An Investigation of THz Backscattered Side-Channels Measurement at a Distance

Sinan Adibelli, Chia-Lin Cheng, Prateek Juyal, Alenka Zajic
School of Electrical and Computer Engineering. Georgia Institute of Technology, Atlanta, GA, USA

***Abstract*— This paper presents the measurement setup and the investigation on the backscatter side-channel signal detected and received, at 300Ghz, from the activated FPGA board. First, the ellipsoidal reflector, used as an incident source, with a spot size of 0.7mm is designed and fabricated. Next, a region on the FPGA chip is divided geometrically into various cells with cell dimensions corresponding to reflector spot size. Finally, it was shown that the backscatter side-channel signal can be detected by a diagonal horn antenna placed at a distance from the FPGA board. The received signal behavior is investigated in terms of absolute signal strength, measured noise power level and signal to noise ratio. This provides deeper insight into the detected backscatter side-channel emanating for the FPGA board.**

***Index Terms*— EM side channel, Near field focusing, THz Signals, Ellipsoidal Reflectors**

I. Introduction

Side-channel based on backscattered signal created by switching activity of transistors have been reported in [1]. When transistors in digital circuits switch between the high and low states, the impedances connected to wires within an IC change, which creates backscatter signals from the IC. Earlier work on backscatter-based side-channel has focused on lower frequency range [1], while higher frequencies, e.g., THz, have not been investigated yet.

We presented in [2] that the THz near field focusing can be used to detect backscatter side-channels emanating from the processor activity in the board. For this, a 3-D printed cassegrain reflector configuration, operating at 300 GHz, having the near field directivity of 46 dBi, was designed to get the near field focus at 28 cm away from the reflector aperture. The designed reflector was used in the measurements and it was observed that the backscatter side-channels could be detected 28 cm away from the board, with the enhancement in the detected power of the side-channel signal. The designed antenna in [2] has the focal width and depth of 4 mm and 10 cm respectively. To develop deeper physical insight in understanding of the backscatter side-channel radiation mechanism and to locate the source position or region on the chip, a better spatial resolution or more focused spot beam is required.

One method to do this is to use the high resolution (~ 1mm) near field probes for the incident beam. At lower frequencies, near field probes are generally used to study the radiation emanating from the various PCB boards and interconnect lines. In those measurement setups, the probes are used as the receiving near field antenna that is connected to spectrum analyzer. In backscatter measurements setup both incident and receiving probes should be placed in the close vicinity to the chip surface, which is usually not convenient for the commercially available probes and can result in high coupling between the probes. This is also not beneficial for the practical security applications, for instance Trojan detection in FPGA boards.

For the detection of the backscattered side-channel at a distance, and to investigate the propagation mechanisms that govern this side-channel, this paper presents a measurement setup at THz frequencies. The region on the chip, which is under investigation, has the dimension of 5x5mm. This region was further divided geometrically into various rectangular cells, the dimensions of which are decided by the incident spot beam width of the focuser. In the measurements, the incident beam of spot size 0.7 mm, at 300GHz, was focused on each cell and the corresponding emanated fields from the board, by the backscatter side-channel signal were measured by using diagonal horn antenna. The detected measured signal power, spatial variation of the radiated electric field, the SNR and the measured noise levels are studied and discussed.

The rest of the paper is organized as follows. Section II describes the measurement scenario, chip dimensions and the region of investigation. Section III presents the design of the ellipsoidal reflector. Section IV discusses the backscattered side-channel measurement results, which includes measured power levels, noise floor and SNR. Finally, Section VI concludes the paper.

II. Backscattered side-channel measurement scenario

In this section, the measurement region on the chip and its division into various cells is discussed. Fig. 1 (a) and (b) show the picture of the Terasic DEO-CV board and the Altera cyclone V FPGA chip respectively. The chip dimensions is 2.5 cm and the selected middle square region has a dimension 5 mm, as shown in Fig. 1 (b), which is the region of investigation. The square region is further geometrically divided into cells of dimensions 0.5 mm by 0.5 mm as shown in Fig. 2. As explained

This work has been supported, in part, by NSF grants 1651273 and 1740962 and ONR grant N00014-17-1-2540. 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

later in Section IV, the incident beam is focused on each of these cells and the corresponding backscatter side-channel signal is measured.

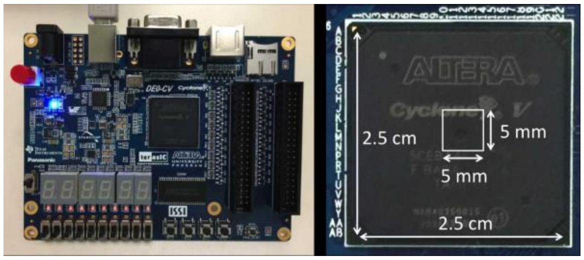

Fig. 1 (a) Terasic DE0-CV board (b) Altera Cyclone V chip.

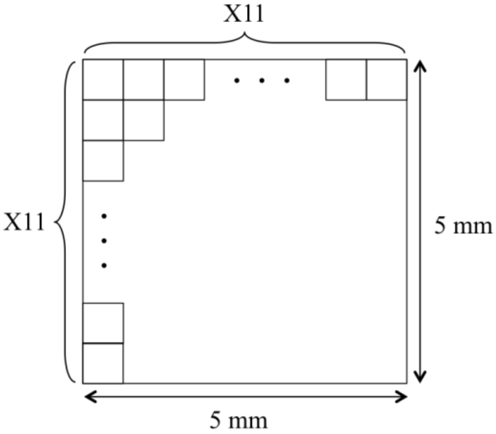

Fig. 2 Selected region of the chip divided into cells.

III. Ellipsoidal reflector Design

To focus the incident beam, ellipsoidal reflector has been designed. This section presents the parameters and constraints of the reflector design. The primary considerations are the focus size (resolution) and focus intensity. Focus size needs to be small enough to resolve variation in the signal levels emanating from the FPGA and the focus intensity needs to be high enough to detect these inherently weak signals. Based on the required focal spot size, the initial geometrical parameters of the ellipsoid was selected. The diffraction-limited resolution can be derived by modifying Abbe's criterion as shown in [3]. In the transverse direction (xy-plane), the resolution can be approximated by [4]

$$\Delta y \approx \frac{0.82\,\lambda}{\sqrt{2}\,\mathrm{NA}} \tag{1}$$

where λ is the wavelength and NA is the numerical aperture. The resolution in the axial direction (z-axis) can be approximated as

$$\Delta z \approx \frac{4.4\,\lambda}{2\pi\,(\mathrm{NA})^2} \tag{2}$$

To achieve the desired focus at 300 GHz, an ellipsoidal main reflector with a hyperboloidal subreflector fed by a 25 dBi diagonal horn, was designed and simulated. Simulation has been done in CST version 2017. A CST model is shown in the Fig. 3.

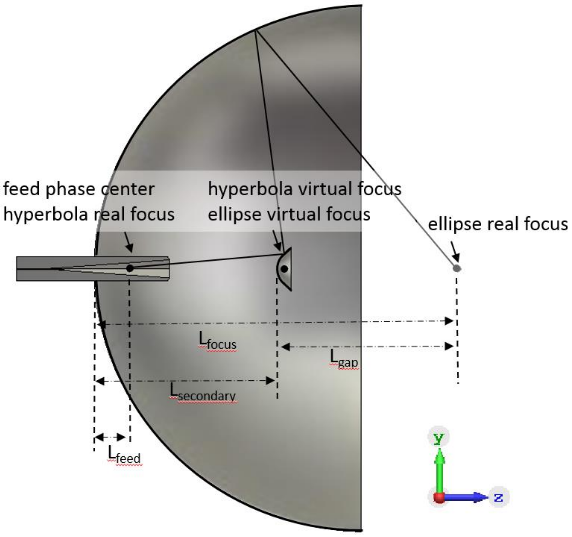

Fig. 3 The nearfield focuser CST model.

Table I Design parameters for the focused ellipsoidal reflector shown in Fig. 3

D_m	190 mm	Main reflector diameter
a_m	100 mm	Main reflector - ellipse parameter
b_m	95mm	Main reflector - ellipse parameter
L_{depth}	96mm	Main reflector depth
D_s	16 mm	Secondary reflector diameter
a_s	25 mm	Secondary reflector - hyperbola parameter
b_s	12 mm	Secondary reflector - hyperbola parameter
L_{feed}	13.3 mm	Feed point offset wrt. main reflector vertex
$L_{secondary}$	45.95	Distance between the vertices of the main and the secondary reflectors
L_{focus}	131	Distance between main reflector vertex and the focus
L_{gap}	35	Separation between the aperture of the main reflector and the focus

$$\frac{z^2}{a_m^2} + \frac{y^2}{b_m^2} = 1 \tag{3}$$

$$\frac{z^2}{a_s^2} - \frac{y^2}{b_s^2} = 1 \tag{4}$$

Equation (3) describes the elliptical profile of the main reflector and (4) describes the hyperbolic profile of the secondary reflector. The numerical values and the descriptions of the parameters used in this design are shown in Table I.

Fig. 4 shows the 2-D relative power density plot in yz-plane. The primary reflector is fed by the hyperboloid sub-reflector, which is in turn directly fed by the feed horn. The wave fronts converges at the desired focal spot. The wave front diverges quickly beyond the focal plane, as shown in Fig. 4, which is desirable. Fig. 5 show the power density in the focus spot region highlighted by the circle in Fig. 4. The simulated full width at half maximum (FWHM) values of the focus are 1.5mm for Δz (focus depth) and 0.7mm for Δy (focus width) which are within 10% of the theoretical formulas given in (1) and (2). The 3dB and 10dB contour lines of the focus is also indicated in Fig. 3.

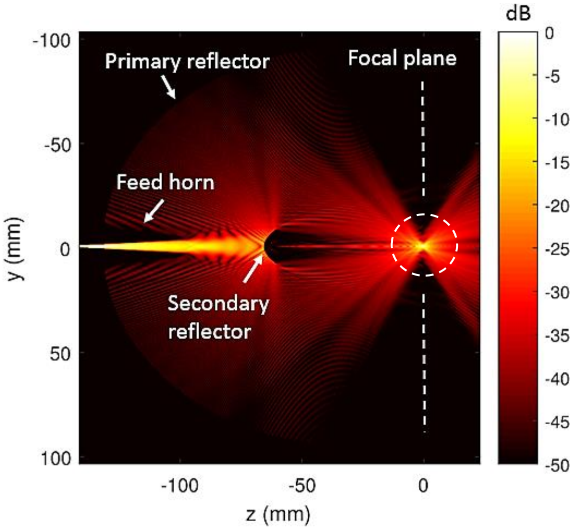

Fig. 4 2D Relative power density plot of the reflector model shown in Fig. 3

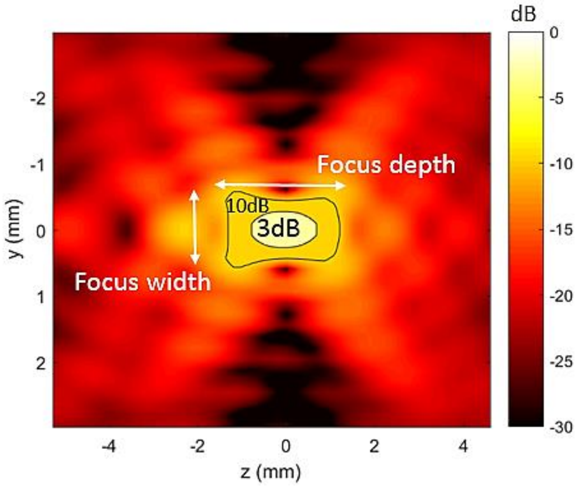

Fig. 5 2D Relative power density plot on the focal spot region

IV. Backscatter Side-Channel measurements

The simulation model shown in Fig. 3 was fabricated. The geometrical parameters for the fabrication have been listed in Table I. The main reflector is carved out of an aluminum block using a CNC lathe, the subreflector and the struts holding it are 3D-printed. The fabricated prototype is shown in Fig. 6. The diagonal feedhorn has a directivity of 25dBi and is a part of the Rx-Tx system. The measurement were done using a custom built 300GHz Virginia Diodes Tx-271 and Rx-159, pointed in Fig. 7, a more detailed overview of the components can be found in [5]. A diagonal horn antenna is used to receive the backscatter side-channel signal. The FPGA was positioned at the focal point of the fabricated reflector at an angle of 45° as shown in Fig. 7. The FPGA was shifted with a step of 0.5mm to scan a 5mm by 5mm area on the chip using the focuser. A 2D heatmap of the measured backscattered side-channel signal strength is overlaid on a picture of the FPGA package shown in Fig. 8. The received signal is investigated further in terms of absolute signal strength, noise floor levels and SNR within the cells region mentioned in Fig. 2. Fig. 9 (a)-(j), shows the received signal absolute power levels when the beam is incident on the horizontal row as described in Fig. 2.

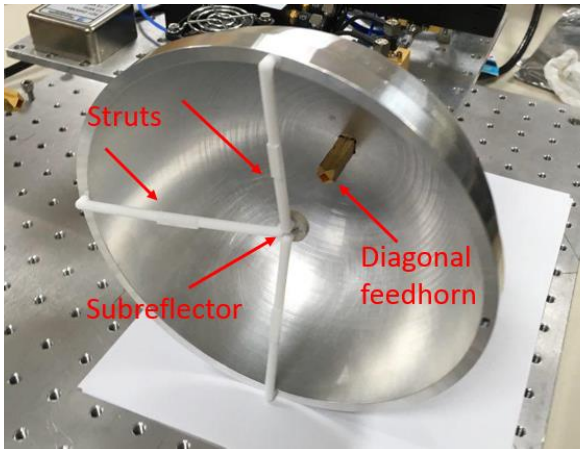

Fig. 6 The fabricated prototype of the model shown in Fig. 3

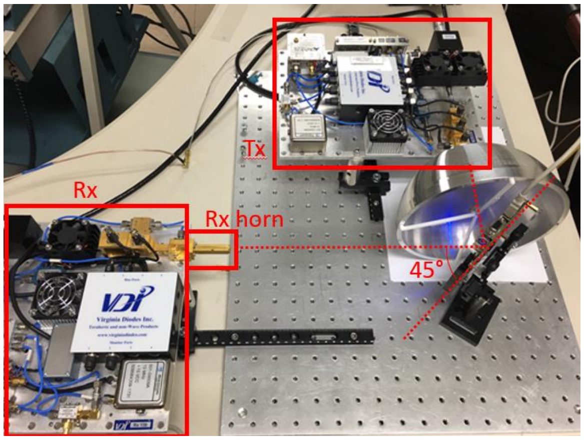

Fig. 7 The backscattered side-channel measurement setup

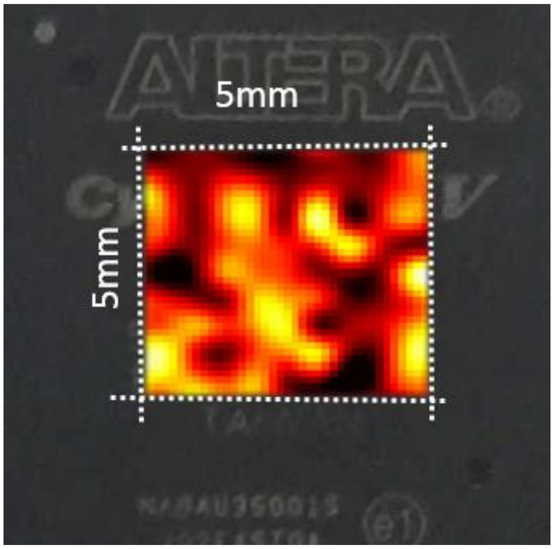

Fig. 8 Received backscatter sidechannel signal heat map on the selected chip region

The maximum received signal power measured in the entire region is -123dBm with a noise floor of -148dBm. The minimum received signal amplitude is 19dB below the maximum.

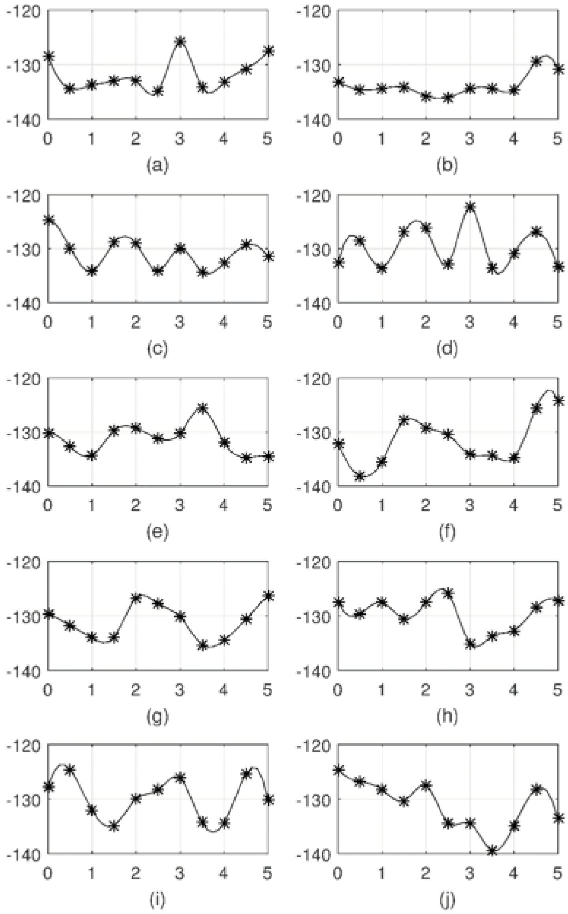

Fig. 9 (a)-(j) Measured absolute power levels of the scanned rows shown in Fig. 2.

The measured noise floor levels are plotted in Fig. 10. It is observed that for most of the part in the region the noise floor is at level of -137 dBm. However, in some cells the noise level is reduced by 5-10 dB.

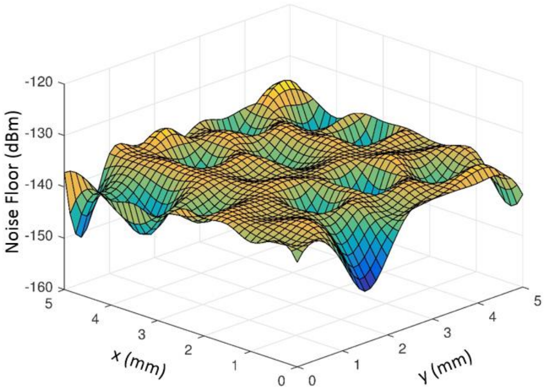

Fig. 10 Noise floor level represented as a surface plot

The SNR values for each cell in the measured region is shown in Table II. The median for the SNR values is around 8 dB. The maximum SNR level measured is 25dB, which is in the location of minimum noise floor.

Table II Measured SNR values in grid form

11.3	2.6	8.9	16.9	11.8	2.6	10.7	2.4	3.4	5.9	14.4
3.8	2.6	2.3	8.3	2.7	2.9	2.5	2.4	2.5	7.1	12.5
14.1	6.8	2.8	9.1	8.8	2.7	9.0	2.7	9.1	9.7	5.1
3.0	7.3	3.0	10.5	16.6	3.2	25.2	2.7	4.7	8.7	2.5
6.9	4.0	2.4	7.1	7.8	5.8	8.4	11.3	4.7	2.8	2.9
4.5	2.7	3.5	8.9	8.1	7.2	3.7	2.5	2.5	11.5	12.5
10.4	6.7	2.7	2.7	11.1	8.8	10.0	2.3	2.5	13.9	10.5
11.4	15.5	9.9	6.1	9.3	11.0	5.7	3.0	4.7	8.2	9.3
12.0	18.1	4.9	2.4	13.0	8.7	10.5	2.5	2.8	19.3	9.0
12.8	13.4	8.5	6.4	9.1	2.6	2.7	3.2	2.8	8.5	3.3
12.1	21.0	9.3	4.5	5.5	9.2	8.6	12.2	2.4	5.0	9.9

V. Conclusion

An investigation on the backscattered side-channel signal detection, emanating from an FPGA, measured at a distance, at 300 GHz was presented in this paper. To study the variation in the detected signal within a 1mm step, an ellipsoidal reflector was designed, fabricated, and used as an incident source in the backscatter side channel measurements setup. Measured side channel signal level were analyzed in terms of absolute signal power, noise floor and SNR. It was found that the maximum side channel power is 19 dB above the minimum measured power level, which is caused by the periodically switching the gates.

A potential application of the presented method is that different regions of a chip or a board could be performing different activities, which can give off different information about the periodic activity of FPGA.

References

[1] 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.

[2] P. Juyal, S. Adibelli, and A. Zajic, “THz near field focusing using Cassegranian configuration for EM side-channel detection,” *Proceedings of 2018 IEEE AP-S Symposium on Antennas and Propagation and URSI CNC/USNC*, Boston, USA, July 8-13, 2018.

[3] C.-B. Juang, L. Finzi, and C. J. Bustamante, “Design and application of a computer-controlled confocal scanning differential polarization microscope,” *Rev. Sci. Instrum.*, vol. 59, no. 11, pp. 2399–2408, 1988.

[4] C. Ciano et al., "Confocal Imaging at 0.3 THz With Depth Resolution of a Painted Wood Artwork for the Identification of Buried Thin Metal Foils," in *IEEE Transactions on Terahertz Science and Technology*, vol. 8, no. 4, pp. 390-396, July 2018.

[5] S. Kim and A. G. Zajić, "Statistical Characterization of 300-GHz Propagation on a Desktop," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3330-3338, Aug. 2015.