THz Bistatic Backscatter Side-Channel Sensing at a Distance

Sinan Adibelli, *Student Member, IEEE*, Prateek Juyal, *Member, IEEE* Milos Prvulovic, *Senior Member, IEEE,* and Alenka Zajic, *Senior Member, IEEE*

***Abstract*— This paper presents the sensing and detection of backscattered THz side-channels unintentionally created by FPGA activity using a bistatic arrangement. At first, a single frequency is modulated onto a THz carrier due to the switching activity inside the FPGA and this modulated frequency is received at a distance. The effects of polarization and the receiver distance on the backscattered signal are studied and it is found that deliberately introducing a polarization mismatch between the transmitter and the receiver can improve the signal to noise ratio (SNR) by more than 10 dB. This allows the signal to be received at distances greater than 45 cm with SNR above 54 dB, making detection feasible at several meters away. Through the use of a near field focuser, the properties of the side-channel signal are measured over the surface of the FPGA board with a resolution of 0.5 mm. Next, backscatter signal at 4 distinct frequencies is created and detected through splitting the FPGA into 4 distinct modules. The relative strength of the frequencies is compared and conclusions about the physical location and the strength of these signals originating from distinct modules are analyzed. It is found that by focusing the backscatter system on certain locations on the FPGA can preferentially receive the signal from one module while filtering out the other modules. This helps isolating the signals created by various modules in an FPGA and significantly improving the effectiveness of side-channel detection techniques.**

***Index Terms*— EM side-channel, Sensing, THz Focusing, polarization**

I. Introduction

Electromagnetic (EM) emanations from the digital device or computing systems can create side-channels [1]-[6]. These EM side-channels have been earlier exploited for physical attacks which are of major concern for electronic security [7]- [9] . More recently, EM side-channels have been used for other applications. For instance, in attestation of embedded hardware devices [10], external malware and malicious activity detection [11]- [13] and detection of dormant hardware Trojans [14]-[16]. There has been a growing attention to use the EM side-channels for profiling and monitoring the digital electronics and computing systems. The basic approach is to establish correlation between the received side-channels signals and the application execution which can be used to build the reference model for the normal behavior of a system. To monitor, the received signal can be compared to the model to make a decision regarding the functioning or state of a system.

Specifically, monitoring the program activity at a distance is of a major interest. EM based monitoring requires antenna or near field focusers. For example, detection and monitoring of the external malware at microwave frequencies in both near field and far field using EM probe and antenna, respectively, was shown in [8]. A high gain antenna with operating frequency about 1 GHz was shown to detect malware at a distance [17]. A micro level simulation tool was developed which enables the simulation of EM side-channels and helps in measuring side-channel leakage from systems [18]. To enable the EM based monitoring at a distance, fundamental mechanism of the backscatter radiation from FPGA needs to be understood. The mechanism of the radiation from the FPGA is based on the unintentional modulation caused by the switching of transistors. In order to do its tasks, the digital circuits in the FPGA are fed a clock signal which causes the impedance of the circuit traces to periodically change. When the surface of the FPGA is excited by a strong carrier signal, that signal couples onto the digital circuit and gets modulated by the switching activity. All of these signals are then backscattered through EM leakage and can be detected. For practical purposes and the limitations of the equipment, a bistatic arrangement is explored in this paper [19]- [23]; however, an arrangement where the transmitter and the receiver are collocated would yield equivalent results.

Previous EM side-channel research has mainly focused on microwave frequencies. Monitoring and other security applications such as malware and Trojan detection using side channels at THz frequencies has several advantages compared to microwave band. First, THz signals have great advantage over GHz signals for side-channel detection due to larger bandwidth. Using THz backscattering tens of signal points per nanosecond can be collected, which is sufficient to provide information not only about switching activity from one cycle to another, but also within the cycle, which can provide important information about software and hardware activity via side-channels that was not available before. Second, THz signals have lower noise/interference. Microwave frequencies have a lot of strong sources of interference such as AC power, AM, FM, and satellite radio, cellular phone, etc., while these sources of interference are not present at THz frequencies. Another advantage is that the beam can be focused in the region of interest in the small part of a processor or FPGA chip.

Sensing of unintentional modulation from the digital electronics at THz frequencies has been shown earlier where a

This work has been supported, in part, by NSF grant 1651273 and ONR grant N00014-19-1-2287. The views and findings in this paper are those of the authors and do not necessarily reflect the views of NSF or ONR.

The authors are with Electrical Engineering Department, Georgia Institute of Technology, Atlanta, USA

new backscattering side-channels were observed and leveraged for RFID communications and monitoring applications [24]-[27]. In [26], the characterization of the received backscatter signal at THz was shown up to 25 cm distance for RFID applications. It was shown that near field focuser can be used to receive multiple side-channel bits at a distance from the EM source. The strong carrier signal was observed with 4 modulated backscatter peaks 1 MHz away from the clock frequency. To understand the side-channel sensing and detection and to enable their usefulness at THz frequencies, further investigation is required. Also, to utilize these side-channels for security monitoring at a distance, various aspects of the signals need to be studied and modeled. This paper attempts to further develop the understanding of these backscattered side-channels at THz frequencies and enable their use for monitoring the program activity.

Owing to the complex nature of connections on the FPGA board such as bond-wires, circuit traces, high density of transistors, power connections, etc., there is limited knowledge and understanding about the spatial variations and the polarization of the backscatter signal that is modulated by the program activity of the FPGA. As compared to scattering from a uniform passive surface such as metal or insulator, the backscattered signal modulated by program activity shows significant variance based on the incident signal location. Also, the behavior of the received power and SNR vs. distance is not known. To this end, main contributions of our paper are:

- Explain and model the polarization effect using EM-circuit co-simulation.
- Present the SNR enhancing effects of polarization on the received modulated backscatter at THz frequencies.
- Study the spatial variations of the signal backscattered from the FPGA. In particular, the ability to focus and isolate the signal from individual modules on an FPGA while limiting the interference from other modules.
- Study and present the effect of distance of the receiver on SNR.

The rest of the paper is organized as follows. Section II describes EM circuit co-simulation to show the modulated backscattering. Section III presents the measurement of one bit backscattered signal at a distance with polarization effects and the 2D scan results showing the spatial variation of these signals. Section IV presents the measurement results for the side-channel sensing for multiple frequency peaks simultaneously and how much each frequency can be selectively targeted via near field focusing. Finally, Section V concludes the paper.

II. THz Side channel Sensing: EM-Circuit Simulation

This section presents an EM-circuit co-simulation model and analysis for sensing of backscattered side-channels from digital circuits at 300 GHz and its effect of polarization. We propose a proof of concept simulation for this phenomenon of unintentional modulation and polarization at 300 GHz. The goal here is to draw a distinction between the factors that are affected by linear scattering parameters of the 3D EM configuration and the nonlinear modulation effects that are caused by the switching elements in a simplified FPGA circuit. The circuit is simplified because of the infeasibility of having a full scale electromagnetic simulation of an FPGA. There is no surprise that modulation happens through this mechanism, any nonlinear element can create some unintentional modulation. This simulation configuration will examine what factors play the key roles and if the modulation is strong enough to be sensed and detected at a distance.

In the EM simulation model, a 25 dBi diagonal horn is used on the transmitter side with a 20 cm diameter near field reflector focuser with an elliptical profile that creates a focus 35 mm away from the aperture of the main reflector. This reflector system illuminates the simplified FPGA circuit with a 3 dB spot diameter of 0.7 mm. More details about design specifications of the focuser are given in [28]. Another 25 dBi diagonal horn is used on the receiver side at a distance of d = 150 mm. The entire simulation is repeated for the case where the receiver horn is polarized vertically and horizontally. It may seem counter intuitive to have an intentional polarization mismatch between the transmitter and the receiver; however, this results in significant benefits in terms of SNR as we will analyze it further here. The basic circuit components in FPGA are modeled as a 10 mm diameter wire loop placed 0.5 mm above a 50 mm square ground plane encased in a 1 mm thick encapsulant. This model intends to mimic the power connections of the FPGA so it has a similar size as the FPGA chip. The 3D configuration is shown in Fig. 1. The 3 port S-parameter values are simulated using CST's Integral Equation Solver.

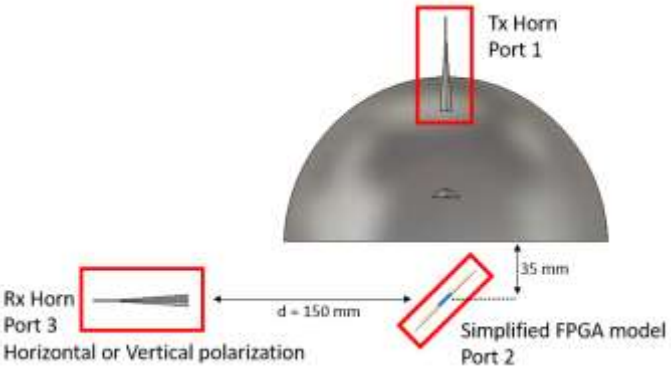


Fig. 1 The 3D EM model showing the transmitter, receiver, and the simplified FPGA circuit.

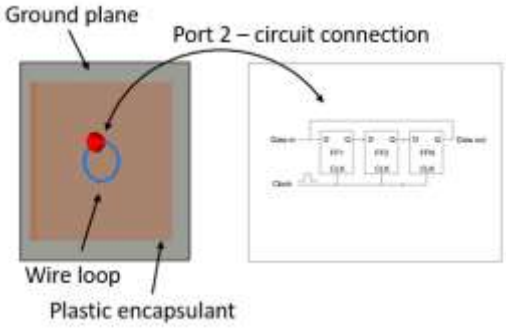
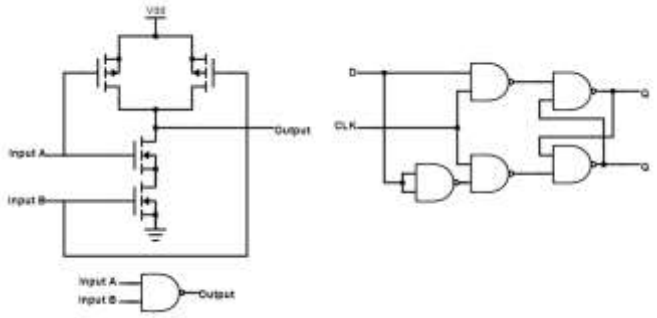


Fig. 2 Diagram of the switching circuit that is inserted into the simplified FPGA circuit.

In the next step of the simulation, a switching circuit is inserted into the loop modeled in the 3D EM simulation. The real implementation of the switching circuit that we use in measurements in Section III involves a shift register made of a

cascade of thousands of flip-flops that are all switched at a particular frequency. In the results presented in this section, this frequency is chosen to be 1 GHz and 1.3 GHz and used as the clock of the flip flops. We model the same scenario in ADS at a smaller scale, where we use only a single flip flop as opposed to thousands of cascaded flip flops. Three flip-flops are cascaded and the power lines that supply them are connected to the simplified FPGA model in the 3D EM model. A diagram of this configuration is shown in Fig. 2. The flip-flops are realized using NAND gates made up of CMOS transistors as shown in Fig. 3.



(a) (b)

Fig. 3 The schematic of a CMOS NAND gate is shown in (a) and the schematic of a D Flip Flop made up of NAND gates is shown in (b).

There are two main paths for the signal from the transmitter to arrive at the receiver. The primary route is simply through specular reflection from the ground plane, mostly explained by S_{31}. This route mostly preserves polarization and involves no nonlinear effects. The secondary route is through modulated scattering from the simplified FPGA circuit. The transmitted signal is initially received by the simplified FPGA circuit, mostly explained by S_{21}. The signal experiences some nonlinear effects due to the active circuit, calculated by the circuit simulation. Finally, the signal is scattered from the simplified FPGA circuit and received by the receiver horn, mostly explained by S_{32}.

As the excitation signal, we use a 0 dBm 300 GHz carrier with a -90 dBm flat spectrum noise (this value is chosen to be consistent with the noise floor levels of the measured signal in the bandwidth of interest). The simulated received spectrums for the polarization filtered and non-polarization filtered case are shown in Fig. 4 and Fig. 5. It should be noted that the frequency peaks exactly overlap in reality, the shift is introduced while plotting to make visual comparison easier. The two traces correspond to two scenarios where the receiver horn (port 3) in Fig. 1 is polarized vertically (no polarization filtering) or horizontally (polarization filtering). The case where the horn is polarized horizontally is labeled as "polarization filtering" because it uses deliberate mismatch between the transmitter and the receiver to filter out the undesirable carrier and the noise coming from the transmitter which is predominantly vertically polarized. The 300 GHz carrier, transmitter caused noise, 1 GHz peaks caused by switching activity and its harmonics can be seen for both polarization cases. It can also be seen that the undesirable 300 GHz carrier is approximately 29 dB weaker for the polarization filtered case which is perfectly consistent with the reduction in S_{31} when polarization filtering is used (when Tx is vertical, but Rx is horizontal). This also results in a 29 dB reduction in the transmitter caused noise, which directly translates to an increase in SNR. The desirable 1 GHz modulated peak is slightly stronger for the polarization filtered case. This is due to a slight difference in S_{32} values for the horizontal and vertical receivers. The difference is very much dependent on the geometry of the simplified FPGA model, which was a 10 mm diameter wire loop and the location at which it is fed. Different geometries such as rectangular and elliptical loops were used to excite different polarization characteristics which resulted in differences in the relative strengths of the modulated peaks, which is to be expected. Only the 10 mm loop result is shown here due to its simplicity.

Since the phenomenon of unintentional modulation depends on a carrier signal injected onto the surface of the FPGA from an outside source, the electromagnetic contribution of every single transistor and connection is relevant. Therefore, an exact simulation of this phenomenon would require every transistor and connection to be simulated in a full wave EM solver. It is infeasible to simulate this level of complexity. Instead, for the proof of concept, we use simplified substitute for the FPGA to mimic the nonlinear effects that cause this unintentional modulation. Moreover, simulating a very low frequency modulation (~1 MHz) onto very high frequency (300 GHz) creates significant difficulties. The duration of the simulation must be long enough to contain dozens of cycles of the low frequency and the time samples must be fine enough to have many samples within a single cycle of the high frequency. For this reason, the modulation frequency is chosen to be 1 GHz in the simulation and 1.6 MHz in measurements shown in Section III.

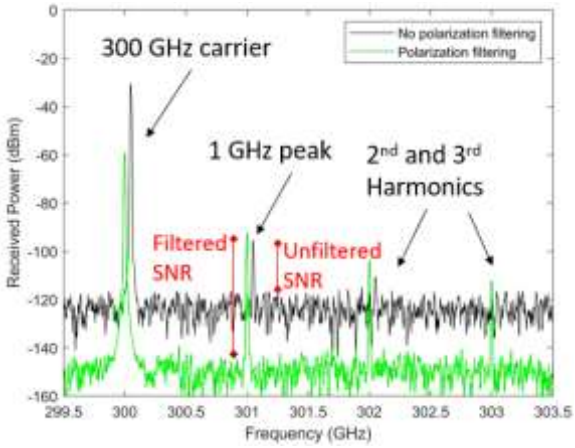


Fig. 4 Simulated received spectrum when flip-flop shift frequency is 1.0 GHz. The no polarization filtering trace is shifted by 0.05 GHz to prevent overlapping and allow for easier visual comparison.

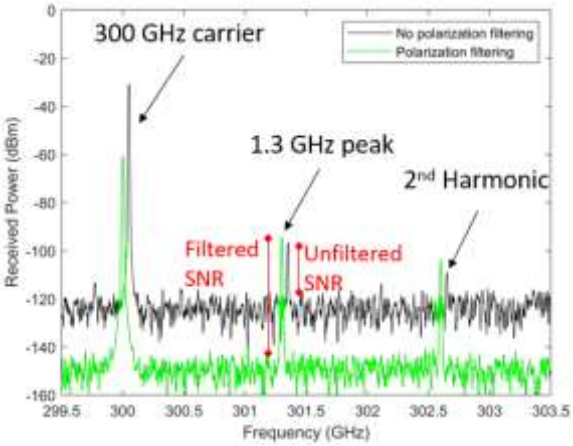
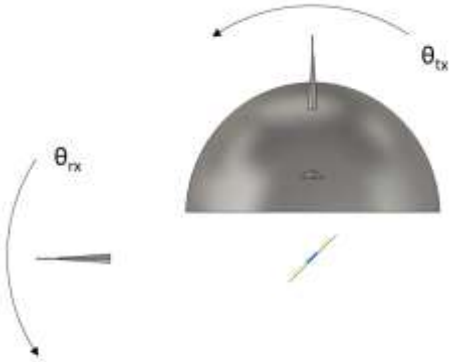
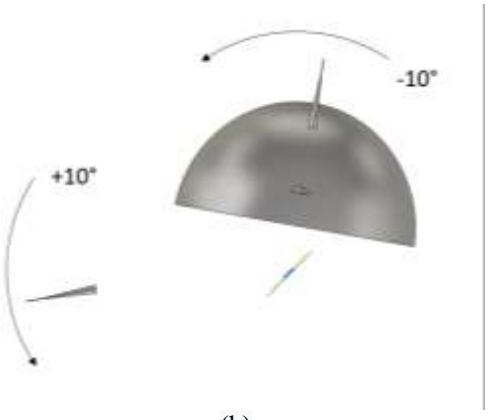


Fig. 5 Simulated received spectrum when flip-flop shift frequency is 1.3 GHz. The no polarization filtering trace is shifted by 0.05 GHz to prevent overlapping and allow for easier visual comparison.

The simulation set up shown in the Fig. 1 is further used to observe and study the angular dependency of the Tx and Rx. The Tx and Rx are independently rotated -30° to +30° around the FPGA with 5° increments, as shown in Fig. 6 (a) Model showing the angular rotation (b) angular rotation of 10 deg (c) Unfiltered signal strength variation (d) filtered signal strength variation (a). For instance, a 10° rotation is shown in Fig. 6 (a) Model showing the angular rotation (b) angular rotation of 10 deg (c) Unfiltered signal strength variation (d) filtered signal strength variation (b). The similar analysis as shown in Fig. 4 and Fig. 5 were performed to get signal level, noise level, SNR for both filtered and unfiltered Rx.



(a)



(b)

Unfiltered Signal Level

rx \ tx	-30	-25	-20	-15	-10	-5	0	5	10	15	20	25	30
-30	-132	-133	-138	-139	-134	-136	-128	-134	-143	-142	-137	-133	-131
-25	-130	-130	-134	-137	-136	-123	-124	-131	-142	-139	-135	-139	-131
-20	-130	-132	-132	-135	-130	-118	-110	-128	-140	-139	-135	-133	-141
-15	-130	-130	-130	-132	-133	-115	-110	-109	-134	-134	-136	-140	-141
-10	-128	-129	-128	-131	-127	-111	-108	-97	-117	-135	-141	-141	-143
-5	-125	-127	-129	-128	-123	-112	-91	-101	-124	-128	-140	-147	-144
0	-130	-127	-128	-130	-123	-97	-97	-114	-120	-129	-133	-143	-152
5	-137	-127	-128	-122	-111	-109	-117	-108	-129	-136	-130	-137	-144
10	-129	-130	-116	-114	-122	-111	-103	-117	-142	-132	-131	-136	-141
15	-132	-133	-115	-122	-130	-115	-106	-125	-139	-150	-136	-142	-138
20	-127	-118	-125	-119	-126	-115	-113	-117	-133	-132	-131	-132	-131
25	-123	-125	-124	-121	-122	-122	-109	-116	-131	-129	-128	-127	-128
30	-123	-122	-128	-131	-127	-113	-108	-114	-130	-129	-129	-125	-126

(c)

Filtered Signal Level

rx \ tx	-30	-25	-20	-15	-10	-5	0	5	10	15	20	25	30
-30	-126	-125	-126	-130	-125	-120	-112	-124	-133	-132	-129	-125	-123
-25	-122	-122	-122	-128	-129	-112	-111	-123	-134	-129	-129	-130	-125
-20	-123	-124	-125	-124	-120	-105	-106	-127	-133	-133	-136	-127	-132
-15	-122	-120	-124	-121	-121	-106	-99	-106	-127	-127	-129	-130	-138
-10	-121	-119	-120	-120	-117	-101	-91	-99	-112	-128	-134	-133	-134
-5	-118	-119	-120	-121	-114	-103	-84	-98	-116	-120	-133	-135	-132
0	-121	-121	-124	-118	-114	-86	-94	-106	-112	-118	-121	-135	-133
5	-127	-125	-120	-116	-108	-100	-106	-98	-122	-129	-123	-124	-133
10	-129	-119	-108	-106	-122	-105	-95	-118	-131	-123	-125	-122	-122
15	-126	-119	-105	-118	-119	-104	-100	-111	-132	-125	-137	-132	-140
20	-125	-110	-113	-113	-123	-108	-101	-108	-128	-127	-126	-126	-125
25	-114	-115	-111	-116	-121	-112	-99	-109	-125	-124	-122	-121	-121
30	-116	-112	-125	-124	-121	-108	-107	-108	-126	-125	-124	-119	-120

(d)

Fig. 6 (a) Model showing the angular rotation (b) angular rotation of 10 deg (c) Unfiltered signal strength variation (d) filtered signal strength variation

Fig. 6 (c) and (d) show the unfiltered and the filtered signal strength. For the signal level, two green (well performing) regions can be observed, which are indicated by ellipses. The first region is a vertical green strip around $\theta_{tx} = 0°$, meaning better performance is achieved when the Tx (focuser) targets the FPGA with an angle $\sim 45°$. We believe this is because an angle of 45° results in a balanced spot between how much signal is injected into the FPGA and how much signal can escape from the FPGA and reach the Rx. If Tx targets the FPGA with a grazing angle, very little of the power will be absorbed by the FPGA. On the other hand, if the Tx targets the FPGA with an angle close to 0°, the huge reflector will obstruct all the modulated signal coming out of the FPGA. The second green region corresponds to $\theta_{tx} = -\theta_{rx}$, which preserves specular arrangement.

III. Side Channel Sensing: Polarization and Distance

This section presents the measurement results for the scenario outlined in the previous section. Subsection A describes the details of the equipment, components, and the measurement setup. Subsection B presents the measured SNR values obtained from a 2D scan of the FPGA and the difference that polarization makes at a fixed receiver to FPGA distance. Finally, Subsection C describes effect of receiver to FGPA distance has on the SNR.

A. Measurement Setup

The concept of backscatter side channels as described in Section II is realized at 300 GHz using a Terasic board with Altera Cyclone V FPGA, custom made Virginia Diodes 300 GHz transmitter (Tx-271) and receiver (Rx-159) pair, optical positioning tools to ensure alignment and proper scanning. The transmitter is connected to a 25 dBi diagonal horn antenna [29] which feeds a 20 cm diameter elliptical near field focuser with a 0.7 mm 3 dB spot size that is 35 mm away from the aperture of the main reflector as detailed in [28]. The feed antenna was measured by us to have better than 30 dB cross polarization to ensure validity of the polarization measurement. The focuser illuminates a 0.7 mm diameter spot on an FPGA that angled at 45 degrees and is mounted on two Zaber brand micron precision positioners which move it vertically and at a 45° angle [30]. Having this specular arrangement could make direct coupling from Tx to Rx worse; however, proper alignment is of extreme importance for good SNR but more importantly for repeatability. Good SNR results can be obtained with very slight misalignment, but this would still create huge repeatability problems in our research. The optical components that we use allowed for greater repeatability if we went along with the perfect 90° grid alignment.

The FPGA is toggling its gates at a frequency of 1.6 MHz to create the unintentional modulation. The backscattered signal is received by the receiver that is connected to an identical diagonal horn antenna. The receiver is d = 150 mm away from the board unless stated otherwise. All of the components are fixed to an optical breadboard and optical rails for alignment. The measurement setup is shown in Fig. 6.

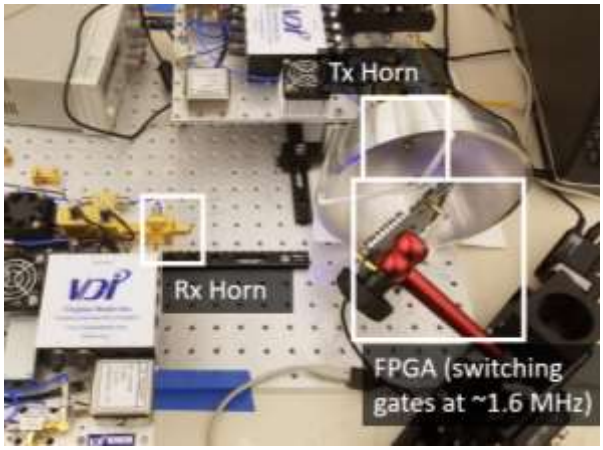


Fig. 6 300 GHz backscatter side channel measurement setup.

There is a high variability of signal strength and noise floor based on which region of the FPGA is illuminated by the transmitter. Two hot spots were identified on the FPGA board by a 2D scan with a resolution of 1mm: a capacitor region on the board and the center of the FPGA chip. Two 6 mm by 7 mm region that contain these hotspots were further scanned with more precise 0.5 mm increments to get a better understanding of the signal variation and find the optimum spot for the best signal. Cell dimension corresponds to the spot size of ellipsoidal transmitter used in measurements. These rectangular regions are highlighted in Fig. 7.

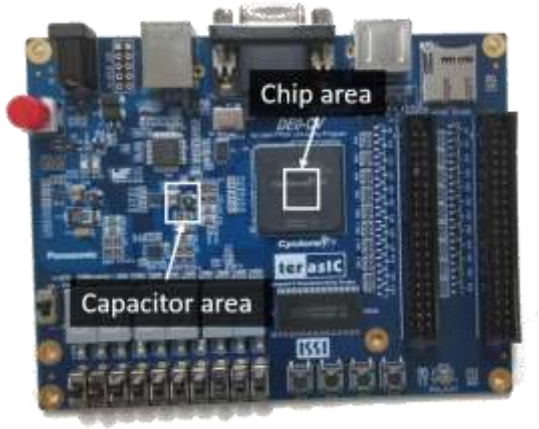


Fig. 7 The rectangular regions that contain the hotspots.

B. Effect of Polarization Filtering

In this EM backscattering side-channel measurement scheme, we are only interested in the signals that are modulated onto the carrier frequency. The reception of the carrier signal itself and all other artifacts created by the transmitter are an undesirable consequence of the method. Also, since the entire mechanism uses the FPGA as an unintentional modulator, the desired signal ends up being much weaker (e.g. 40 dB) than the carrier. This relatively much stronger carrier signal causes significant saturation problems in the receiver due to issues with dynamic range. Using a millimeter wave filter is infeasible since the modulation frequency is very small compared to the carrier (~2 MHz vs. 300 GHz), the filter would require an infeasibly sharp response to reject the undesired 300 GHz carrier without reducing the modulated signal. Moreover, the imperfections of the transmitter create a noise floor higher than that of the thermal noise floor of the receiver.

The transmitter is configured to create a vertically polarized spot on the FPGA. Most of the transmitted wave, containing a strong carrier and transmitter noise, has a specular reflection from the surface and remains vertically polarized. A small part of the incident wave is absorbed, unintentionally modulated, and backscattered. This backscattered component is what we are interested in and its polarization depends on the bond-wires, traces, connection routing, etc. within the FPGA. This makes the polarization difficult to predict exactly; however, we know that it is not necessarily vertical.

Even though predicting the precise polarization characteristics is infeasible as mentioned in the earlier section, we can say for certain that the polarization of the relevant part of the backscattered signal will depend heavily on the geometry of the FPGA circuit. Consider a transceiver that captures ~1 GHz signals from the air and retransmits them after shifting the carrier to ~2 GHz. If a circularly polarized antenna is connected to this transceiver, the polarization of the retransmitted ~2 GHz signal would also be circularly polarized. The polarization of the reradiated signal depends only on the antenna connected to the transceiver doing the frequency shifting. The original ~1 GHz signal could have any arbitrary polarization, but this would not influence the polarization of the retransmitted 2 GHz signal. This is the principle that the filtering we use relies on.

To reduce the effect of the carrier and the transmitter noise, we introduce a polarization mismatch between the transmitter and the receiver as shown in Fig. 8. The receiver is converted from vertical to horizontal polarization using a 90 degree waveguide twist from Virginia Diodes [31]. This filters out a significant portion of the specular-reflected carrier and transmitter noise which is almost entirely vertically polarized.

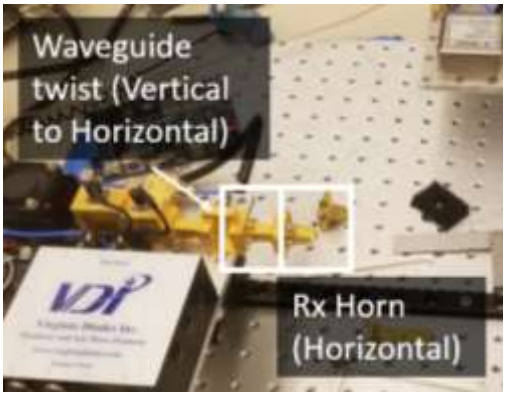


Fig. 8 The measurement setup using polarization filtering.

Comparison of measured spectrums with and without polarization filtering is shown in Fig. 9. The 300 GHz carrier is suppressed by 20 dB (-28 dBm vs -48 dBm), this helps prevent receiver saturation and shows that the carrier is almost entirely vertically polarized. The noise floor around the frequency of interest is reduced by 11 dB (-122 dBm vs. -133 dBm), this is because the noise floor is elevated due to the transmitter nonidealities. Finally, most interestingly, the signal of interest is enhanced by 2 dB (-77 dBm vs -75 dBm). As stated earlier, the backscattered signal of interest is not necessarily vertically polarized, in fact it has a greater horizontal component than vertical component. Indeed, a similar enhancement of 2 dB was also observed in simulation for the simplified FPGA model consisting of a circular wire loop. The combined effect of an 11 dB reduction in noise floor reduction and 2 dB signal power enhancement yields a 13 dB increase in SNR.

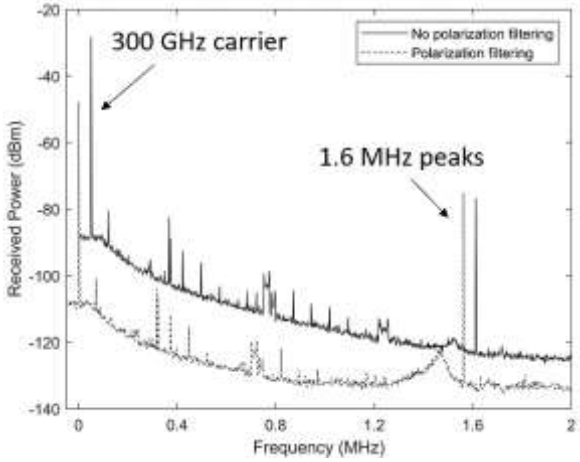
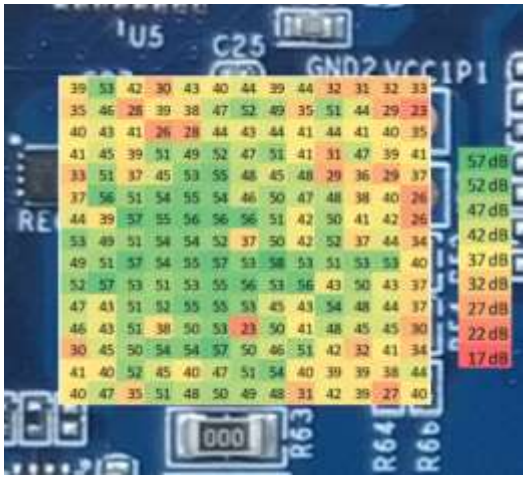


Fig. 9 Spectrums measured from the capacitor area with and without polarization filtering. The no polarization filtering trace is shifted by 0.05 MHz to prevent overlapping and allow for easier visual comparison.

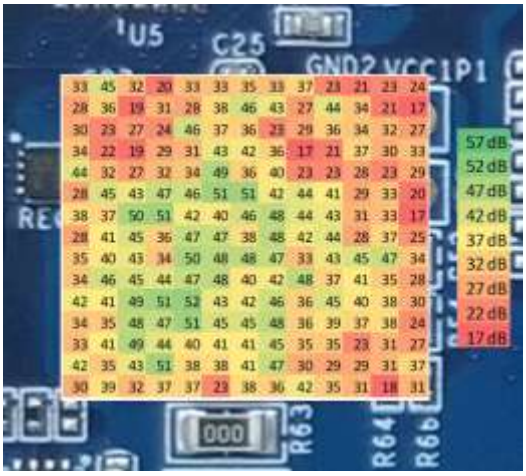
This measurement was conducted for the two 6 mm by 7 mm regions that are highlighted as capacitor area and chip area in Fig. 7. The entire region was scanned with 0.5 mm increments resulting in 13 by 15 data points.

The SNR values measured from the capacitor area are shown in Fig. 10. In Fig. 10. (a) the SNR values with the polarization filtering can be seen. The highest values are localized in a roughly circular region corresponding to the location of the capacitor. An average SNR value of 48 dB with a maximum of 58 dB is observed. In Fig. 10. (b) the SNR values without the polarization filtering can be seen. Similar to the filtered case, the highest values are localized in a roughly circular region corresponding to the location of the capacitor. An average SNR value of 36 dB with a maximum of 52 dB is observed. It can be seen that polarization filtering yields 12 dB better SNR on the average. This is due to a 2 dB signal strength increase on the average and 10 dB noise floor reduction on the average. The noise floor values measured from each spatial sample showed significant variation for both cases (-130 dBm to -150 dBm with polarization filtering, -120 dBm to -140 dBm without polarization filtering). The highest SNR values were measured close to the center of the capacitor region for both filtered and unfiltered cases.

Similar SNR results were obtained from the chip area as shown in Fig. 11. The signal levels are approximately 20 dB weaker for the chip area as compared to the capacitor area. This could be due to the interference of the plastic encapsulant material that protect the FPGA and the interconnections. The highest SNR values for the filtered case is located close to the center whereas for the unfiltered case the highest SNR values were measured towards the top right corner of the highlighted region. Average SNR is enhanced by 15 dB. For this region, polarization filtering is significantly more impactful. Most importantly, there are weak spots for the unfiltered case where little to no signal is received (0 dB SNR) whereas the enhancement from polarization filtering was enough to boost the SNR to a level that can be detected anywhere.



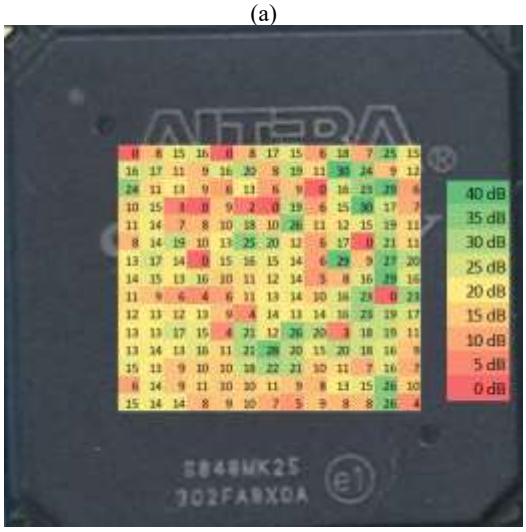
(a)



(b)

Fig. 10 Measured SNR values in dB for d = 15 cm from the capacitor area: a) with polarization filtering (average 48 dB) and b) without polarization filtering (average 36 dB). (0.5mm resolution)

(a)



(b)

Fig. 11 Measured SNR values in dB for d = 15 cm from the chip area in dB: a) with polarization filtering (average 27 dB) and b) without polarization filtering (average 12 dB).

C. *Effect of receiver distance*

There is significant difference when it comes to the noise characteristics of the signal with and without polarization filtering. Here we will examine the effect receiver distance d, as shown in Fig. 1, has on SNR. In these tests, the receiver distance is kept constant, so one would expect the SNR to have a $1/r^2$ trend. However, the primary source of the noise is not the thermal noise of the receiver but instead the unintentionally generated signals coming from the transmitter and the FPGA. This means the SNR will decay slower than $1/r^2$. This behavior can be characterized by including the transmitter noise in the simple SNR formula.

$$SNR\ (dB)\ =\ S\ (dB) - N\ (dB) \tag{1}$$

$$\text{SNR} = \frac{P_{modulated}}{N_{transmitter}+N_{thermal}} \tag{2}$$

where, $P_{modulated} \propto \frac{1}{r^2}$ is the strength of the desired modulated peak. $N_{transmitter} \propto \frac{1}{r^2}$ is the noise created by the transmitter and decays as the receiver moves away. $N_{thermal}$ is the thermal noise, independent of distance.

To explain the measured SNR, with the theoretical model, the noise observed in the measurements is assumed to be created by these two sources: thermal noise and the noise generated by transmitter itself. Since the processor is not intended to function as a transmitter, only a part of the total radiation coming out of the board carries meaningful information. This undesired part of the transmitted signal lowers the quality of the signal in a way that is more complex. Since this part of the signal is radiated from the transmitter, it gets weaker by a factor of r^2 , whereas the thermal noise is constant, as pointed out in (2). For this reason; at smaller distances $N_{transmitter}$ is more significant, at larger distances $N_{thermal}$ is more significant, and at intermediate distances the SNR trend is neither constant nor r^2. This behavior can be captured using the following SNR fit expression:

$$SNR_{fit} = \frac{\frac{a}{r^2}}{\frac{b}{r^2}+c} \tag{3}$$

The change in measured SNR for receiver distances of up to 45 cm is shown in Fig. 12 for both with and without polarization filtering and the fitted curved. The polarization filtered case has better SNR for all distances. The decay trend is indeed slower than $1/r^2$ as predicted. For even longer distances, the noise created by the transmitter would start to be dominated by the thermal noise of the receiver and the SNR behavior would start to follow a $1/r^2$ trend, which was not reached. In these ranges, the fitted curves are able to show the same type of decay with respect to distance. The measured results have variations from this curve due to multipath interference from the ground and the large transmitter/receiver system as well as the difficulty in maintaining perfect alignment when the system is repositioned. The measurements were only taken up to 45 cm due to the limitations caused by the length of the optical flat plane on which the equipment was placed. The SNR values measured at this 45 cm limit are 44 and 54 dB for unfiltered and filtered configurations respectively, indicating that the signal can be detected at distances much farther than 45 cm.

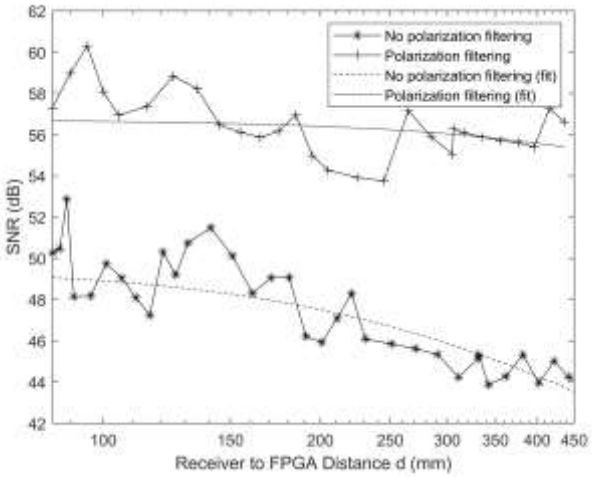


Fig. 12 The SNR behavior as the distance between the receiver and FPGA increases with and without polarization filtering along with the fitted SNR curves.

The coefficients calculated for the polarization filtered curve fit shown in Fig. 12 using equation (3) are as follows:

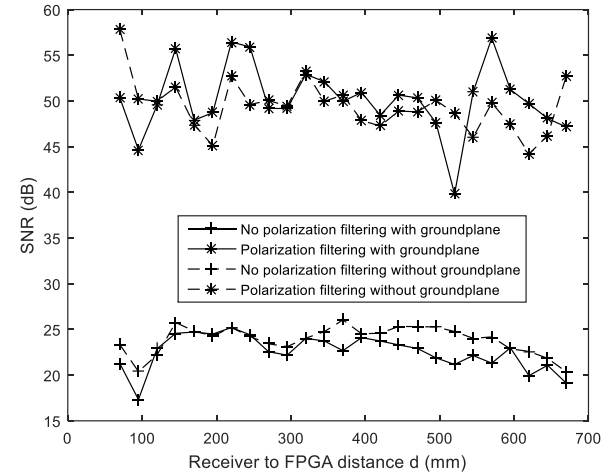
$$(a_1, b_1, c_1) = (1mm^2, 2.07\text{x}10^{-6}mm^2, 2.48\text{x}10^{-12})$$

And the coefficients calculated for the no polarization filtered curve are:

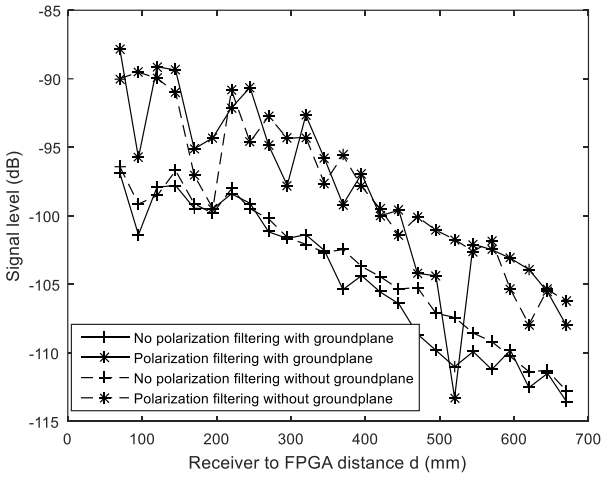
$$(a_2, b_2, c_2) = (1mm^2, 1.15\text{x}10^{-5}mm^2, 1.51\text{x}10^{-10})$$

For both cases, a was normalized to be 1 mm^2. To rule out the possibility of strong nonlinearity effects, we have examined the linearity of the modulation behavior. Our experimental setup allows us to manually change the output power of the transmitter. So we have examined the linearity of the modulation behavior. When the output power of the transmitter was varied between -20 dBm to +10 dBm, no noticeable deviation from linear response was observed. The strong variance of the distance response of the SNR is possibly due to multipath interference caused by the reflectors, ground, PCB of the FPGA.

SNR variation with the receiver to FPGA range d, for two cases: with and without ground plane (perfect electric conductor PEC), was further explored using our simulation set up shown in Fig. 1. Fig. 14 (a) shows the SNR with distance. It can be observed that the SNR does not change as the distance increases. Here, neither the Rx to FPGA distance nor the presence of a ground plane have any meaningful effect on the SNR. This is due to the fact that the Tx noise dominates the thermal noise in the simulation. The simulated signal strength shown in Fig. 14 (b) show $\sim 1/r^2$ trend.



(a)



(b)

Fig. 13 (a) Simulated SNR and (b) signal strength with receiver to FPGA distance with and without the ground plane

IV. Side Channel Sensing: Multiple Bits

In previous sections, the FPGA was configured to switch all of its gates at the same frequency. This allows for maximum signal strength for a single modulated peak, in other words a 1-bit backscattered side-channel. However, thanks to the additional SNR that can be achieved with polarization filtering, it is possible to excite and detect such unintended backscattered peaks at multiple frequencies (bits) simultaneously. Increase in the number of bits that can be backscattered in parallel increases the capacity of how much data can be detected, which has great benefits for practical side-channel applications such as monitoring the behavior of an IC, secretly transmitting data using malicious hardware modifications such as Hardware Trojans, or deliberately toggling FPGA gates to create an antenna-less RF transceiver using nothing but an FPGA which can be used as RFID device.

In this section we divide the FPGA into 4 modules and switch the gates in each module at a different frequency. This creates a 4-bit channel where each bit corresponds to a different physical location on the chip as shown in Fig. 14. The measurement set up used is shown in Fig. 6 with a distance

d = 15 cm. The overall signal received from the chip is shown in Fig. 15.

Fig. 14 Location and the frequencies of modules that create the 4 bits.

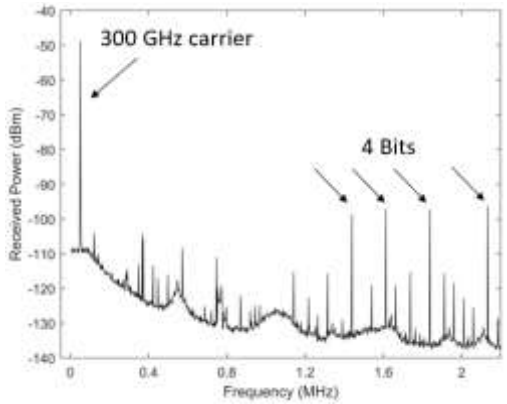


Fig. 15 Spectrum received from the entire chip.

Moreover, the usage of a THz focuser allows for the spatial analysis of this side-channel phenomenon. In a practical application, the FPGA will not be configured such that the entire chip does a single task. It will have different modules in different locations with different tasks and different electromagnetic signatures. It is desirable for a focused measurement scheme to be able to amplify the signal of one module while keeping the interference from other modules to a minimum. With the 4-bit FPGA configuration, we try to measure how much the signal from a single module can be isolated from other modules. Since a smaller part of the FPGA is generating each bit, the signal strength is lower compared to the 1-bit configuration. For this reason, the measurements are only done using the polarization filtering technique.

To quantify how much the signal of a single module (in other words a single bit) can be emphasized over others, we find the spatial locations where that bit is the strongest and compare its signal strength with that of the second strongest bit (a positive value). To quantify how much the signal of a single bit can be filtered out, we find the spatial locations where that bit is not the strongest and compare its signal strength with the signal strength of the strongest bit (a negative value).

The spectrums received from the most dominant and least dominant locations for bit 1 is shown in Fig. 16. For the spectrum where Bit 1 is the most dominant, it is 6.8 dB stronger than the second strongest bit received from that location. This means, if we were only interested in the signals coming from Bit 1 region, we could target the focuser on this location and reduce the interference from other modules by at least 6.8 dB. For the spectrum where Bit 1 is the least dominant, it is 11.3 dB weaker than the strongest bit received from that location. This means, if Module 1 was creating significant interference that we didn't want to receive, we could target the focuser on this location and maximally limit the contribution of Module 1 compared to other modules.

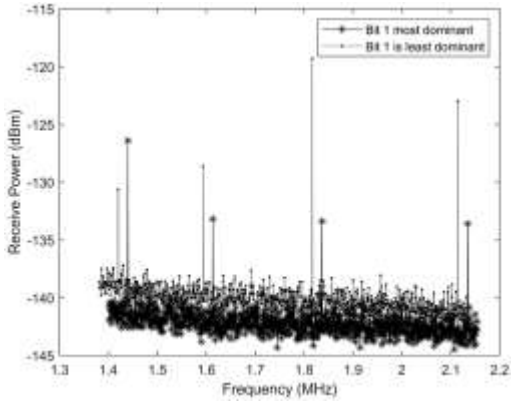


Fig. 16 The spectrums received from the spatial samples that yielded the most dominant and the least dominant results for Bit 1.

The analysis described above has been done for the entire chip area and the results are shown in Fig. 17. The focuser was targeted at each of these locations, the SNR value was recorded, and then overlaid on the image of the chip where they were measured. The two optimum locations that yield -11.3 dB and 6.8 dB can be found here. The most important thing to note here is the lack of any apparent order. Intuitively one might expect that the signal coming from Bit 1 would be the most dominant when the focuser targets the location that corresponds to Module 1. In a practical side-channel application it would be convenient if this were the case. With only the knowledge of the locations of the modules, a focuser could be directed at the optimal spot without any guess work or any need for scan. Unfortunately, this is not what we observe. The locations where a module is dominant or not seems to be scattered randomly. This reinforces the idea that this modulation is not created primarily by the logic circuit itself but instead the supplementary circuits around it such as bondwires, connection blocks, power connections, capacitor connections, etc. This makes it difficult to guess the optimal spots ahead of time since the location of a module on an FPGA is easier to control compared to these supplementary circuits which could explain the lack of correlation between the location where certain modules are most and least dominant.

Fig. 17 Relative strength of bit 1 compared to other bits.

This analysis is done for all 4 bits. The most dominant and the least dominant signal values for each bit is shown in Table I. Other than Bit 4 having slightly greater variance, there is no significant difference between the level of dominance between bits. To reemphasize, the values quoted in this section are not SNR values, they are variances in the SNR between the bits and how much they are greater or lower than the SNR of other bits.

Table I Best achieved relative strengths that emphasize or filter out a single bit.

	Most Dominant (w.r.t. second most dominant bit)	**Least Dominant (w.r.t. most dominant bit)**
Bit 1	6.8 dB	-11.3 dB
Bit 2	6.7 dB	-9.5 dB
Bit 3	6.4 dB	-10.7 dB
Bit 4	7.3 dB	-11.9 dB

As mentioned previously, there is no apparent correlation between the locations of the modules and optimal signal locations. However, this lack of correlation does not mean the ability to focus on different spatial locations is not useful. As we show in Table I, for any particular bit, it is possible to find a spot where it is at least 6.4 dB stronger than all the other bits and a spot where it is at least 9.5 dB weaker than all the other bits. All the benefits of being able to focus on a single module over other modules is still realizable as long as these optimal locations are characterized by a 2D scan of the FPGA.

Additionally, one might ask what the effects of no focusing and uniform illumination would be on the received signals. The main reason for using focusing techniques is because the information about the chip activity in the FPGA is location dependent. If the illumination is done on the entire chip, it would be an average response which is not desirable for our study.

V. Conclusions

We present a backscattered side-channel sensing scheme at 300 GHz using an ordinary FPGA not designed to operate anywhere close to this band. A proof of concept EM-circuit co-simulation analysis of this surprising phenomenon is given using a structurally simplified FPGA model and a near field focuser. In these simulations, the effect of polarization is also explored. Specifically, creating a deliberate polarization mismatch between the receiver and the transmitter. This is shown to suppress the very strong undesirable carrier signal significantly and reducing the high level of noise created by the transmitter. We realize this 300 GHz backscattered side-channel using an ordinary FPGA that is configured to flip its gates at a particular frequency single frequency transmitting a single bit. This backscattered side-channel was measured to have an SNR as high as 36 dB, which was further elevated to 48 dB using the proposed polarization filtering technique. In addition to this, we use a 300 GHz near field focuser to scan the FPGA with a resolution of 0.7 mm to find hotspots for these backscattered signals and characterize spatial variance. Furthermore, the FPGA is then configured to have 4 different modules flipping its gates at 4 different frequencies thereby transmitting 4 bits in parallel, which greatly improves the capacity for practical side-channel applications. Finally, the spatial resolution and the scanning capability of the near field focuser is used to scan the FPGA to find spatial variances between these 4 modules, with the purpose of isolating to enhance or reject the signal from each module. It was found that it is possible to find distinct spots where each of the modules can be enhanced to be at least 6.4 dB stronger than the other modules.

VI. References

[1] D. Agrawal, B. Archambeult, J. R. Rao, and P. Rohatgi, “The EM
Proceedings of Cryptographic Hardware and Embedded Systems - CH
29–45.

[2] L. Batina and M. Robshaw, Cryptographic Hardware and Embedde
2014 16th International Workshop, Busan, South Korea, Septer
Proceedings. Berlin: Heidelberg, 2014.

[3] M. G. Khun, “Compromising emanations: eavesdropping risks of c
The complete unofficial TEMPEST
http://www.eskimo.com/˜joelm/tempest.html, 2003.

[4] A. Zajic and M. Prvulovic, “Experimental demonstration of electrom
leakage from modern processor-memory systems,” Electromagnetic C
Transactions on, vol. 56, no. 4, pp. 885–893, Aug 2014.

[5] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “Stealing ke
radio: Cheap electromagnetic attacks on windowed exponentiation
Workshop on Cryptographic Hardware and Embedded Systems. Sprin
228..

[6] Y.-i. Hayashi, N. Homma, T. Mizuki, H. Shimada, T. Aoki, H. Sone,
L. Danger, “Efficient evaluation of em radiation associated with inform
cryptographic devices, ”IEEE Transactions on Electromagnetic Comp

[7] M. G. Kuhn, “Compromising emanations of lcd tv sets,” IEEE Trans. C
Compatibility, vol. 55, no. 3, pp. 564–570, June 2013.

[8] H. Sekiguchi and S. Seto, “Study on maximum receivable distance fo
of information technology equipment causing information leakage
Electromagnetic Compatibility, vol. 55, no. 3, pp. 547–554, June 201

[9] Y. Hayashi et al., "Analysis of Electromagnetic Information Leakage F
Devices With Different Physical Structures," in IEEE Transactions
Compatibility, vol. 55, no. 3, pp. 571-580, June 2013.

[10] e. a. Nader Sehatbakhsh, EMMA: Hardware/Software Attestatio
Embedded Systems Using Electromagnetic Signals, New York: IEEE

Symposium on Microarchitecture (MICRO '52). Association for Computing Machinery, New York, NY, USA, 2019.

[11] N. Sehatbakhsh et al., "REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals," in IEEE Transactions on Computers, vol. 69, no. 3, pp. 312-326, 1 March 2020.

[12] Khan, H.A., Sehatbakhsh, N., Nguyen, L.N. et al. Malware Detection in Embedded Systems Using Neural Network Model for Electromagnetic Side-Channel Signals. J Hardw Syst Secur 3, 305–318 (2019).

[13] H. A. Khan et al., "IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems," in IEEE Transactions on Dependable and Secure Computing, 2019.

[14] L. N. Nguyen, C. Cheng, M. Prvulovic and A. Zajić, "Creating a Backscattering Side Channel to Enable Detection of Dormant Hardware Trojans," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 7, pp. 1561-1574, July 2019.

[15] L.N. Nguyen, et al. "A Comparison of Backscattering, EM, and Power Side-Channels and Their Performance in Detecting Software and Hardware Intrusions". J Hardw Syst Secur, 2020.

[16] S. Adibelli, P. Juyal, L. N. Nguyen, M. Prvulovic and A. Zajic, "Near Field Backscattering based Sensing for Hardware Trojan Detection," in IEEE Transactions on Antennas and Propagation, June 2020.

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

[18] N. Sehatbakhsh, et. al. "EMSim: A Microarchitecture-Level Simulation Tool for Modeling Electromagnetic Side-Channel Signals," in 2020 IEEE International Symposium on High Performance Computer Architecture (HPCA), San Diego, CA, USA, 2020.

[19] J. Kimionis, A. Bletsas and J. N. Sahalos, "Bistatic backscatter radio for power-limited sensor networks," 2013 IEEE Global Communications Conference (GLOBECOM), 2013, pp. 353-358.

[20] B. Badihi, A. Liljemark, M. U. Sheikh, J. Lietzén and R. Jäntti, "Link Budget Validation for Backscatter-Radio System in Sub-1GHz," 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019, pp. 1-6.

[21] Q. Tao, Y. Li, C. Zhong, S. Shao and Z. Zhang, "A Novel Interference Cancellation Scheme for Bistatic Backscatter Communication Systems," in IEEE Communications Letters, vol. 25, no. 6, pp. 2014-2018, June 2021.

[22] M. Katanbaf, A. Saffari and J. R. Smith, "Receiver Selectivity Limits on Bistatic Backscatter Range," 2020 IEEE International Conference on RFID (RFID), 2020, pp. 1-8.

[23] B. Yang, S. Wang, H. Ding and W. Zhang, "Signal Detection for Bistatic Backscatter with Dual Antennas," 2020 IEEE 20th International Conference on Communication Technology (ICCT), 2020, pp. 1195-1199.

[24] C.-L. Cheng, L. N. Nguyen, M. Prvulovic, and A. Zajic, “Exploiting switching of transistors in Digital electronics for RFID tag design,” IEEE International Conference on RFID, pp. 1-2, April 2018, Orlando FL..

[25] P. Juyal, S. Adibelli and A. Zajic, "THz Near Field Focusing using Cassegranian Configuration for EM Side-channel Detection," 2018 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, Boston, MA, 2018.

[26] C. Cheng, S. Sangodoyin, L. N. Nguyen, M. Prvulovic and A. Zajić, "Digital Electronics as RFID Tags: Impedance Estimation and Propagation Characterization at 26.5 GHz and 300 GHz," in IEEE Journal of Radio Frequency Identification.

[27] S. Adibelli, P. Juyal, C. Cheng and A. Zajic, "Terahertz Near-Field Focusing Using a 3-D Printed Cassegrain Configuration for Backscattered Side-Channel Detection," in IEEE Transactions on Antennas and Propagation, Oct. 2019.

[28] S. Adibelli, C. Cheng, P. Juyal and A. Zajic, "An Investigation of THz Backscattered Side-Channels Measurement at a Distance," 2019 13th European Conference on Antennas and Propagation (EuCAP), Krakow, Poland, 2019, pp. 1-5.

[29] Virginia Diodes, Horn Specifications. [Online]. Available: https://www.vadiodes.com/images/AppNotes/VDI_Feedhorn_Summary_2020.05.04.pdf.

[30] (2020). Zaber. [Online]. Available:https://www.zaber.com/products/linear-stages/X-LSQ-E/details/X-LSQ150A-E01/documents.

[31] [Online]. Available: https://www.ultra-herley.com/uploads/herley/datasheets/cti/Ultra%20Herley%20Series% 20PDRO.pdf.