
2) The distance-dependent pathloss exponent η in the outdoor environment was mostly comparable for the carrier and sidebands. The received power values (M_0) at the reference distance are more tolerant to polarization changes of the EM source if the circularly polarized QHA receiver antenna is used. However, this was not the case for the vertically polarized PDA antenna, which shows a wide variation of about 10 dB for the carrier and about 6-7 dB for sideband results in the outdoor environment.
3) The shadowing gain (in decibels) was modeled as a zero-mean Gaussian distribution with standard deviation values ranging from 2.8-3.5 dB in the sidebands and 3.0-3.6 dB in the carrier for measurements conducted with the QHA antenna while values ranged from 1.3-4.0 dB in the sidebands and 1.1-2.1 dB in the carrier for measurements conducted with the PDA in the outdoor environment.
4) In the indoor measurements, we observed that the difference between pathloss parameters at the reference distance i.e., Q_0 in the LOS and NLOS was approximately

15 dB for the carrier and about 17 dB for the sidebands while the pathloss exponents $\hat{\eta}$ were comparable in both scenarios with values ranging from -1.54 to -1.59 and -1.54 to -1.69 in the LOS and NLOS scenarios respectively. It is important to note that results from works such as [33] have shown the pathloss exponent in the LOS scenario to be smaller than that obtained from NLOS, however, that is not the case in this paper as the results are in fact comparable. A caveat to always consider is that difference in environment, measurement setup and frequency of operation could lead to different outcome in an empirical engagement such as this.

5) We found the environment shadowing gain to be higher in the NLOS scenario than the LOS case while the board shadowing gain values were similar in both cases. These observations intuitively makes sense.

Overall, it is clearly observable from the results presented in this paper that there is a need for the characterization of the propagation mechanisms of EM side-channel signals in different scenarios and environments. The models presented in this work serve as generic solutions to characterizing side-channel signals emanating from electronic devices. It is important to note that although the emanated (transmitted) power could differ for each device under test, this can be compensated for in the power received at the reference distance without loss of generality to the overall model. This type of work will aid the prediction of the received power of EM side-channel signals and inform on the proximity ranges from which leakages emanating from an IoT device (or network) can be monitored. Our work provides pertinent information for EM side-channel countermeasure development.

VI. ACKNOWLEDGEMENT

The authors will like to thank Dr. Alireza Nazari and Moumita Dey for several interesting discussions regarding this work and Sinan Abdelli, Dr. Juyal Prateek, and Jibang Fu for their help with the measurements.

REFERENCES

[1] N. Leavitt, "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers," *Computer*, vol. 43, no. 8, pp. 11–14, Aug. 2010. [Online]. Available: https://doi.org/10.1109/MC.2010.237

[2] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design Challenges for Secure Implantable Medical Devices," in *DAC Design Automation Conference 2012*, June 2012, pp. 12–17.

[3] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of Medical Devices and Body Area Networks," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug 2014.

[4] "Hacker Breach US Air-traffic Control," https://phys.org/news/2009-05-hackers-breach-air-traffic.html, accessed: 2019-7-16.

[5] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018. [Online]. Available: https://doi.org/10.1038/s41586-018-0609-x

[6] H. Shi and A. Tennant, "Enhancing the security of communication via directly modulated antenna arrays," *IET Microwaves, Antennas & Propagation*, vol. 7, no. 8, pp. 606–611, 2013.

[7] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, pp. 6300–6310, 2014.

[8] N. Zhao, Z. Zhang, M. U. Rehman, A. Ren, X. Yang, J. Zhao, W. Zhao, and B. Dong, "Authentication in millimeter-wave body-centric networks through wireless channel characterization," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, pp. 6616–6623, 2017.

[9] Alam, Monjur and Khan, Haider Adnan and Dey, Moumita and Sinha, Nishith and Callan, Robert and Zajic, Alenka and Prvulovic, Milos, "One&Done: A Single-Decryption EM-Based Attack on OpenSSLs Constant-Time Blinded {RSA}," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 585–602.

[10] R. Callan, A. Zajić, and M. Prvulovic, "FASE: Finding Amplitude-modulated Side-channel Emanations," in *Proceedings of the 42Nd Annual International Symposium on Computer Architecture*, ser. ISCA '15. New York, NY, USA: ACM, 2015, pp. 592–603. [Online]. Available: http://doi.acm.org/10.1145/2749469.2750394

[11] M. Prvulovic, A. Zajić, R. L. Callan, and C. J. Wang, "A Method for Finding Frequency-Modulated and Amplitude-Modulated Electromagnetic Emanations in Computer Systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, no. 1, pp. 34–42, Feb 2017.

[12] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic Side-channel Attacks on Printers," in *Proceedings of the 19th USENIX Conference on Security*, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 20–20. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929847

[13] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '99. Berlin, Heidelberg: Springer-Verlag, 1999, pp. 388–397. [Online]. Available: http://dl.acm.org/citation.cfm?id=646764.703989

[14] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards," in *Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '99. London, UK, UK: Springer-Verlag, 1999, pp. 144–157. [Online]. Available: http://dl.acm.org/citation.cfm?id=648252.752374

[15] A. G. Bayrak, F. Regazzoni, P. Brisk, F. Standaert, and P. Ienne, "A first step towards automatic application of power analysis countermeasures," in *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2011, pp. 230–235.

[16] M. G. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-panel Displays," in *Proceedings of the 4th International Conference on Privacy Enhancing Technologies*, ser. PET'04. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 88–107. [Online]. Available: http://dx.doi.org/10.1007/11423409_7

[17] Z. Wang and R. B. Lee, "New Cache Designs for Thwarting Software Cache-based Side Channel Attacks," in *Proceedings of the 34th Annual International Symposium on Computer Architecture*, ser. ISCA '07. New York, NY, USA: ACM, 2007, pp. 494–505. [Online]. Available: http://doi.acm.org/10.1145/1250662.1250723

[18] R. Callan, A. Zajić, and M. Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events," in *2014 47th Annual IEEE/ACM International Symposium on Microarchitecture*, Dec 2014, pp. 242–254.

[19] R. Callan, N. Popovic, A. Daruna, E. Pollmann, A. Zajić, and M. Prvulovic, "Comparison of electromagnetic side-channel energy available to the attacker from different computer systems," in *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Aug 2015, pp. 219–223.

[20] N. Sehatbakhsh, A. Nazari, A. Zajić, and M. Prvulovic, "Spectral profiling: Observer-effect-free profiling by monitoring em emanations," in *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, Oct 2016, pp. 1–11.

[21] A. Zajić, M. Prvulovic, and D. Chu, "Path loss Prediction for Electromagnetic Side-Channel Signals," in *2017 11th European Conference on Antennas and Propagation (EUCAP)*, March 2017, pp. 3877–3881.

[22] Camurati, Giovanni and Poeplau, Sebastian and Muench, Marius and Hayes, Tom and Francillon, Aurélien, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *CCS 2018, 25th ACM conference on Computer and communications security, 15-19 October 2018, Toronto, Canada*, Toronto, CANADA, 10 2018. [Online]. Available: http://www.eurecom.fr/publication/5625

[23] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

[24] L. Goubin and J. Patarin, "Des and differential power analysis the duplication method," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 1999, pp. 158–172.

[25] S. Sangodoyin, F. Werner, B. B. Yilmaz, C. Cheng, E. Ugurlu, N. Sehatbakhsh, M. Prvulovic, and A. Zajić, "Remote Monitoring and Propagation Modeling of EM Side-Channel Signals for IoT Device Security," in *(submitted) to 2020 14th European Conference on Antennas and Propagation (EUCAP)*, March 2020.

[26] F. Werner, D. A. Chu, A. R. Djordjevi, D. I. Olan, M. Prvulovic, and A. Zajić, "A Method for Efficient Localization of Magnetic Field Sources Excited by Execution of Instructions in a Processor," *IEEE Transactions on Electromagnetic Compatibility*, vol. 60, no. 3, pp. 613–622, June 2018.

[27] M. R. Guthaus, J. S. Ringenberg, D. Ernst, T. M. Austin, T. Mudge, and R. B. Brown, "MiBench: A free, commercially representative embedded benchmark suite," in *Proceedings of the fourth annual IEEE international workshop on workload characterization. WWC-4 (Cat. No. 01EX538)*. IEEE, 2001, pp. 3–14.

[28] "Olimex A13 OLinuXino specification and description," https://www.olimex.com/Products/OLinuXino/A13/A13-OLinuXino-MICRO/resources/A13-OLINUXINO-MICRO.pdf, accessed: 2019-6-21.

[29] Dinkić, Jelena Lj and Olćan, Dragan I and Djordjević, Antonije R and Zajić, Alenka G, "High-Gain Quad Array of Nonuniform Helical Antennas," *International Journal of Antennas and Propagation*, vol. 2019, 2019.

[30] P. Juyal, S. Adibelli, N. Sehatbakhsh, and A. Zajić, "A Directive Antenna Based on Conducting Disks for Detecting Unintentional EM Emissions at Large Distances," *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 12, pp. 6751–6761, Dec 2018.

[31] "FPGA DEO-CV Cyclone V Board specification and description," https://www.intel.com/content/dam/altera-www/global/en_US/portal/dsn/42/doc-us-dsnbk-42-1504012210-de0-cv-user-manual.pdf, accessed: 2019-6-21.

[32] A. F. Molisch, *Wireless communications*. John Wiley & Sons, 2012, vol. 34.

[33] S. Sangodoyin, V. Kristem, A. F. Molisch, R. He, F. Tufvesson, and H. M. Behairy, "Statistical Modeling of Ultrawideband MIMO Propagation Channel in a Warehouse Environment," *IEEE Transactions on Antennas and Propagation*, vol. 64, no. 9, pp. 4049–4063, Sep. 2016.

[34] S. Sangodoyin and V. Kristem and C. U. Bas and M. Käske and J. Lee and C. Schneider and G. Sommerkorn and C. J. Zhang and R. Thom and A. F. Molisch, "Cluster Characterization of 3-D MIMO Propagation Channel in an Urban Macrocellular Environment," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5076–5091, Aug 2018.

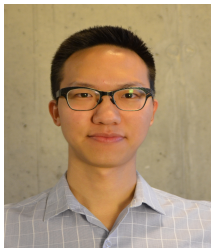
[35] J. Karedal, S. Wyne, P. Almers, F. Tufvesson, and A. F. Molisch, "A measurement-based statistical model for industrial ultra-wideband channels," *IEEE transactions on wireless communications*, vol. 6, no. 8, pp. 3028–3037, 2007.

[36] T. Santos, F. Tufvesson, and A. F. Molisch, "Modeling the ultra-wideband outdoor channel: Model specification and validation," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, p. 1987, 2010.

Seun Sangodoyin (S'14) received his B.Sc in Electrical Engineering from Oklahoma State University in May 2007, and the M.Sc and Ph.D in Electrical Engineering from the University of Southern California (USC) in 2009 and 2018 respectively. He is currently a Postdoctoral Fellow at the Georgia Institute of Technology. His research interest includes Millimeter-wave (measurement-based) MIMO channel Modeling and analysis, Tera-hertz communications, UWB MIMO Radar, Parameter Estimation, Bioelectronics, Body area Networks and Stochastic dynamical Systems.

Frank T. Werner (S'16) received his B.S. degree (2013) and his M.S. (2016) in electrical engineering from Auburn University, Alabama. Currently, he is completing his PhD in electrical engineering at Georgia Institute of Technology. His research interests include electromagnetic compatibility, wireless communications, signal processing, and applied electromagnetics.

Baki B. Yilmaz (S'16) received the B.Sc. and M.Sc. degrees in Electrical and Electronics Engineering from Koc University, Turkey in 2013 and 2015 respectively. He joined Georgia Institute of Technology in Fall 2016 and he is currently pursuing his PhD in School of Electrical and Computer Engineering, focusing on quantifying covert/side-channel information leakage. Previously, he worked on channel equalization and sparse reconstruction. His research interests span areas of electromagnetic, signal processing and information theory.



Chia-Lin Cheng (M'20) received the B.Sc. degree in electrical engineering from National Taiwan University in 2013, and the M.Sc. degree and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology in 2017 and 2020, respectively, where he worked in the Electromagnetic Measurements in Communications and Computing (EMC^2) Lab, focusing on THz chip-to-chip channel measurements and modeling. He also worked on signal integrity and non-linear circuits I/O modeling using machine learning. His research interests span areas of electromagnetics, wireless channel measurements, and modeling. He was a recipient of the TechConnect Innovation Award at the 2019 TechConnect World Innovation Conference and Expo, the Second Best Hardware Demo Award at the 2019 IEEE International Symposium on Hardware Oriented Security and Trust, and the Best Poster Award at the 2018 IEEE International Conference on RFID.

Elvan M. Ugurlu (S'19) received the B.Sc. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey in 2018. He is currently pursuing his Ph.D. in the School of Electrical and Computer Engineering at Georgia Institute of Technology, Atlanta, Georgia, USA. He is a graduate research assistant in Electromagnetic Measurements in Communications and Computing (EMC^2) Lab at the Georgia Institute of Technology focusing on electromagnetic side-channel analysis. His research interests include digital signal processing, machine learning and electromagnetics.

Nader Sehatbakhsh (S'12) received the B.Sc. degree in Electrical Engineering from the University of Tehran in 2013 and the M.Sc. in Electrical Engineering and PhD in Computer Science from Georgia Institute of Technology in 2016 and 2020 respectively. Since 2020, he has been an Assistant Professor at the University of California, Los Angeles. His main research interests are Computer Architecture, Embedded System, and Hardware Security. He won the best paper award in MIRCO'49 for his work on using EM side-channel signals for software profiling.

Milos Prvulovic (S'97–M'03–SM'09) received the B.Sc. degree in electrical engineering from the University of Belgrade in 1998, and the M.Sc. and Ph.D. degrees in computer science from the University of Illinois at UrbanaChampaign, in 2001 and 2003, respectively. He is currently a Professor with the School of Computer Science, Georgia Institute of Technology, where he joined in 2003. His research interests are in computer architecture, especially hardware support for software monitoring, debugging, and security. He was a past recipient of the NSF CAREER Award, and a Senior Member of the ACM and the IEEE Computer Society.

Alenka Zajić (S'99–M'09–SM'13) received the B.Sc. and M.Sc. degrees from the School of Electrical Engineering, University of Belgrade, in 2001 and 2003, respectively, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology in 2008. She is currently an Associate Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology. Prior to that, she was a Visiting Faculty Member at the School of Computer Science, Georgia Institute of Technology, a Postdoctoral Fellow at the Naval Research Laboratory, and a Design Engineer at Skyworks Solutions Inc. Her research interests span areas of electromagnetic, wireless communications, signal processing, and computer engineering. Dr. Zajić was a recipient of the 2017 NSF CAREER Award, the 2012 Neal Shepherd Memorial Best Propagation Paper Award, the Best Student Paper Award at the IEEE International Conference on Communications and Electronics 2014, the Best Paper Award at the International Conference on Telecommunications 2008, the Best Student Paper Award at the 2007 Wireless Communications and Networking Conference, and the Dan Noble Fellowship in 2004, which was awarded by Motorola Inc., and the IEEE Vehicular Technology Society for quality impact in the area of vehicular technology. She is currently an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.