

Side Channel Analysis using giant magneto-resistive (GMR) sensors

Edgar Mateos, Catherine H. Gebotys
 Department of Electrical and Computer Engineering
 University of Waterloo
 200 University Avenue West
 Waterloo, Ontario, Canada N2L 3G1
 +1 519 888 4567
 emateoss@uwaterloo.ca, cgebotys@uwaterloo.ca

ABSTRACT

Giant magnetoresistors (GMR) are nanotechnology devices able to detect tiny magnetic fields. This paper proposes the use of these sensors to acquire electromagnetic (EM) signals and analyze them using correlation analysis in the time domain and frequency domain. The objective is to analyze the small electromagnetic emanations that the hardware implementation may unintentionally leak, and try to recover the secret keys used when the cryptographic computations are performed. This work compares the performance of a GMR probe with a common inductive loop EM probe. The results show the success of GMR sensors in retrieving the correct key in 8-bit systems even in a scenario where the inductive probe failed.

Keywords

Side channel Analysis, Correlation Analysis, Giant magnetoresistance, GMR.

1. INTRODUCTION

Over the past few years, electromagnetic analysis has consolidated as a strong methodology to attack software and hardware implementations of cryptographic algorithms. EM analysis has been studied with detail in works such as [1, 3, 10]. They have explored diverse probes from a variety of materials in their analysis; however, almost all of them are inductive probes. In a similar manner, publications like [4, 9, 15] used inductive probes. In this paper, a different type of probe is introduced which uses giant magnetoresistors (GMR) sensors. These sensors are based on the magnetoresistance quantum mechanical effect discovered in the late 1980s to detect small magnetic fields. Nowadays, these sensors are used in high density hard drives to read the magnetic information stored in the plates of the disk. In a similar way, this work proposes the use of these types of sensors to detect the small magnetic fields produced by cryptographic devices when they

perform cryptographic algorithms. This work compares the performance of a commercial inductive EM probe and a GMR probe when they acquire EM traces from an 8-bit processor-based system. This analysis includes different sampling rates to compare the capabilities of each probe under a variety of scenarios, including the case where the sampling frequency is almost twice the frequency of the clock system. The next section outlines the previous research in this field followed by a brief review of EM analysis and correlation analysis. Then the experimental results are presented followed by the conclusions.

2. PREVIOUS RESEARCH

Side channel attack is the process of obtaining additional information through unintentional channels from the internal activity of a physical device [12]. Electromagnetic power analysis is one technique used in side channel analysis to look for weaknesses in the algorithm implementations [1, 3, 10]. The main idea is to measure the EM emanations from an electronic device when it's encrypting or decrypting a plaintext/ciphertext using a secret key and later try to recover the key through analysing the recorded measurements. Differential Power Analysis (DPA) is a powerful type of side channel analysis, which was introduced by Kocher, Jaffe and Jun [6]. A similar approach to differential analysis is presented in [4] where an attack is launched in the frequency domain using EM signals. Correlation power analysis is a variation of DPA that uses the correlation factor between the power traces and the power consumption model to determine the level of association. This type of attack has been used against software and hardware implementations of cryptographic algorithms [2]. In [9, 13, 15] different attacks against AES are presented using correlation analysis in the frequency domain.

Unlike previous research, this paper presents results of EM analysis using a giant magnetoresistance (GMR) probe and these results are compared with the ones obtained using a 1 cm loop inductive EM probe.

The results show successful attacks on an 8-bit software implementation of AES using the GMR probe in some conditions where the inductive EM probe fails to return the correct key. The next section will review some fundamentals of EM analysis attacks including the physics of the inductive and GMR effects. It also includes a brief review of correlation analysis in the time and frequency domain.

3. EM ANALYSIS ATTACKS

EM analysis is an attack that uses EM emissions to obtain information about the information processed by the electronic device. It works similar to power analysis; the difference is that EM analysis uses EM signals instead of power signals. EM analysis is based on some principles of the EM theory that are briefly described below.

In the first place, Biot-Savart's law states that when an electrical current i_c moves through a straight conductor, at all points on a circle of radius r around that conductor, the magnitude of the magnetic field \vec{B} generated is given by (1), where μ_0 is the permeability of free space ($\mu_0=4\pi \times 10^{-7}$ Wb/A.m) [14].

$$B = \frac{\mu_0 i_c}{2\pi r} \quad (1)$$

In a more generic way the third equation of Maxwell's (2) refers to a similar phenomenon. It states that the magnetic field \vec{B} depends on the conduction current i_c and the displacement current $\epsilon_0 d\Phi_E/dt$, where ϵ_0 is the permittivity of free space ($\epsilon_0 \approx 8.85 \times 10^{-12}$ F/m) and $d\Phi_E/dt$, is the time rate of change of electric flux [14].

$$\oint \vec{B} \cdot d\vec{l} = \mu_0 \left(i_c + \epsilon_0 \frac{d\Phi_E}{dt} \right) \quad (2)$$

In this scenario, one might assume that when an electronic device is processing information, some currents are flowing inside the internal circuits and consequently producing magnetic fields.

Another principle exploited by EM analysis is Faraday's law (3), which states that the induced electromotive force ε in a closed loop equals the negative of the time rate of change of magnetic flux $d\Phi_B$ through the loop. Where $d\Phi_B$ equals the magnetic field \vec{B} for an infinitesimal area $d\vec{A}$ [14].

$$\varepsilon = - \frac{d\Phi_B}{dt} \quad (3)$$

In a similar way Maxwell's fourth equation (4) states that a changing magnetic flux $d\Phi_B$ induces an electric field \vec{E} [14].

$$\oint \vec{E} \cdot d\vec{l} = - \frac{d\Phi_B}{dt} \quad (4)$$

For this reason every time a coil is placed close to a magnetic field, it induces an electromotive force on the coil. Specifically placing a coil or an EM probe close to an electronic circuit that is processing data, might induce some voltages on the terminals of the probe that are correlated with the data processed by the circuit and consequently provide information about the data itself.

3.1 Giant Magnetoresistance (GMS) sensors

The magnetoresistance phenomenon was documented by Lord Kelvin in 1857. The giant magnetoresistance was discovered by Peter Grünberg and Albert Fert in the late 1980s and nowadays is widely used in the read head of hard disc drives [5, 7]. The word "giant" refers to the large change in resistance that is present in these devices (10% to 20%) when they are in the presence of a magnetic field.

Giant magnetoresistance sensors are nanotechnology devices that are able to change their resistance when they are exposed to a magnetic field. The basic structure of this device is two ferromagnetic metal films (such as Fe or Co or they alloys, etc.) separated by a metallic nonmagnetic film (such as Cu). The magnetic layers are thin (less than 10 nm) and the nonmagnetic layer is thinner [5].

In the absence of external magnetic fields the magnetic moment of the layers adjacent to the copper face different directions, this is due to the antiferromagnetic coupling of the built device. Normally copper is a good conductor however when it's a few atoms thick, electron scattering increases its resistance notoriously. This resistance depends on the relative orientation of the electrons spins next to the thin copper layer. When an external magnetic field is applied and the magnetic moments of the layers adjacent are aligned in the same direction, the resistance decreases [11].

3.2 Correlation EM analysis

In the case of EM correlation analysis, the correlation coefficient r is used to measure the relationship between the hypothetical power consumption model of the circuit and the measured EM signals when the circuit is processing a given data.

Correlation power analysis has been explained in different publications [2, 8, 9]. EM correlation analysis is similar, first it is necessary to acquire a set of EM traces T when the electronic device under study is encrypting/decrypting D different plaintexts/ciphertext C_d . Each trace T contains N samples. With them a matrix of measured EM traces is formed $T_d(j)$, $d=1, \dots, D$, $j=1, \dots, N$.

Then it is necessary to define an attack point in the algorithm implementation. This point must be a function of non-constant data and a small part of the secret key K_i . Next, a matrix of hypothetical values is created from the D plaintexts or ciphertext C_d , and all possible values of the small part of the secret key K_i . The hypothetical values matrix is mapped into a hypothetical power consumption matrix HP using a power consumption model. Frequently the power consumption model used for this is mapping is the Hamming distance or Hamming weight.

The sample Pearson correlation (5) can be used to determine the linear relationship (correlation) r between the measured EM traces $T_d(j)$ and the hypothetical power consumption $HP_{d,i}$. Where $d=1, \dots, D$, corresponds to the number of traces used in the analysis; $j=1, \dots, N$, corresponds to the j -th sample from a EM trace; $i=1, \dots, k$, corresponds to the i -th hypothetical value of the small part of the key K_i ; $\overline{T(j)}$ corresponds to the mean from all d traces $T_d(j)$, at the j -th sample; and $\overline{HP_i}$ corresponds to the average hypothetical power at the hypothetical i -th key guess.

$$r_{i,j} = \frac{D \sum_{d=1}^D (HP_{d,i} \cdot T_d(j)) - \sum_{d=1}^D (HP_{d,i}) \cdot \sum_{d=1}^D (T_d(j))}{\sqrt{D \sum_{d=1}^D (HP_{d,i} - \overline{HP_i})^2 \cdot D \sum_{d=1}^D (T_d(j) - \overline{T_d(j)})^2}} \quad (5)$$

Finally the absolute value of each element of the correlation matrix R is found. The row i that contains the maximum value from this matrix then most likely corresponds to the (small part of the secret key) K_i used for the encryption/decryption of the data.

3.3 Correlation in the frequency domain

Correlation analysis in the frequency is similar to correlation analysis in the time domain, but here the analysis focuses on determining the level of

association between the hypothetical power consumption model and the power spectrum from the measured EM signals. The correlation in the frequency domain works as follows [9]. First the power spectrum F_d is obtained from the traces $T_d(j)$, $j=1, \dots, N$, using the Fast Fourier Transform (FFT) as shown in equation 6.

$$F_d = |FFT(T_d)|^2 \quad (6)$$

In order to take advantage of the FFT algorithm the value of N should be a power of 2. Also considering the FFT transformation is symmetrical, it is possible to analyze only one-half of the frequencies. Thus, the size of F becomes D rows and $NFFT/2$ columns, where $j'=1, \dots, NFFT/2$.

The hypothetical power consumption model is obtained following the same steps as in the time domain. The correlation r between the hypothetical power consumption model and the power spectrum is calculated using equation 7. Equations 6 and 7 have the same structure, with the differences that (6) uses the EM traces $T_d(j)$ and is of size $[D \times N]$; while equation 7 utilize the power spectrum $F_d(j')$ and is of size $[D \times NFFT/2]$.

$$r_{i,j'} = \frac{D \sum_{d=1}^D (HP_{d,i} \cdot F_d(j')) - \sum_{d=1}^D (HP_{d,i}) \cdot \sum_{d=1}^D (F_d(j'))}{\sqrt{D \sum_{d=1}^D (HP_{d,i} - \overline{HP_i})^2 \cdot D \sum_{d=1}^D (F_d(j') - \overline{F_d(j')})^2}} \quad (7)$$

Each column from the correlation matrix R corresponds to one of the frequencies analysed and each row represents a possible key guess. The possible correct key is obtained by finding the row with the maximum absolute values from the matrix.

4. EXPERIMENTAL RESULTS

The microcontroller AT89C51ED2 within the Keil MCB251 evaluation board was used to analyze the performance of the GMR and inductive probes. The board uses a 24 MHz crystal. In consideration of the Nyquist-Shannon sampling theorem, the EM traces where captured using different resolutions above 2 times the clock frequency. The resolutions analyzed include 500 MS/s, 250 MS/s, 125 MS/s, and 50 MS/s. The probes used were the commercial 1cm loop EM probe and the GMR probe. The GMR probe uses the NVA AB001-02 sensor [11]. This sensor has a Wheatstone bridge configuration. The attack focus was the microcontroller processing one byte of the key at the first round of AES. For the cases of 500 MS/s, 250 MS/s, and 125 MS/s, the results were verified utilizing 10 sets of 2048 traces each. For the sampling rate of 50 MS/s, 50 sets of 2048 traces were used.

4.1 Correlation analysis in the time domain

In the case of correlation analysis in the time domain, different sets of traces captured using the inductive probe (EM Probe) and the GRM probe were analysed.

Table 1 presents the maximum values of the correlation matrix when the EM traces obtained with the inductive and GMR probe are analysed using correlation analysis in the time domain. In the table most of the correlation values for the inductive probe are larger than those for the GMR probe. However, in the case of the GMR probe the correct key was recovered in all the cases, even where the inductive probe failed in 39 of 50 experiments with a sampling resolution of 50 MS/s.

Table 1: Maximum correlation for the time domain analysis

Correlation analysis in the time domain		
Sampling frequency [MS/s]	EM probe	GMR probe
500	0.913	0.523
250	0.708	0.426
125	0.629	0.306
50	0.161*	0.212

* Able to recover the correct key in 11 of 50 experiments.

Next correlation vales for the extreme cases of 500 MS/s and 50 MS/s were explored. Figure 1 shows the values of the correlation matrix for the case of 500MS/s, using the EM probe and correlation analysis in the time domain. In this case, a clear spike appears at 7.35 μ s on the key guess 162. It's evident that it corresponds to the correct value of the key.

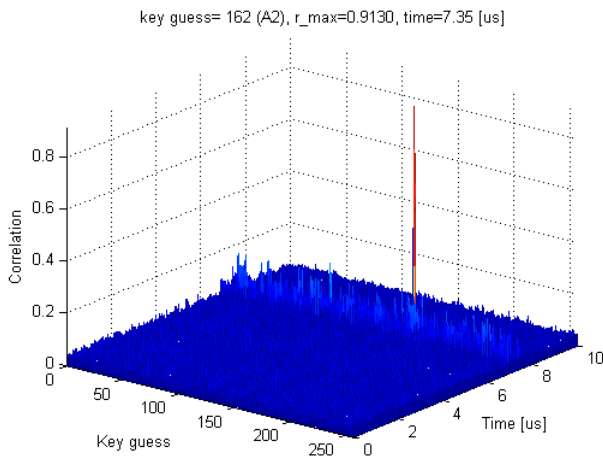


Figure 1: Correlation matrix in the time domain for 2048 traces using EM probe and sampling frequency of 500 MS/s.

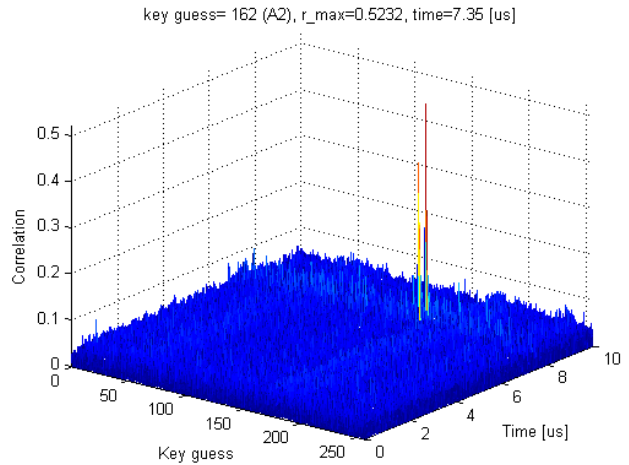


Figure 2: Correlation matrix in the time domain for 2048 traces using the GMR probe and sampling frequency of 500 MS/s.

Figure 2 illustrates the maximum correlation for the GMR probe using correlation analysis in the time domain. Similar to the inductive probe the maximum correlation of 0.523 occurs at 7.35 μ s. However, with the GMR probe a second spike is visible for the same correct key guess (162) at 7.032 μ s.

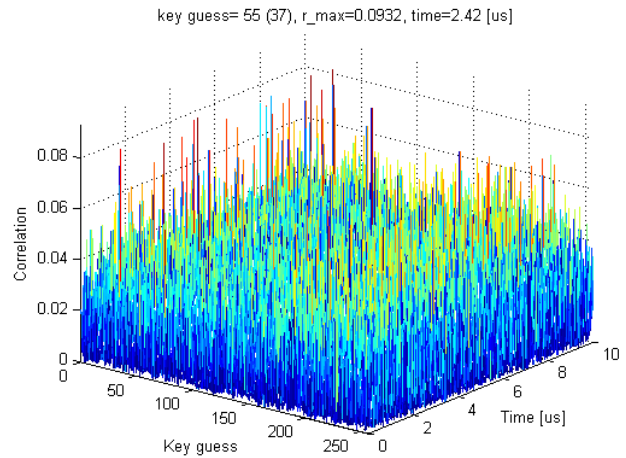


Figure 3: Correlation matrix in the time domain for 2048 traces using EM probe and sampling frequency of 50 MS/s. The analysis returns a wrong key.

Figure 3 presents the values for the correlation analysis using 2048 traces acquired using an inductive probe and a sampling resolution of 50MS/s. The key guessed is 55 with a maximum correlation of 0.0932 at 2.42 μ s. In this case correlation analysis in the time domain using the inductive probe was unable to recover the correct key (162).

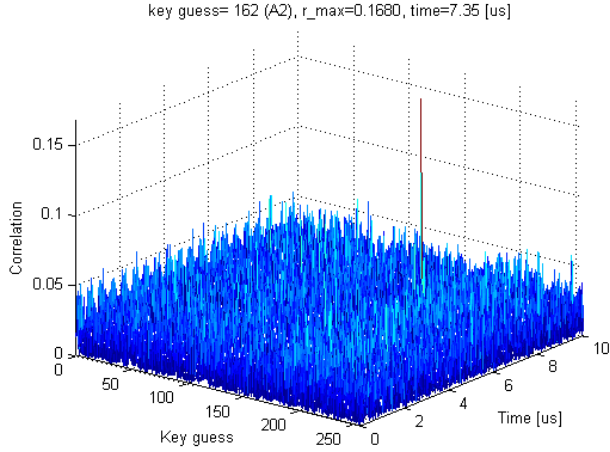


Figure 4: Correlation matrix in the time domain for 2048 traces using the GMR probe and sampling frequency of 50 MS/s.

For the case of the 50 MS/s using the GMR probe, figure 4 shows the correct key guess (162) with a spike at 7.35 μ s. As expected it is located at the same time where other analyses with higher resolutions revealed the correct key. It's important to emphasize the clarity of this result considering the proximity to the minimum sampling rate according to the Nyquist-Shannon sampling theorem. For this scenario 50 sets of 2048 traces were captured. In the 50 experiments, the GMR probe was able to guess the correct key all the times. In the same scenario, the inductive probe failed to recover the correct key in 39 of the 50 experiments.

4.2 Correlation analysis in the frequency domain

For correlation analysis in the frequency domain, the same EM traces were analysed as in the case of the time domain analysis. Table 2 presents the maximum values from the correlation matrix when the traces are analysed in the frequency domain. The respective correlation values in the table are all smaller than the values obtained in the time domain.

Table 2: Maximum correlation values for the frequency domain analysis

Correlation analysis frequency domain		
Sampling frequency [MS/s]	EM probe	GMR probe
500	0.680	0.370
250	0.435	0.320
125	0.231	0.176
50	0.132*	0.110*

* Able to recover the correct key in 7 of 50 experiments.

For the sampling rates of 500 MS/s, 250 MS/s and 125 MS/s it was possible to recover the correct key using both probes. For the sampling rate of 50 MS/s the GMR and the inductive probe were able to recover the correct key in 7 of 50 experiments.

Figure 5 presents the correlation matrix values for the inductive probe using a sampling rate of 500 MS/s. It shows that the frequencies between 15 and 70 MHz present the higher correlations for the correct key guess, where the maximum occurs at 41.52 MHz.

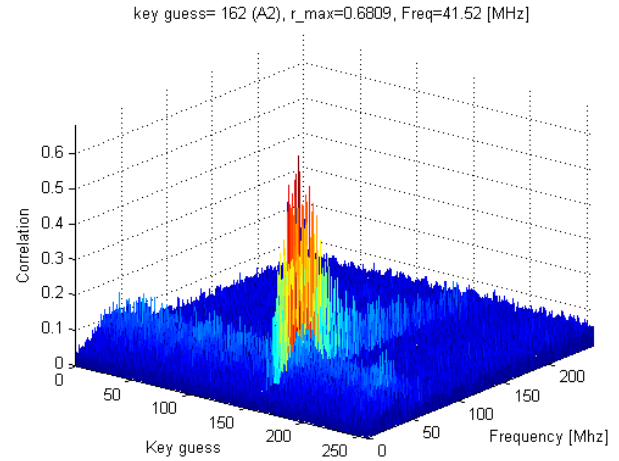


Figure 5: Correlation matrix in the frequency domain for 2048 traces using EM probe and sampling frequency of 500 MS/s.

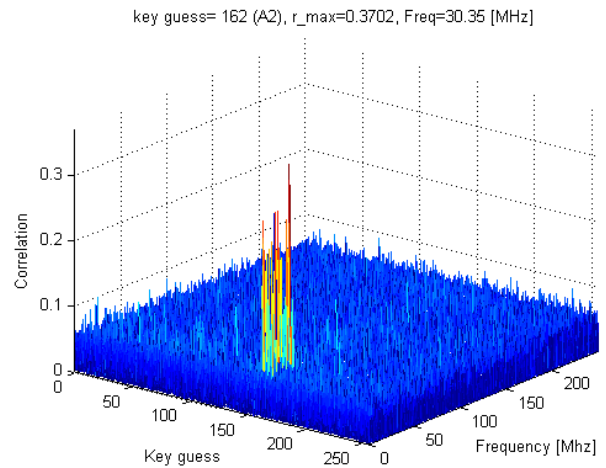


Figure 6: Correlation matrix in the frequency domain for 2048 traces using GMR probe and sampling frequency of 500 MS/s.

Figure 6 shows the values obtained after analyzing the traces obtained with the GMR probe, with a sampling rate of 500 MS/s. In this case, the correct key was retrieved and the range of frequencies with higher correlations for the correct key are between 1 MHz and 33 MHz.

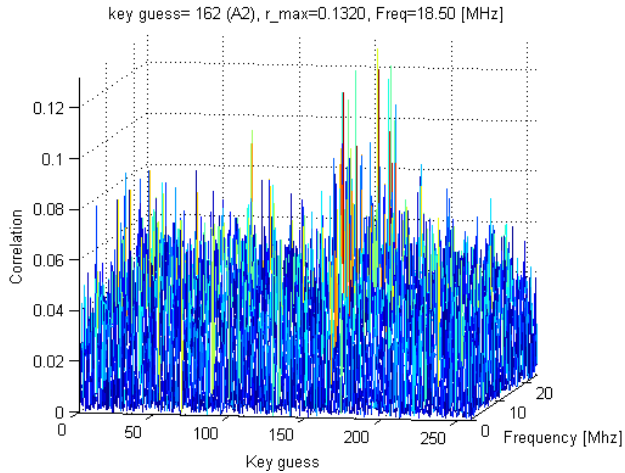


Figure 7: Correlation matrix in the frequency domain for 2048 traces using EM probe and sampling frequency of 50 MS/s.

Figure 7 shows the results obtained after analyzing the EM traces with the inductive probe captured using a sampling frequency of 50 MS/s. The figure shows 1 result of the 7 cases where it was possible to guess the correct key. Here the maximum correlation appeared at 18.5 MHz.

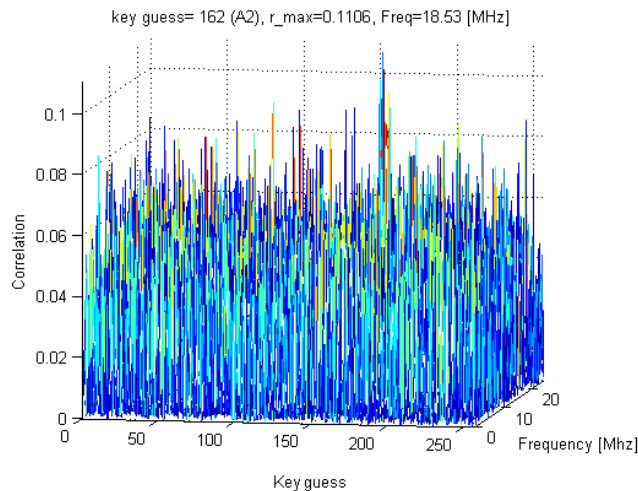


Figure 8: Correlation matrix in the frequency domain for 2048 traces using GMR probe and sampling frequency of 50 MS/s.

Figure 8 presents the correlation values for the frequency domain analysis using the GMR traces acquired with 50 MS/s resolution. The figure shows the maximum correlation in the correlation matrix with a magnitude of 0.11 and corresponds to the frequency of 18.53 MHz. In this analysis similar to the EM probe only 7 of 50 experiments were able to recover the correct key.

4.3 Frequency Response of the probes

In order to illustrate the frequency response of the GMR and the inductive 1 cm loop EM probe, a resistive load was connected to the signal generator Rohde & Schwarz SMA100A using two 30 cm cables AWG22. Then a sinusoidal signal was applied with magnitude of 10dB and frequencies between 1 MHz and 625 MHz with steps of 1 MHz. Each one of the probes was placed on top of one of the cables and the frequency response was measured using a digital oscilloscope using a sampling frequency of 1.25 GS/s.

Figure 9 works as reference to shows the frequency response of the inductive probe (EM probe) next to the AWG22 cable to different frequencies.

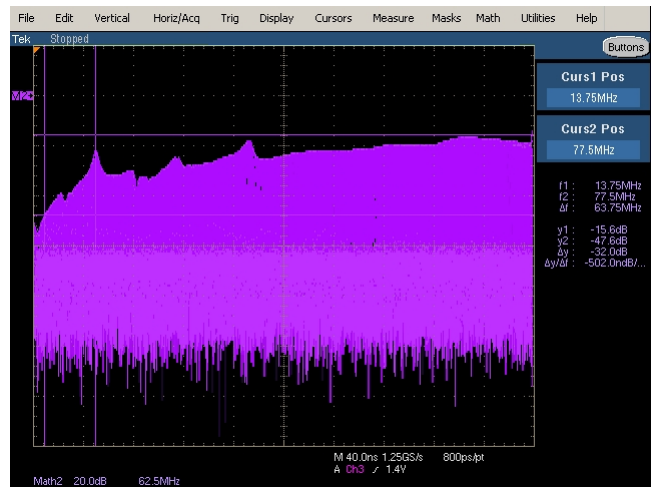


Figure 9: Frequency response of EM probe form 1 to 625 MHz with steps of 1 MHz. Y-axis shows the magnitude in dB.

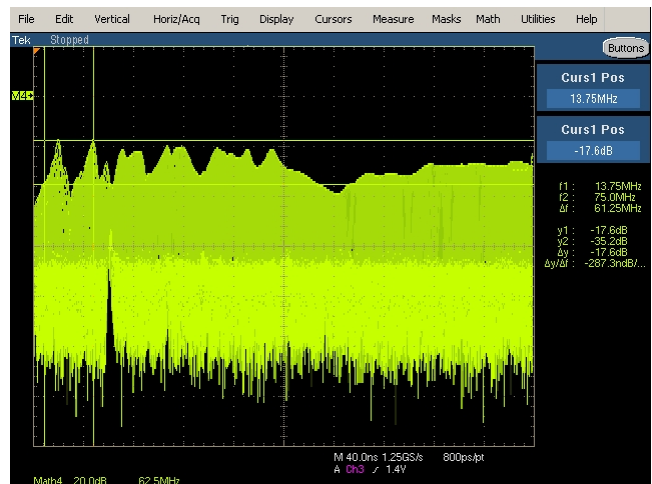


Figure 10: Frequency response of GMR probe form 1 to 625 MHz with steps of 1 MHz. Y-axis shows the magnitude in dB.

Figure 10 shows the response of the GMR probe to different frequencies on the AWG22 cable. It is visible that the GMR probe presents higher magnitudes in the range from 1 MHz to 300 MHz than the inductive 1cm loop commercial probe and the response of the GMR probe remains acceptable even above 600 MHz.

5. DISCUSSIONS AND CONCLUSIONS

This work compares the performance of a commercial inductive loop EM probe with a GMR probe under a variety of scenarios. In general the results show higher correlations for the traces obtained using the inductive probe than those acquired using the GMR probe. However, for the time domain analysis, the GMR probe was able to recover the correct key in all the cases tested, while in the case of the inductive probe using a sampling rate of 50 MS/s it failed to recover the key in 39 of 50 experiments.

For the analysis in the frequency domain using sampling rates of 500 MS/s, 250 MS/s and 125 MS/s it was possible to recover the correct key using the traces acquired with both probes all the times. Using analysis in the frequency domain with a resolution of 50 MS/s, both probes succeed just in 7 of 50 cases. Comparing the time domain and the frequency domain results, it's clear that the time domain analysis returns higher correlations than the frequency domain analysis. Also for very low sampling rates, correlation analysis in the time domain returns better results than the analysis in the frequency domain.

The results show that higher sampling rates return higher correlations. Nevertheless, there are some applications where due to scope memory limitations it is not possible to acquire enough traces using a high sampling rate to determine the region of the attack. In these cases it would be of interest to use the GMR sensors which provide good results even at these low sampling rates.

This paper has shown the effectiveness of using GMR sensors to acquire EM traces for side channel analysis purposes on a 8-bit processor. Although this research does not necessarily suggest the replacement of inductive EM probes with GMRs, it will be important to further explore the properties of GMR in response to the gradients of the magnetic field and their ability to react to magnetic fields in some directions when this kind of sensor is placed in environments with a high magnetic field like in the case of card readers of contactless smartcards.

6. ACKNOWLEDGMENTS

This research was supported in part by CONACYT and grants from NSERC and OCE.

7. REFERENCES

- [1] Agrawal, D., Archambeault, B., Rao, J. R., and Rohatgi, P. The EM Side-Channel(s), *Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Computer Science*, Springer, 2003, pp. 29–45.
- [2] Brier, E., Clavier, C., and Olivier, F. Correlation power analysis with a leakage model. In *Proceedings of the Cryptographic Hardware and Embedded Systems – CHES 2004*. Cambridge, MA, USA, 2004, Springer-Verlag, pp. 16–29.
- [3] Gandolfi, K., Mourtel, C., and Olivier, F., Electromagnetic Analysis: Concrete Results, *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, 2001, pp. 251–261.
- [4] Gebotys C.H., Ho, S., and Tiu C.C. EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. *Cryptographic Hardware and Embedded Systems – CHES 2005*, Springer Berlin / Heidelberg, 2005, pp. 250–264.
- [5] Kasap, S. O. *Principles of electronic materials and devices*, 3rd ed., McGraw-Hill, Boston, MA, 2006.
- [6] Kocher, P. Jaffe, J., and Jun B. Differential Power Analysis, *Proceedings of Advances in Cryptology-CRYPTO'99*, Springer-Verlag, 1999, pp. 388–397.
- [7] Mallinson, J. C. *Magneto-resistive and spin valve heads: fundamentals and applications*, 2nd ed., Academic Press, San Diego, CA, 2002.
- [8] Mangard, S., Oswald, E., and Popp, T. *Power analysis attacks: revealing the secrets of smart cards*. Springer, New York, N.Y. 2007.
- [9] Mateos, E. and Gebotys C.H. A new correlation frequency analysis of the side channel, In *WESS '10 Proceedings of the 5th Workshop on Embedded Systems Security*, 2010, doi>10.1145/1873548.1873552
- [10] Quisquater, J. and Samyde, D. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards, *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security*, 2001, pp. 200–210.

- [11] NVE Sensor Engineering and Application Notes, Non Volatile Electronics Corporation, Eden Prairie, Minnesota, Retrieved from: <http://www.nve.com/Downloads/apps.pdf>
- [12] Rohatgi, P. Side-Channel Attacks, In *H. Bidgoli (Ed), Handbook of information security: Treats, vulnerabilities, prevention, detection and management*, volume 3, Hoboken, NJ, John Wiley and Sons, 2006, pp. 241–259.
- [13] Schimmel, O., Duplys, P., Boehl, E., Hayek, J., Bosch, R., and Rosenstiel, W. Correlation power analysis in frequency domain. In *COSADE 2010 – First International Workshop on Constructive Side-Channel Analysis and Secure Design*, 2010.
- [14] Young, H., Freedman, R., Sandin, T., and Ford, A. *University Physics*, 9th edition, USA, Addison-Wesley Pub. Co., 1996.
- [15] Zhang, P., Deng, G., Zhao, Q., and Chen, K. EM Frequency Domain Correlation Analysis on Cipher Chips. In *Proceedings of the 2009 First IEEE international Conference on information Science and Engineering* (December 26 – 28, 2009). ICISE. IEEE Computer Society, Washington, DC, 1729-1732. DOI=<http://dx.doi.org/10.1109/ICISE.2009.542>