Remote Monitoring and Propagation Modeling of EM Side-Channel Signals for IoT Device Security

Seun Sangodoyin[1], *Member, IEEE*, Frank Werner[1], *Student Member, IEEE*, Baki B. Yilmaz[1], *Student Member, IEEE*, Chia-Lin Cheng[1] *Student Member, IEEE*, Elvan M. Ugurlu[1] *Student Member, IEEE*, Nader Sehatbakhsh [2] *Student Member, IEEE*, Milos Prvulovic[2] *Senior Member, IEEE* and Alenka Zajic[1], *Senior Member, IEEE*

[1] School of Electrical and Computer Engineering Georgia Institute of Technology, Atlanta, Georgia 30332–0250

[2]School of Computer Science Georgia Institute of Technology, Atlanta, Georgia 30332–0250

***Abstract*—This paper presents results from an investigation into long-range detection and monitoring of Electromagnetic (EM) side-channel signals leaked from Internet-of-Things (IoT) and Field Programmable Gate Array (FPGA) devices. Our work shows that operational information and program activities of the IoT and FPGA modules can be garnered at distances excess of 25 m in an indoor Line-Of-Sight (LOS) environment, while at about 10 m in an indoor (through wall) Non-Line-Of-Sight (NLOS) scenario. We provide a propagation model that can be used to predict the received power (and corresponding variation i.e., shadowing gain) of leaked EM side-channel signals at various distances and scenarios. Benchmark program *bitcount* used in the performance evaluation of ARM-based microprocessors and a microbenchmark SAVAT running on an IoT device were detected and monitored remotely in our work.**

I. Introduction

The initial excitement about the use cases of Internet-of-Things (IoT) devices has been tapered of late with concerns about the possible security vulnerabilities to these devices. Security attacks on IoT wireless medical devices , e.g., pacemakers and insulin pumps [1], [2] have elevated the level of threats to wireless medical devices from the realm of theoretical possibility to an immediate concern [3]. A security vulnerability prevalent to embedded hardware devices include the EM side-channel attack [4]. These 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 [4].[1]

Accurate propagation models of the EM side-channel signals would be required for the development of any security countermeasures. It is therefore of utmost importance that a comprehensive and realistic characterization be conducted to aid the prediction of range and conditions at which the emanated signals can be intercepted. A number of works such as [4]–[9] have discussed side-channel attacks and defense. [5] and [6] presented the use of power consumption measurements to find secret keys and attack implementation of modular exponentiation algorithms on smart cards respectively while [7] presented a new metric called Signal Available to Attacker (SAVAT), which explores the EM side-channel signals emanated from a computer system as a consequence of the difference in the execution of two program activities running on the computer system. [4] investigated the propagation mechanisms that EM side-channel signals observed at different frequencies and proposed models for near-field and far-field propagation, however this work was done for a small samples of distances (≤ 3 m). [8] and [9] both presented countermeasures to thwart power analysis attacks. To the knowledge of the authors, there are hardly any works detailing the propagation of EM side-channel signals at large distances excess of 10 m.

In this paper, we present a detailed description of measurement campaigns conducted in an indoor environment to characterize the propagation of EM side-channel signals. We explored scenarios such as Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS). We present results of key propagation parameters such as pathloss and shadowing gain of the aforementioned signals. We also provide results from the remote monitoring of benchmark program *bitcount* running on the IoT devices. It is important to note that while characterization of wireless signals in various environments is not a novel concept, however, the measurements (and proposed models) in this work are primarily for understanding the propagation mechanisms of EM side-channel signals radiated from an unintentional source.

The rest of this paper is organized as follows. Section II described the measurement campaign while data processing procedure and results are discussed in section III. Summary and conclusion are inferred in Section V.

II. Measurement Campaign

A. EM Emanations and Alternation Frequency

The characterization of the propagation mechanism of the EM side-channel signal will require a procedure for generating a *controlled* emanation of the signal from an IoT device. This signal will serve as the channel excitation waveform. Firstly, we will discuss the procedure for generating the aforementioned EM side-channel signal using a modification

[1]This work has been 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.

to the microbenchmark SAVAT [7] and secondly, discuss the signal emanation as a result of *bitcount* running on the IoT device.

Using SAVAT , controllable emanations were generated by executing two types of program activities repeatedly on the IoT device. Typical program activities include simple instructions such as addition (ADD), multiplication (MUL), load (LDX), and store (STR). 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 program activities results in a periodic current being superimposed onto the traces of 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: The X/Y alternation pseudo-code.

An example of a microbenchmark, which is used for generating 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 comprises 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 $\frac{1}{T_{alt}}$. 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

$$T_{alt} = t_X \times n_X + t_Y \times n_Y. \quad (1)$$

The generated excitation signal also amplitude modulates other periodic signals generated by the device. In this situation, the clocks of components such as the processor and memory, which are used for executing the alternating program activity act as carriers for the modulating waveform. During normal operations, the clocks produce periodic currents at the clock frequency f_c along the device's traces thereby generating an EM field. When the alternating program activity is executed,

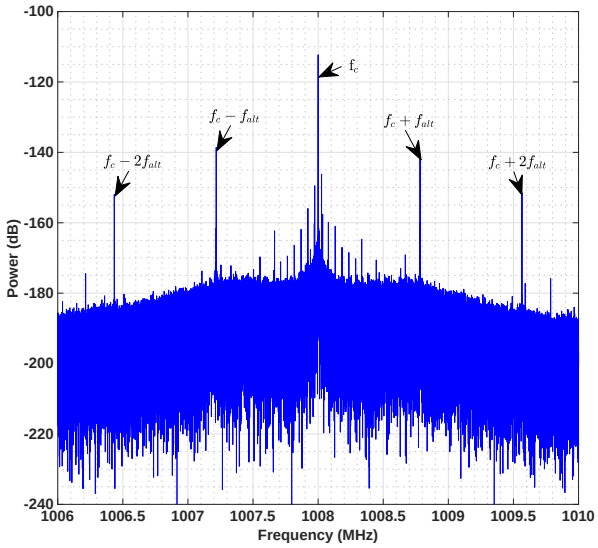


Fig. 2: Example of the processor clock being modulated by a 1 MHz excitation signal.

the periodic current from the clock is then modulated. Fig. 2 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 the 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.

The *Bitcount* program was implemented in our work to run seven segment loops with each segment corresponding to distinct task – hence varying loop duration. Our objective is to detect and monitor these segment loops through EM signals emanated from the IoT device.

B. 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 with four elevator cars present. A structural layout of the measurement site has been provided in Fig. 3.

C. Measurement Setup

We designed and assembled a task-specific measurement system for this indoor measurement campaign. The block diagram of the system is shown in Fig. 4. At the TX end of the

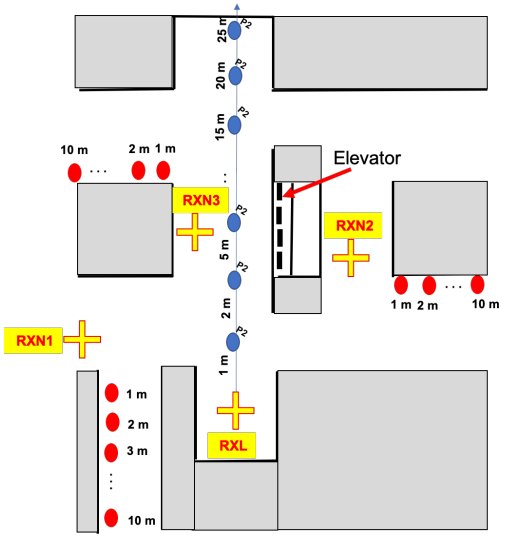


Fig. 3: Floor map of the indoor environment.

measurement setup is an EM source/emitter – an IoT device (Olimex A13-OLinuXino-MICRO) [10] and a Personal Computer (PC) to interface and power the IoT device. The Olimex device is an open-source embedded ARM linux computer with A13 cortex-A8 processor and an on-board clock frequency of 1.008 GHz. At the RX end is a high-gain quadrature array of nonuniform helical antennas (*abbreviated as* QHA) [11], which was connected to a Spectrum Analyzer (SA, Keysight N9030B). The QHA is circularly polarized with a directive gain of approximately 20.5 dBi in the frequency range 0.9 GHz to 1.1 GHz. Note that in this work, a second measurement campaign was conducted using a similar setup as described above, however with the exception of the EM source/emitter used – a Field Programmable Gate Array (FPGA, DEV0-CV Cyclone V) [12] was used instead. The DEV0-CV is a development board running the Altera Cyclone V FPGA with an on-board clock frequency of 50 MHz. With the relatively low[2] fundamental frequency of the on-board clock, we were only able to capture the 20$^{\text{th}}$ harmonic of the EM side-channel signal – with the operation range of the RX antenna (QHA) ranging from 0.9 to 1.1 GHz.

We ran the instruction set MUL/ADD in SAVAT (see [7] for more details) for this particular experiment while setting f_{alt} to 500 KHz. 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. Multiple measurements were taken for each distance measured, by placing the TX and RX at different positions. These positions provide different realizations of shadowing i.e., power variations due to blockage effects in the environment. A total of 3 shadowing positions (RXN1, RXN2 and RXN3 in Fig. 3) were used for measurements in the NLOS scenario while a single position (P2 in Fig. 3) was

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

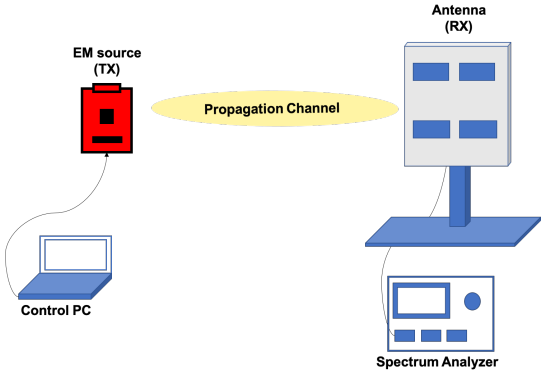
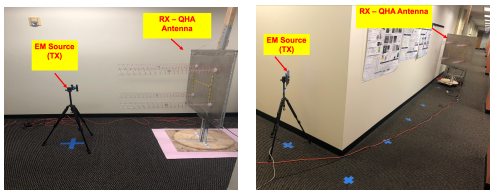


Fig. 4: Measurement setup

used in the LOS case. Pictures of the measurement setup for both LOS and NLOS scenarios are shown in Figs. 5(a) and 5(b). For the FPGA module, measurements were conducted for a LOS scenario at P2 (see Fig. 3) in the large hallways at TX-RX separation distances of 1, 2, 5, and 10 m.



(a) LOS (b) NLOS

Fig. 5: Measurement setup in the indoor LOS and NLOS scenarios.

III. Data Processing and Results

A. Results from indoor measurements

The data structure of the received power in the indoor measurement can be represented as $\hat{M}^{\kappa_c,\psi,s,c}$, 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 distances for different scenarios 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 $d_{\kappa_{c=1}} \in [1,2,5,10,15,20$ and 25 m$]$ while $d_{\kappa_{c=2}} \in [1,2,3,5,8$ 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 $s_{c=1} \in [S = 1]$ and $s_{c=2} \in [1,...,S = 3]$ denotes the shadowing points measured for the LOS and NLOS cases respectively.

*1) **Distance-dependent pathloss**:* The motivation for the pathloss model proposed in this work is due to its similarity to the conventional power law [13], which is a standard procedure for modeling pathloss and shadowing gain. One of the main challenges in predicting propagation loss of EM side-channel signals is the fact that the transmit power and transmit "antenna" gain are unknown [4] therefore pathloss cannot be computed using the aforementioned power law

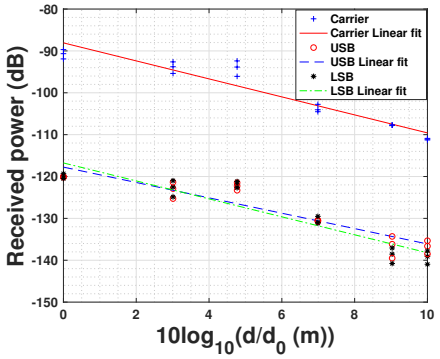


Fig. 6: Scatterplot of pathloss for NLOS indoor measurement.

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.

From the empirical data, the received power at different distances can modeled as

$$\hat{M}^{\kappa_c,\psi,s_c,c} = \hat{M}_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\hat{\eta}^{\psi,c}} \cdot \hat{\xi}^{\kappa_c,s_c,\psi,c} \tag{2}$$

where $\hat{M}_0$ is the power received at the reference distance d_0 (1 m), with $\hat{\eta}$ and $\hat{\xi}$ representing the pathloss exponent and the shadowing gain in the indoor environment respectively.

$$\hat{\bar{M}}^{\kappa_c,\psi,c} = \frac{1}{S}\sum_{s_c=1}^{S}\left[\hat{M}_0^{\psi,c} \cdot \left(\frac{d_{\kappa_c}}{d_0}\right)^{\hat{\eta}^{\psi,c}} \cdot \hat{\xi}^{\kappa_c,s_c,\psi,c}\right] \tag{3}$$

To aid parameter extraction, (2) was averaged over an ensemble of shadowing points in the environment as shown in (3) so as to create a local mean power ($\hat{\bar{M}}$). A linear regression fit is then used to infer the monotonically decreasing relationship between the local mean power and distances measured. Fig. 6 show the linear fit on the scatter plot of the empirical data measured in the NLOS scenarios. Propagation channel parameters $\hat{M}_0$ and $\hat{\eta}$ extracted from the linear fit are presented in Table I.

It can be observed from the results in Table I that the sidebands channel parameters are similar (with the exception of $\hat{\eta}$ in the NLOS scenario) while differing from that of the carrier in both LOS and NLOS scenarios. It can also be observed that $\hat{M}_0$ differed in the LOS and NLOS by approximately 17 dB for the carrier and about 20 dB for the sidebands. This difference can be attributed to the penetration loss through walls in the NLOS. A similar trend can be observed from the outcome of the FPGA measurements (see Table I). However, the smaller $\hat{M}_0$ values (compared to IoT LOS scenario) can be attributed to the fact that the 20^{th} harmonic, which is low-powered was used for the modeling – nevertheless, the EM emanation was still noticeable at large distances.

	$\hat{M}_0$(dB)	$\hat{\eta}$	$\hat{\sigma}_{\hat{\xi}}$ (dB)
IoT: LOS scenario			
Carrier	-71.75	-1.80	2.17
USB	-99.00	-1.88	1.64
LSB	-99.67	-1.76	2.38
IoT: NLOS scenario			
Carrier	-88.08	-2.15	2.39
USB	-117.75	-1.83	2.80
LSB	-116.75	-2.14	3.10
FPGA: LOS scenario			
Carrier	-90.69	-1.91	2.37
USB	-125.65	-1.54	3.18
LSB	-126.42	-1.61	2.97

TABLE I: Propagation channel parameters for LOS and NLOS indoor measurements using IoT and FPGA devices.

*2) **Shadowing gain**:* The shadowing gain ($\hat{\xi}$) was obtained by computing the deviation of the received power ($\hat{M}$) at each measured location (i.e., shadowing point and distance) from the linear regression fit.

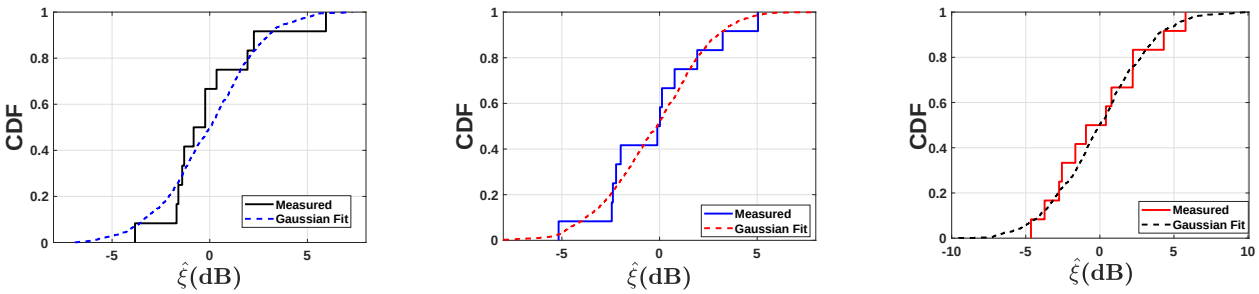
We modeled the logarithmic equivalent of the extracted shadowing gain as a Gaussian distribution $\mathcal{N}(\hat{\mu}_{\hat{\xi}}(\text{dB}), \hat{\sigma}_{\hat{\xi}}(\text{dB}))$ in the LOS and NLOS scenarios. The shadowing gain (dB) was found to have a mean value of zero in this indoor environment (for both LOS and NLOS scenarios) while the extracted standard deviation ($\hat{\sigma}_{\hat{\xi}}$ (dB)) has been provided in Table I. The cumulative distribution function (CDF) plots of the shadowing gain and corresponding Gaussian fit for USB, Carrier and LSB in the indoor NLOS scenario (for the IoT device) have been provided in Figs. 7(a) - 7(c). Results in Table I show that the standard deviation ($\hat{\sigma}_{\hat{\xi}}$) values for the sidebands and carrier are similar in the LOS scenario while differing in the NLOS scenarios.

B. Results from indoor bitcount measurements

The results from the indoor *bitcount* measurements reveals that peaks generated (at each frequency) by the seven segments of the *bitcount* programs are identifiable in both LOS and NLOS scenarios as shown in sample spectrogram plots at select LOS distance 25 m and NLOS distance 8 m in Figs.8(a) - 8(b). Note that each set of "shorter-lines" (numbered on the spectrogram plots) corresponds to the segments of programs being executed.

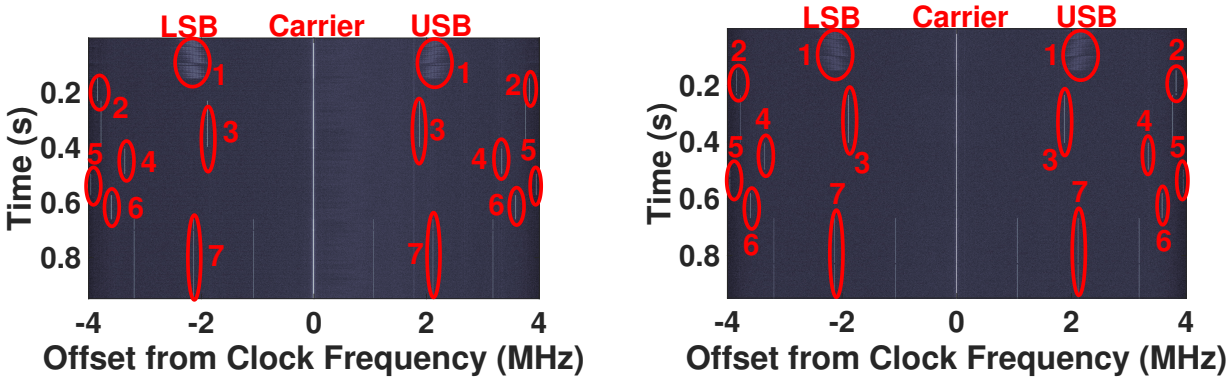
IV. Summary and Conclusion

We conducted a measurement campaign to characterize the propagation of EM side-channel signals in an indoor LOS and NLOS environment using an IoT device and an FPGA module. We found the distance-dependent pathloss exponent for USB, LSB and Carrier to be almost similar with values ranging between -1.76 to -1.88 in the LOS case and -1.83 to -2.15 in the NLOS when using the IoT device and -1.54 to -1.91 when using the FPGA module. Pathloss at the reference distance i.e., $\hat{M}_0$ in the LOS case differed from NLOS by about 17 for the carrier and 20 dB for the sidebands while the logarithmic equivalent of the shadowing gain followed a zero-mean Gaussian distribution in all experiments. Results



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

Fig. 7: Empirical CDF plot of shadowing gain for Carrier, USB and LSB in the NLOS indoor measurement.



(a) LOS 25 m (b) NLOS 8 m

Fig. 8: *Bitcount* results at measured (a) 25 m LOS and (b) 8 m NLOS distances in the indoor environment.

from the *bitcount* experiment confirms that EM side-channel leakage stemming from "regular programs" such as the type of benchmark running on the IoT device can also be detected at long proximity ranges in an indoor environment.

This work is relevant for EM side-channel leakage countermeasure development and provides pertinent information towards embedded systems and wireless network security.

V. Acknowledgment

The authors will like to thank the members of staff of TSRB for helping facilitate the measurement campaign.

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] 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.

[5] 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

[6] 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

[7] 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.

[8] 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.

[9] L. Goubin and J. Patarin, "DES and Differential Power Analysis (The "Duplication" Method)," in *Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '99. London, UK, UK: Springer-Verlag, 1999, pp. 158–172. [Online]. Available: http://dl.acm.org/citation.cfm?id=648252.752372

[10] "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.

[11] 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.

[12] "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.

[13] A. Molisch, *Wireless Communications*, ser. Wiley - IEEE. Wiley, 2010.