ISSN (Print) 1226-1750
ISSN (Online) 2233-6656
Journal of Magnetics 23(2), 207-213 (2018) https://doi.org/10.4283/JMAG.2018.23.2.207

Design of High Resolution Magnetic Probe for Magnetic Field Measurement on AES Cryptographic FPGA to Analyze the Side Channel Attack

S. Jegadeesan[1]*, M. Dhamodaran[1], M. Azees[2], and S. Sri Shanmugapriya[2]

[1]M. Kumarasamy College of Engineering, Karur, Tamilnadu, India
[2]V.S.B. Engineering College, Karur, Tamilnadu, India

(Received 22 March 2018, Received in final form 18 June 2018, Accepted 20 June 2018)

In this paper, a high resolution magnetic measurements are performed in an AES (advanced encryption standard) cryptographic FPGA by using a newly designed magnetic probe. The probe consists of high resolution scanning system and magnetic field collecting coil integrated with 3-stage low noise amplifier to enhance the sensed voltage. Also, to improve the performance of the magnetic coil, the Si-substrate is removed under the coil by using FIB process. The results and discussion section clearly shows that, the proposed magnetic probe gives more detailed information about the susceptible area of an AES cryptographic FPGA surface with high resolution maps in different frequency bands compared with the existing magnetic probe.

Keywords : Cryptographic FPGA, magnetic flux leakage, magnetic field collecting coil, high resolution magnetic map

1. Introduction

Information stored in cryptographic FPGA (field programmable gate array) is disclosed by continuous monitoring of information leakage such as power leakage and electromagnetic field leakage; this is known as side channel attack. The electromagnetic field sensing method is more suitable than the analysis of the power consumption approach [1]. The electromagnetic field sensing method is used to predict the vulnerable areas to attack and it finds the direction of magnetic flux leakage in the LSI (large scale integration) chips. In the LSI circuits, CMOS gates produce on-chip currents based on the changes in the clock signal or data given to the CMOS gate [2, 3]. These changes in the on-chip current produce a magnetic field around the conductors. The Sensor is placed nearer to the LSI chip surface to monitor and measure the magnetic field leakage depends on stored data. Through the measurement of magnetic field leakage, leakage of secret information is detected. In order to avoid the side channel attack, it is necessary to find the technique for detecting the vulnerable area of cryptographic LSI chips [4-6].

In previous works, leakage of magnetic field from the LSI chip is detected by a magnetic coil integrated with the low noise amplifier probe. The existing magnetic probe consists of a metal probe holder and size of magnetic coil is very small. Also, the output of this probe is affected by eddy currents [7, 8]. Therefore, to detect detailed information from the magnetic field leakage, it should be captured with high sensitivity and wide range of frequency. To overcome the above problem, a new magnetic field probe is designed to analyze the magnetic field of advanced encryption standard cryptographic FPGA [9-12]. The magnetic field probe is designed with magnetic field collecting coil with a plastic probe holder. To obtain the detailed information from the detected magnetic field, the detected signal is processed by using image processing [13-16].

The remaining content of this research work is organized as follows, design and implementation of the new magnetic probe are presented in section 2, results and discussion of the proposed magnetic probe are described in section 3 and conclusion of the proposed work is discussed in section 4.

*Corresponding author: Tel: +91-9786800357
Fax: 04324-272457, e-mail: jegadeesans@rediffmail.com

2. Magnetic Probe Description and Fabrication

2.1. A three stage low noise amplifier with magnetic field collector coil design

The proposed magnetic field measurement system shown in Fig. 1, the new magnetic probe consists of on-chip low noise amplifier included into a chip by a 0.21 µm CMOS process and magnetic field collector coil with a size of 400 µm × 100 µm, which is used to collect the magnetic field from the LSI chip based on the relationship between magnetic flux density, inductance coil voltage and also depends on Faradays induction law. The proposed magnetic probe is used to measure the magnetic field over the cryptographic FPGA. The measured signal is stored in a matrix format to detect the vulnerable location in the cryptographic FPGA. During the measurement the sensing angle between the probe and chip is 90 degrees, the gap between the probe and chip is less than 100 µm. Comparison of the proposed magnetic probe with conventional probe is shown in Table 1.

The coil voltage V_I depends on the number of turns in the coil and changes in the magnetic flux density with respect to time. Therefore, the coil voltage is given as,

$$V_I = -N\frac{d\Phi_B}{dt} \tag{1}$$

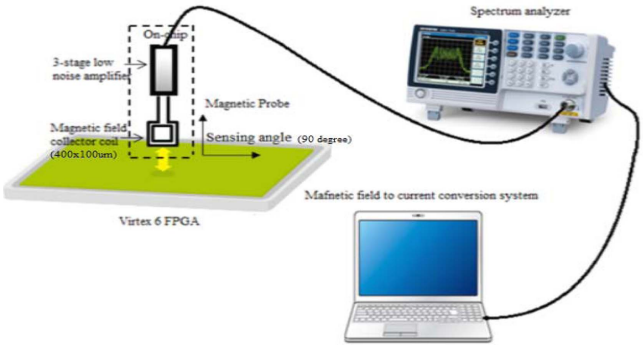

Fig. 1. (Color online) Proposed system model for magnetic field measurement.

The current flow through the wire in the coil produces the magnetic flux

$$\Phi_B = \frac{\mu_o I}{2\pi} X \ln\frac{r+Y}{r}. \tag{2}$$

Therefore, the coil voltage V_I can be written as,

$$V_I = -N\frac{\mu_o}{2\pi}\ln\frac{r+Y}{r}\frac{dI}{dt} \tag{3}$$

Where μ_o - is vacuum permeability.

If the current $I = I_o \sin(2\pi ft)$, then the probe coil voltage V_I becomes,

$$V_I = -N\mu_o X \ln\frac{r+Y}{r} I_o f \cos(2\pi ft) \tag{4}$$

The voltage V_I can be improved by increasing the parameter N and X. Therefore, the proposed magnetic probe consists of a bigger size coil with 5 turns, it is shown in Fig. 2(b) and it is integrated with three stage low noise amplifier. This setup permits more magnetic flux flow through the coil and the size of the coil is very bigger than the existing magnetic probe coils. Also, the Si-substrate of the coil is removed from the coil by using a FIB (focused ion beam) process to improve the coil performance and to avoid the eddy current plastic probe

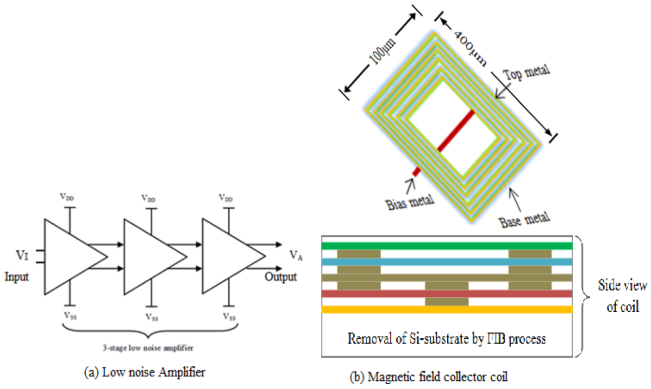

Fig. 2. (Color online) 3-stage low noise amplifier and magnetic field collector coil.

Table 1. Comparison of proposed probe with conventional probe.

S.No.	Conventional magnetic probe	Proposed magnetic probe
1	Probe system affected by eddy currents	To avoid eddy current effect, the magnetic probe is built with plastic probe holder
2	Magnetic probe coil size is very minimum	To acquire more information, the size of the coil is increased (400 µm × 100 µm).
3	The probe must have a wide frequency range	Wide frequency range not required for the proposed probe
4	High sensitivity required to detect the harmonic signals from cryptographic FPGA	Si-substrate area under the coil is removed by using a FIB process to improve the coil performance. High resolution magnetic scanning measurements performed in cryptographic FPGA.
5	Low resolution magnetic map	Producing high resolution magnetic map to detect the vulnerable part in the cryptographic FPGA

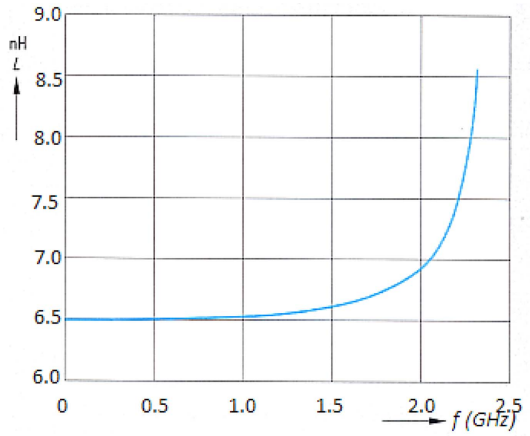

Fig. 3. (Color online) Inductance of magnetic field collector coil.

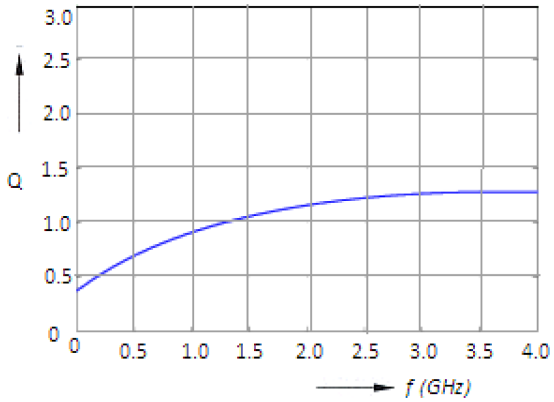

Fig. 4. (Color online) Quality factor of magnetic field collector coil.

holder is used. Simulated result of coil inductance and quality factor are shown in Fig. 3 and 4 respectively.

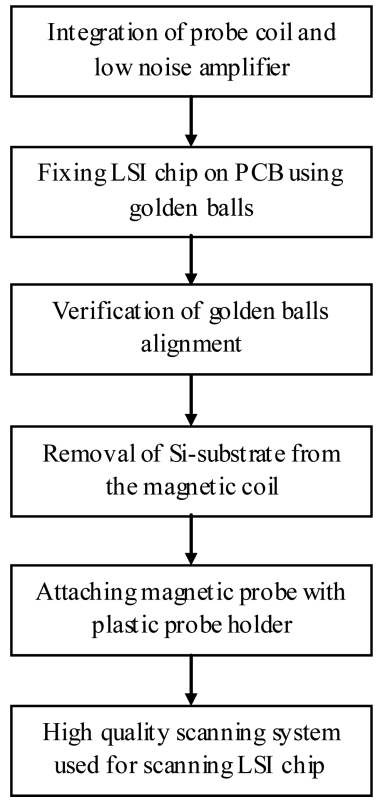

Fig. 5. Magnetic probe fabrication steps.

2.2. Probe fabrication steps

Probe fabrication steps are shown Fig. 5. First, the inductance coil and low noise amplifiers are integrated by 0.21 μm CMOS process. Second, the chip is turned and fixed in the PCB (printed circuit board) by using golden balls. Third, to correct and confirm the alignment of golden balls with the corresponding PCB, an X-ray photograph is used. Fourth, the Si-substrate under the coil is removed

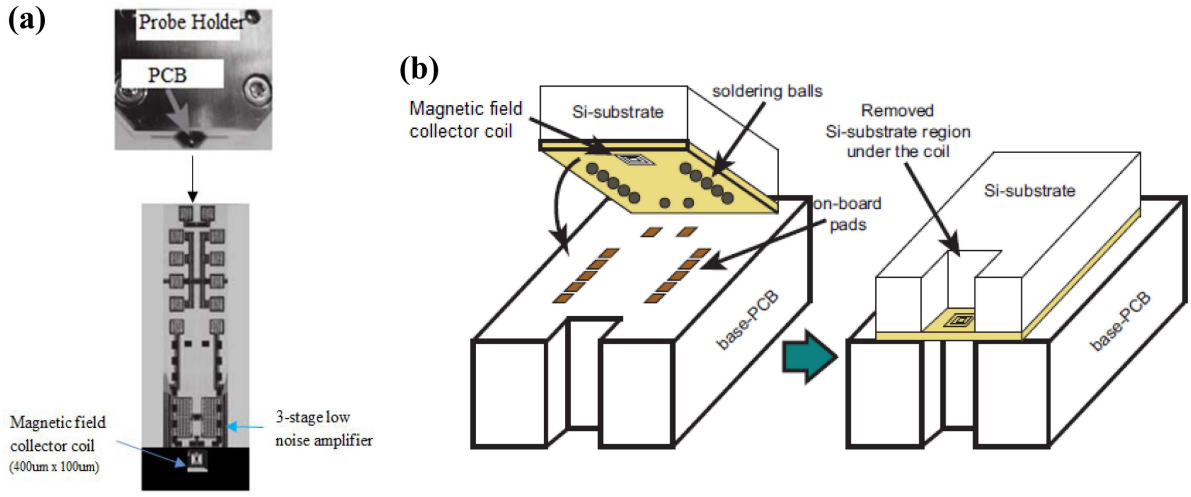

Fig. 6. (Color online) (a) On-chip coil and 3-stage low noise amplifier. (b) Post processing: Si-substrate removal under the coil.

by using FIB process. Fifth, the proposed magnetic probe is attached with plastic holder instead of metal to avoid the eddy currents, noise and also to improve the magnetic probe performance. Sixth, the high quality scanning equipment is used to capture the shielded box to perform calibration and scanning process done automatically to map the magnetic noise. The proposed magnetic probe and Si-substrate removal under the coil are shown in Fig. 6(a) and 6(b) respectively.

3. Results and Discussion

The proposed magnetic probe performs two types of measurement. First, gain values between the micro strip line and magnetic probe for different lift-off distance, d is measured. For calculating this measurement, one end of the micro strip line is terminated with 50 Ω resister, micro strip line and magnetic probe should be placed at 90 degrees and other end of micro strip line and magnetic probe output connected to port 1 and 2 of the network analyzer respectively. Gain values between proposed magnetic probe and the micro strip line for the different liftoff distance, d is measured from 100 μm to 2500 μm, it is shown in Fig. 7 and 8(a). From the Fig. 8(a), it is clear that, the gain values are increased when the frequency range is from 10 MHz to 310 MHz.

To collect more magnetic flux density of the micro strip line, the proposed magnetic probe aligned 90 degrees with the micro strip line during the scanning process. A laser signal is used to scan the surface of the micro strip line and it uses 10 μm thickness with perpendicular to micro strip line. The magnetic strength of the micro strip line is measured at different frequencies. Fig. 8(b) shows the micro strip line magnetic strength at 100 MHz, 150 MHz, 200 MHz and 250 MHz frequency values. The output of the new magnetic probe is measured in spectrum

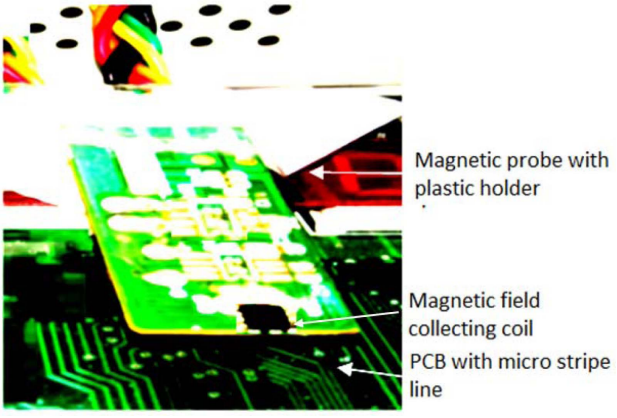

Fig. 7. (Color online) Magnetic probe with micro strip line.

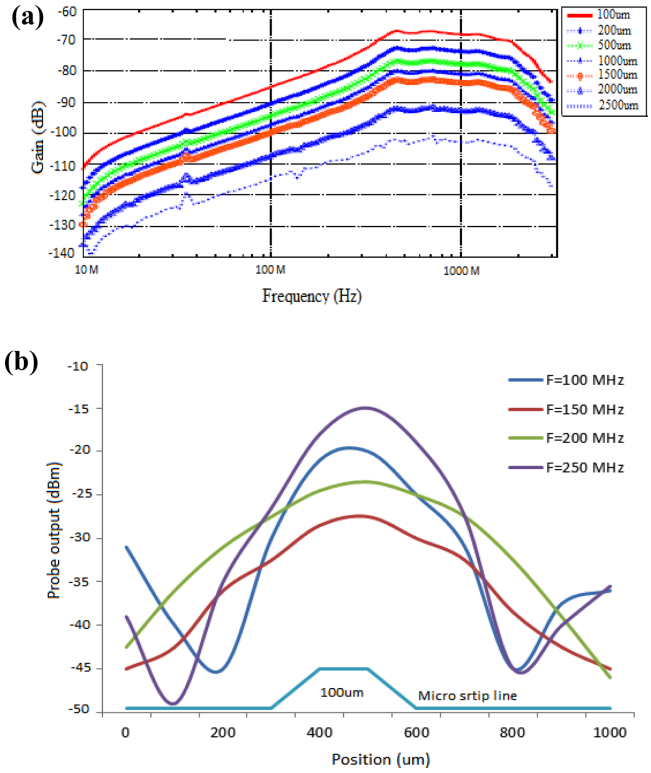

Fig. 8. (Color online) (a) Magnetic probe gain value for different frequencies. (b) Magnetic probe output for different frequencies.

analyzer. The output of the proposed magnetic probe gives 15 dB more gain compared with the existing magnetic probe.

Next, measure the magnetic field mapping of a Virtex-6 FPGA with a clock frequency of 20 MHz. To improve the performance of the proposed magnetic probe, the cooling cover is removed from the FPGA to permit the laser and magnetic probe to do better scanning. First, laser scans the surface of the FPGA and marks the edges, and then the video camera is used to take ridge map to perform the magnetic scanning with same lift-off value for all the scanning points. The magnetic probe output is connected to a spectrum analyzer and the spectrum analyzer output is given to a monitoring system to perform real time data filtering with a possible range of frequencies for the customized computer based program. The scanning process done in both horizontal and vertical axis with 50 μm resolution, 100 μm liftoff distances between the magnetic probe coil and the FPGA surface. To achieve high resolution, the Si-substrate under the coil is removed and also high resolution scanning system is used, it is shown in Fig. 9.

The resolution refers to the number of pixels (dots) per inch (DPI). If an image contains 800-by-600 pixels and

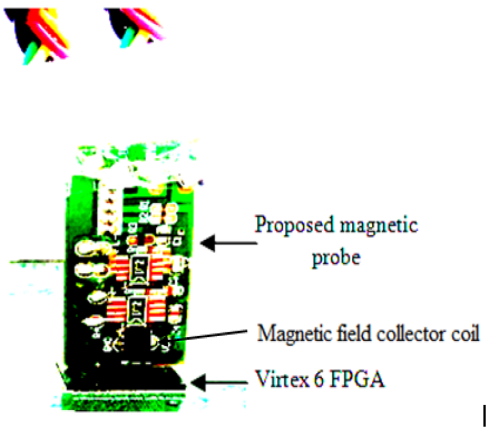

Fig. 9. (Color online) Scanning of FPGA surface using magnetic probe.

has a size of 4-by-3 inches, then the resolution is 800 pixel / 4 inches = 200 DPI. Generally, higher resolution allows you to print or zoom up images to larger sizes without losing quality.

For electromagnetic analysis, AES cryptographic FPGA is considered. There are four steps involved in AES encryption 1) substitute bytes, 2) shift rows, 3) mix columns and 4) add round key. The substitution bytes step uses S - boxes to perform a byte-by-byte substitution of the block. That is, S-box is the basic element in the substitution process. In FPGA's, S-box 1 is intentionally mapped away from the other S-boxes in the AES circuits for analyzing the performance of the proposed magnetic probe in terms of resolution for identifying suspicious or abnormal area in the cryptographic LSI chips. Also, one additional bit is added with S-box 1 to independently run/stop.

Initially, the MT-545 probe was used to scan AES cryptographic FPGA surface for doing magnetic noise mapping. Figure 10 shows the MT-545 probe magnetic maps of running S-box 1, stopping S-box 1 and the difference between the previous two magnetic maps. An image processing technique is used to get the differential maps between the running S-box 1 and stopping S-box 1 maps.

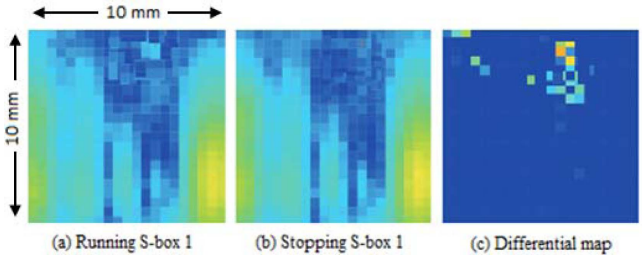

Fig. 10. (Color online) Scanning of FPGA surface by the MT-545 magnetic probe.

A similar setup is used to scan the AES cryptographic FPGA surface by using a proposed magnetic probe. To obtain the magnetic maps in a broad range frequency, the surface of the FPGA is scanned by a proposed magnetic probe with a lift-off distance of 100 μm. Figure 11(a) shows the magnetic maps of AES cryptographic FPGA surface scanned by proposed magnetic probe during the running of S-box 1 at 60 MHz. Figure 11(b) shows the magnetic maps during running S-box 1, stopping S-box 1 and the difference between the previous two magnetic maps for different range of frequencies.

In the differential magnetic maps, during the frequency range from 10 MHz to 300 MHz, the LSI chip discloses nothing, shown in the Fig. 11(a). On the other hand, during the frequency 40 MHz, 60 MHz and 80 MHz, that is at the harmonic frequency of 20 MHz, there is a some

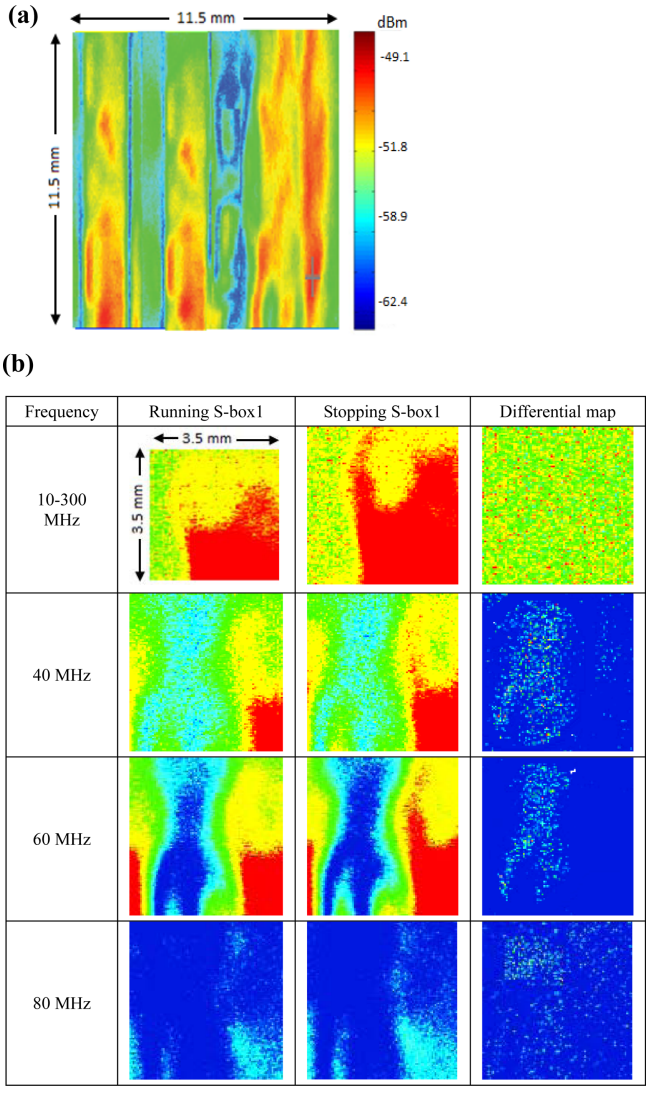

Fig. 11. (Color online) (a) Scanned magnetic map of FPGA surface. (b) Scanning of S-box 1 at running/stopping of S-box 1.

Table 2. Performance analysis of proposed magnetic probe.

Method	Probe fabrication process	Size of the coil	Integration of low noise amplifier	Scanning process	Output image resolution
E. Peeter's scheme	Loop probe – hand made	700 μm	No	No	Not applicable
K. Chen's scheme	Solenoid probe – hand made	300 μm	No	No	Not applicable
M. Yamaguchi's scheme	CMOS process – 0.13 μm	180 × 180 μm^2	No	No	170 μm
N. N. Mai-Khanh's scheme	CMOS process – 0.18 μm	500 × 100 μm^2	Yes	Yes	120 μm
Y. Shigeta's scheme	CMOS process – 0.18 μm	100 × 50 μm^2	Yes	Yes	40 μm
S. Muroga's scheme	CMOS process – 0.18 μm	60 × 60 μm^2	No	Yes	10 μm
Proposed scheme	CMOS process – 0.21 μm	400 × 100 μm^2 – Si-substrate under the coil is removed	Yes	Yes	20 μm

stripe in the top-right corner of differential magnetic maps which is due to the function of the S-box 1. From the differential magnetic maps, the proposed system easily detects the intentionally mapped S-box 1 area which is present in the rightmost column at a harmonic frequency of 20 MHz.

Figure 11(b) presents the magnetic maps of AES cryptographic FPGA surface at 60 MHz during the running of S-box 1. The top-right corner shows the susceptible area in the AES cryptographic FPGA that is intentionally mapped S-box 1 area. By comparing Fig. 10(c) with Fig. 11(b), the proposed magnetic probe gives detailed information with higher resolution about the susceptible area than the conventional MT-545 probe. The measured results explain the ability of the proposed magnetic probe that is identifying suspicious areas in the cryptographic LSI chips with high resolution. A comparison with other works [17-19] are given as in Table 2.

In the proposed work, magnetic coil and 3-stage low-noise amplifiers are integrated. But, the other schemes used only off-chip amplifier. Also, the proposed probe gives better resolution output than the existing methods. Conventional probe gives the output with gain of −52 dB, on the other hand, the proposed probe gives the output with gain of −37 dB. Also, to improve the performance of coil Si-substrate of the coil is removed.

4. Conclusion

A high resolution scanning of magnetic field on AES cryptographic FPGA is presented. High resolution is achieved by removing the Si-substrate under the coil in the proposed magnetic probe and by using high resolution scanning system with plastic probe holder. Magnetic field sensing was performed on AES cryptographic FPGA surface and 100 μm micro strip line. The measured results show that, the proposed magnetic probe gives 15 dB more gain than the existing magnetic probe. Also, the magnetic probe can be used to detect a vulnerable area on AES cryptographic FPGA surface with high resolution from the side channel attack than the conventional probe.

References

[1] F. Peeters, X. Standaert, and J. Quisquater, The VLSI Journal **40**, 1 (2007).
[2] Gao Junxia, Zhang Yiming, and Tian Jiashen, J. Magn. **22**, 1 (2017).
[3] K. Chen, Q. Zhao, P. Zhang, and G. Deng, International Conf. on Embedded Software and Systems Symposia (ISESS), (2008).
[4] N. N. Mai-Khanh, IEEE Sensors **14**, 2 (2012).
[5] C. K. Chandrana, J. A. Neal, D. Platts, B. Morgan, and P. Nath, J. Magn. Mater. **381**, 396 (2015).
[6] H. M. Liang, J. X. You, X. R. Ye, and G. F. Zhai, Trans. of China Electrotechnical Society **26**, 46 (2011).
[7] Yan Shi , Chao Zhang, Rui Li, Maolin Cai, and Guanwei Jia, Sensors **15**, 1 (2015).
[8] Mustafa Göktepe, Advances in Materials Science and Engineering **2013**, 1 (2013).
[9] Derac Son, Wonik Jung, Duck Gun Park, and Kwon Sang Ryu, IEEE Trans. Magn. **45**, 2724 (2009).
[10] M. Li and D. A. Lowther, IEEE Trans. Magn. **46**, 3221 (2010).
[11] Kenji Sakai, Koji Morita, YutaHaga, Toshihiko Kiwa, Katsumi Inoue, and Keiji T. Sukada, IEEE Trans. Magn. **51**, 11 (2015).
[12] D.-G. Park, M. B. Kishore, J. Y. Kim, L. J. Jacobs, and D. H. Lee, J. Magn. **21**, 57 (2016).
[13] X. Dai, Q. Liang, C. Ren, J. Cao, J. Mo, and S. Wang, J. Magn. **20**, 273 (2015).
[14] E. Peeters, F.-X. Standaert, and J.-J. Quisquater, Integr. VLSI J. **40**, 1 (2007).
[15] K. Chen, Q. Zhao, P. Zhang, and G. Deng, in Proc. Int. Conf. Embedded Softw. Syst. Symp. (2008).

[16] M. Yamaguchi, H. Toriduka, S. Kobayashi, T. Sugawara, N. Hommaa, A. Satoh, and T. Aoki, in Proc. IEEE Int. Symp. Electromagn. Compat. (2010).
[17] Nguyen Ngoc Mai-Khanh, Tetsuya Iizuka, Shigeru Nakajima, and Kunihiro Asada, IEEE Trans. Magn. **51**, 6500404 (2015).
[18] Y. Shigeta, N. Sato, K. Arai, M. Yamaguchi, and S. Kageyama. EMC'14/Tokyo, 14837838 (2014).
[19] Sho Muroga, Kaoru Arai, Sandeep Dhungana, Ryosuke Okuta, Yasushi Endo, and Masahiro Yamaguchi, IEEE Trans. Magn. **49**, 3886 (2013).