A Compact Probe for EM Side-Channel Attacks on Cryptographic Systems

Frank T. Werner
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia
fwerner6@gatech.edu

Antonije R. Djordjević
School of Electrical Engineering
University of Belgrade
Belgrade, Serbia
edjordja@etf.rs

Alenka G. Zajić
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia
alenka.zajic@ece.gatech.edu

***Abstract*—A shielded loop probe design for evaluating EM side-channels attacks on cryptographic systems is described. This probe is compact and is sensitive enough to measure extremely weak signals that usually comprise EM side-channels. Furthermore, this probe can greatly suppress the influence of the electric field on its measurements. At its center frequency, the probe has a sensor factor of -0.17 dB S/m and electric field suppression ratio of 30.18 dB.**

***Index Terms*—EM side-channel attacks, cryptography, shielded loop probe, near field measurements.**

I. Introduction

Side-channel attacks are a large threat to the security of cryptographic systems. A side-channel is an unintended avenue for observing confidential information from an electronic device [1]. Examples of side-channels include power, acoustic, temperature, and electromagnetic (EM). EM side-channels are particularly popular since they make it possible to monitor a device from a distance and can provide more information than other side-channels [1]. This channel is a result of the EM radiation unintentionally generated by an electronic device during its operation.

Currently, there are numerous examples of EM side-channels being used to attack cryptographic systems. Early work in [1] and [2] demonstrated that EM side-channel attacks were possible on implementations of DES (Data Encryption Standard), RSA (Rivest-Shamir-Adleman), and COMP1218 cryptographic algorithms run on simple devices, such as smartcards. While ways of protecting cryptographic systems have been implemented, new ways of circumventing these protections using EM side-channels are being discovered just as quickly. For example, in 2018, [3] demonstrated a successful attack on a recent implementation of RSA in the current version of OpenSSL running on mobile phones.

The challenge in researching EM cryptographic attacks is receiving a usable signal. The signals tend to be very weak (otherwise the device would not be compliant with EMC standards) and location dependent [4]. Therefore, any probe used to monitor the side-channel needs to be designed to be sensitive to weak electric or magnetic fields. At the same time the probe needs to be able to scan different parts of the device. Presented is a shielded loop probe designed for monitoring EM side-channels by measuring the magnetic field. In the following sections, the design of the probe and its properties are discussed.

II. Probe Design

Shielded loop probes are regularly used in EMC [5]. A shielded loop composes of a loop or part of a loop with a shield enclosing it. The shield has a small gap in the middle, opposite from the output of the probe. The advantage of a shielded loop probe is that it suppresses the influence of the electric field on its measurements, ensuring that its output is the result of only the perpendicular magnetic field [5]. This makes it easier to focus on specific components on a device and locate potential emanation sources.

Fig. 1 shows the probe and its three copper layers. The first and third layers act as the shield and are connected using vias, while the second layer contains the feed line. The probe was implemented on a PCB for durability and compactness. Its small size and flatness makes it easy to scan over different parts of a devices when searching for the best location to monitor a side-channel. To obtain the required sensitivity, the probe has a diameter of 20 mm. By default, the probe has a center frequency of 0.89 GHz. The center frequency can be decreased by soldering capacitors in between the gaps in the shield or can be increased by increasing the size of the gap. Using this method, probes with center frequencies between 800 MHz and 1.8 GHz have been manufactured.

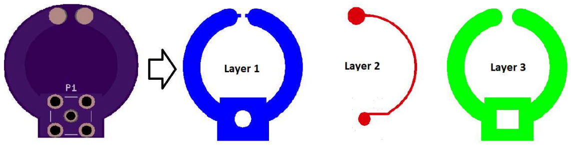

Fig. 1. The probe and its copper layers.

III. Experimental Results

Fig. 2 shows the setup used to test the probe and was based on the setup described in [6]. In this setup, the probe was

This work has been supported, in part, by DARPA LADS contract FA8650-16-C-7620. The views and findings in this paper are those of the authors and do not necessarily reflect the views of DARPA.

situated over a microstrip line at a height of $h = 20$ cm between the center of the probe and the microstrip. The top layer of the microstrip had a length $L = 10$ cm and a width of 2 mm, while the bottom layer was a ground plane. The microstrip substrate had a thickness $t = 1.524$ mm. One end of the microstrip was terminated with 50 Ω, while the other was connected to port 1 of an Agilent N5224A network analyzer. The probe output was connected to port 2 of the analyzer.

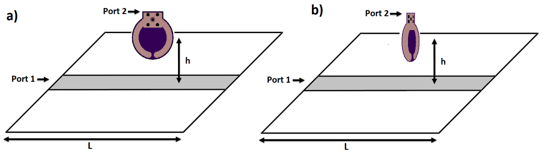

Fig. 2. The measurement setup with the probe oriented so that the central axis of the loop was (a) perpendicular to the line and b) parallel to the line.

First, to demonstrate the probe sensitivity to the magnetic field, this setup was used to calculate the probe sensor factor (SF). SF (also called the antenna factor) is the ratio of the magnetic field passing through the loop to the voltage induced at the probe output by the field. The lower the SF, the lower the magnetic field required to induce a measurable voltage.

To find the SF, S_{21} was measured between the microstrip and the probe while its central axis is perpendicular to the microstrip, as shown in Fig. 2(a). In this orientation, the magnetic field from the microstip is normal to the probe, maximizing the influence of the magnetic field on the output. The layout of the microstrip ensures that its magnetic field is perpendicular to the line and constant at different heights above the line. This constant field and the fact the probe is electrically small makes it possible to calculate the SF from the measured S_{21} [6] as

$$SF(\omega)\text{dB} = 20log\left(\frac{t}{\pi h(h+2t)}\right) - |S_{21}(\omega)| - 34 \qquad (1)$$

Fig. 3 shows the SF calculated for the probe over 0.5 to 2 GHz. At 0.89 GHz, the SF is -0.17 dB S/m. This SF means that to induce a 1 V across the probe output, the magnetic field only needs to be 0.98 A/m.

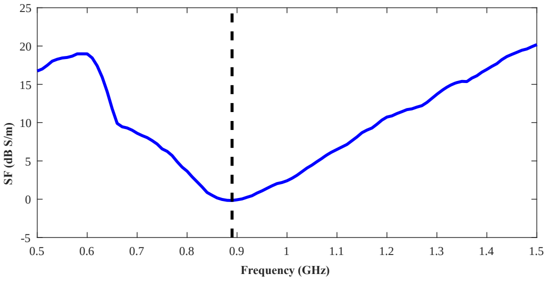

Fig. 3. The probe sensor factor. The black, dashed line indicates the center frequency of the probe.

Next, to demonstrate how well the probe suppresses the influence of the electric field, the S_{21} measured in the first part is compared to S_{21} measured when the influence of the magnetic field is minimized. For simplicity, they are referred to as S_{21H} and S_{21E}. As shown in Fig. 2(b), the probe was rotated 90° so that the central axis of the loop was parallel to the line. In this orientation, the magnetic field is tangential to the loop, minimizing its influence on the output [5]. Instead, the measured voltage is caused by the tangential electric field. While this electric field was also present in the original probe orientation, its influence is negligible compared to the magnetic field.

The ratio of S_{21H} to S_{21E} is called the electric field suppression ratio (H/E). This ratio is commonly used to evaluate how strongly a probe is influenced by the electric field [5]. The suppression ratio calculated from the measurements is shown in Fig. 4. At 0.89 GHz, the ratio is 30.18 dB, indicating the magnetic field has a much stronger impact on the measurements than the electric field.

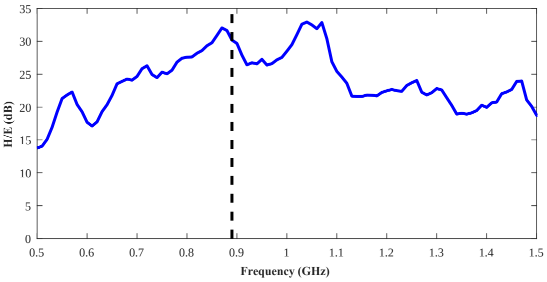

Fig. 4. The electric field suppression ratio for the probe. The black, dashed line indicates the probe's center frequency.

IV. Conclusion

In this work, a shielded loop probe designed for EM side-channel attacks on cryptographic systems is presented. This probe is sensitive enough to detect the weak signals these attacks rely on. Furthermore, it is compact and convenient for scanning a device. Experimental results demonstrate that at its center frequency, the probe has a sensor factor of -0.17 dB S/m and a electric field suppression ratio of 30.18 dB.

References

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side-channel (s)," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 29–45.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2001, pp. 251–261.

[3] M. Alam, H. A. Khan, M. Dey, N. Sinha, R. Callan, A. Zajic, and M. Prvulovic, "One&done: A single-decryption em-based attack on openssl's constant-time blinded rsa," in *Proceedings of the 27th USENIX Conference on Security Symposium*. USENIX Association, 2018, pp. 585–602.

[4] F. Werner, D. A. Chu, A. R. Djordjević, D. I. Olćan, M. Prvulovic, and A. Zajić, "A method for efficient localization of magnetic field sources excited by execution of instructions in a processor," *IEEE Transactions on Electromagnetic Compatibility*, vol. PP, no. 99, pp. 1–10, 2017.

[5] Y. Chou and H. Lu, "Magnetic near-field probes with high-pass and notch filters for electric field suppression," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 6, pp. 2460–2470, June 2013.

[6] T. Harada, H. Sasaki, and E. Hankui, "Time-domain magnetic field waveform measurement near printed circuit boards," *Electrical Engineering in Japan*, vol. 125, no. 4, pp. 9–18, 1998.