A Method for Efficient Localization of Magnetic Field Sources Excited by Execution of Instructions in a Processor

Frank Werner, *Student Member, IEEE*, Derrick Chu, *Student Member, IEEE*, Antonije R. Djordjević, Dragan I. Olćan, *Member, IEEE*, Milos Prvulovic, *Senior Member, IEEE*, and Alenka Zajić, *Senior Member, IEEE*

***Abstract*— This paper proposes a method for efficient identification of instruction-dependent sources on a printed-circuit board (PCB) by localizing magnetic field sources from a limited number of measurements around the PCB. We first excite the processor by generating an artificial leakage signal at a specific frequency that is directly related to processor instructions. Then, we collect all three components of the magnetic field, but only at locations around the edge of the board. Furthermore, we model these magnetic field sources and then solve a forward-backward optimization problem using the model and measured data to identify the locations of the magnetic field sources, the magnitudes of the moments, and their orientations. The localization results are first verified using simulations, then tested when noise is added to the simulation results, and finally verified against measurements on FPGA and IoT development boards. The results show that the number of strong magnetic field sources on a board depends on the instructions used to excite the board. Furthermore, the results show that the proposed localization algorithm can accurately identify those sources, regardless of the frequency at which the measurements are conducted and the instruction pairs that are executed. Finally, the proposed method can significantly reduce the number of measurement points and the time needed to identify magnetic field sources on a PCB.**

***Index Terms*— electromagnetic emanation security and integrity, electromagnetic information leakage, localization of magnetic field sources.**

I. Introduction

Side-channel attacks are a major concern for electronic security. They circumvent traditional security techniques by relying on other conduits of observing confidential information [1], [2], [3]. Researchers have used electromagnetic (EM) emanations to compromise the security of many types of devices [4], from ASIC design primitives to keyboards [5], smartcards [6], and desktop computers [7]. One of the main challenges in studying the side-channel EM emanations is how to identify the best position of the probe near the board to collect the strongest signals without collecting too much noise/interference. An additional challenge is that the source of the emanations is software dependent and can move across the board. Traditionally, locations where the signals should be collected are identified by running a code and scanning the board for the strongest EM locations. This is a long and tedious process, highly dependent on the code that is running.

Another research area that heavily depends on scanning the EM emanations across a board is detection of hardware Trojans. Ensuring the authenticity and integrity of hardware components is becoming one of the major challenges faced by the integrated-circuit industry. The counterfeiting of hardware components has experienced a dramatic increase in the last years [8]. To detect hardware Trojans, researchers heavily depend on 3-D EM scan of the infected versus uninfected components to identify the differences in EM emanations [9].

Finally, to help board designers identify the electromagnetic radiation effects related to their circuit design, it can be useful to have simplified equivalent models that can efficiently simulate the radiated emissions generated by the board [10], [11], [12]. Development of these models also depends on the efficient identification of EM sources on a printed-circuit board (PCB).

To address the problem of efficiently identifying *instruction-dependent sources* on a board, we have developed a method that localizes magnetic field sources from a limited number of measurements around the PCB. To excite the processor in a controlled manner, we use our method [13] to generate an artificial leakage signal at a specific frequency that is directly related to processor instructions. The generated signal has peaks at the desired frequency and is easy to detect and measure.

Note that we can choose the frequency of the emanations to be located on a part of the spectrum that has minimal interference. By changing the instructions in the benchmark, we can excite different parts of the processor and memory circuitry. Another advantage of this approach compared to just running a program is that we can alternate between two particular instructions (e.g., add vs. subtract) for as long as we need to collect the data, making the measurement process very stable and repeatable.

To reduce the number of measurements needed for a full scan of the PCB, we collect all three components of the magnetic field only around the edges of the board (e.g., 5-10 locations per edge). These measurements are then used to solve a forward-backward optimization problem to identify the locations of the magnetic field sources, the magnitudes of

This work has been supported, in part, by NSF grants 1563991 and 1318934, AFOSR grant FA9550-14-1-0223, and 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 NSF, AFOSR, or DARPA.

Frank Werner, Derrick Chu, and Alenka Zajić are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA,
Antonije R. Djordjevic and D. I. Olcan are with the School of Electrical Engineering, University of Belgrade, 11120 Belgrade, Serbia,
Milos Prvulovic is with the School of Computer Science, Georgia Institute of Technology, Atlanta, GA 30332, USA.

their magnetic moments, and their orientations. To solve this optimization problem, we first set up an inverse (backward) electromagnetic problem of identifying sources of a time-harmonic quasi-stationary magnetic field. We assume that each source is a small loop, which can be considered as a magnetic dipole with an unknown magnetic moment **m**. The number of sources in the model can be either known (provided to the model) or unknown (chosen by the model itself). We assume that we do not know the magnitudes of the sources' magnetic moments, nor their orientations. All moments are assumed to be linearly polarized. Then, we develop an electromagnetic model of the sources, i.e., a set of equations which yield the magnetic-flux density of a known set of sources (magnetic dipoles). We refer to this set of equations as the forward model. Finally, we use several optimization techniques, such as Nelder-Mead simplex method [14] or the particle swarm optimization (PSO) [15], to estimate the moments of these dipoles in an attempt to make the forward model produce magnetic fields at the test points as close as possible to the measured fields.

The localization results are first verified using simulations in AWAS [16], then tested when noise is added to the simulation results, and finally verified against measurements on FPGA and IoT development boards. The results show that the number of strong magnetic field sources on a board depends on the instructions used to excite the board. This is an interesting result because it indicates that some instructions cause emanations from multiple sources, making them potentially easier to exploit for side-channel attacks. Finally, our results show that the proposed localization algorithm can accurately identify those sources, regardless of the frequency at which the measurements are conducted and the instruction pairs that are executed. The proposed method can significantly reduce the number of measurement points and the time needed to identify magnetic field sources on a PCB.

The rest of this paper is organized as follows. Section II describes benchmarks that create system activity at controlled frequencies, Section III describes proposed algorithm for localizing magnetic field sources in the computer systems, Section IV tests robustness of the algorithm, Section V describes the measurement setup and presents experimental results, and Section VI concludes the paper.

II. Creating System Activity at Controlled Frequencies

The first step in localizing the sources on the electronic board is to excite the processor in a controlled manner. To achieve that, we use our method in [13] to generate an artificial leakage signal which is directly related to processor instructions at a specific frequency. Here we briefly summarize the approach. The excitation program is shown in Fig. 1. It has two loops, one that repeatedly performs some activity X (line 2) and the other performs some other activity Y (line 8). These loops are enclosed in an outer loop (line 1) which causes the program to repeatedly alternate between activities X and Y. This creates periodically-changing activity whose period equals the execution time of one iteration of the outer loop. This alternation period T_{alt} is the inverse of the frequency $f_{\text{alt}} = 1/T_{\text{alt}}$.

```
1  while(true){
2    // Execute the X activity
3    for(i=0;i<inst_x_count;i++){
4      ptr1=(ptr1&~mask1)|((ptr1+offset)&mask1);
5      // The X-instruction, e.g., a load from L2
6      value=*ptr1;
7    }
8    // Execute the Y activity
9    for(i=0;i<inst_y_count;i++){
10     ptr2=(ptr2&~mask2)|((ptr2+offset)&mask2);
11     // The Y-instruction, e.g a store from L2
12     *ptr2=value;
13   }
14 }
```

Fig. 1. Pseudo-code to generate the X/Y alternation activity.

It is important to emphasize that while the effect of a single event (i.e., execution of a single memory access or processor instruction) on the side-channel signal is unknown, as long as there is some difference between the X and Y activities, there will be a spectral line generated at the frequency f_{alt} and also at some of the harmonics of f_{alt} ($2f_{alt}, 3f_{alt}, ...$). In our measurements, we record the magnitude of the spectral line at f_{alt}. Note that we can choose the frequency of emanations such that it allows us to select a part of the spectrum that has minimal interference. By changing the instructions in the benchmark, we can excite different parts of the processor and memory circuitry. Finally, we note that this signal can also be measured as a modulated signal around the processor clock or memory clock frequency, which we will also explore as a possible signal to be used for localization of the magnetic field sources on a board.

III. Localization of Magnetic Field Sources

In this section we describe the proposed method for the localization of magnetic field sources generated by processor activity.

A. Problem Statement

Here, we consider an inverse electromagnetic problem of identifying sources of a time-harmonic quasi-stationary magnetic field. The operating frequency f is known. Hence, we know the angular frequency $\omega = 2\pi f$. The sources are located in a parallelepiped whose dimensions are $2a_s$, $2b_s$, and h_s, as shown in Fig. 2. We refer to this parallelepiped as the source space (ν). This space is assumed to be known. The source space is sitting on an infinite, perfectly conducting (PEC) ground plane.

Within ν, there can be one or several sources. Each source is a small loop, which can be considered as a magnetic dipole of (an unknown) magnetic moment **m**. As the first step, we assume a known number of dipoles. In Section IV-B, we evaluate the proposed method by assuming an unknown number of dipoles. In both cases, we do not know the magnitudes of the moments nor their orientations. All moments are assumed to be linearly polarized. Although in practice the moments seem to be in-phase across the whole PCB, in the identification of these moments we take one moment as the reference (whose initial phase is 0), and search for the phase differences between each other moment and the reference one.

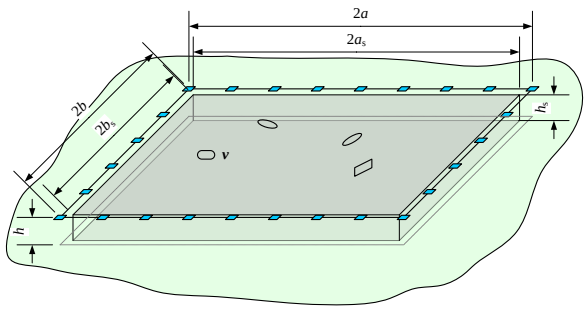


Fig. 2. Source space (ν) with several current-carrying loops and test points (squares).

We assume that measurements of the magnetic field are performed at a known set of P points (referred to as the test points) located around the source space (i.e., the PCB). These points are located on a rectangle, whose sides are $2a$ and $2b$, positioned at an elevation h above the ground plane (Fig. 2). The test points are equally spaced along each side of the rectangle, with n_a and n_b spacings along a and b, respectively. The total number of the test points is thus $P = 2n_a + 2n_b$. At each point, we measure the magnitudes of the three Cartesian components of the magnetic-flux density (magnetic induction) vector (B_x, B_y, and B_z). Hence, we know $3P$ scalar quantities for each test point.

The objective is to estimate the magnetic moment vectors of the sources. To achieve the objective, we need to develop the forward model, as described in the following section, and use the simplex method [14] or the particle swarm optimization (PSO) [15] to estimate the moments of these dipoles in an attempt to make the forward model produce magnetic fields at the test points as close as possible to the measured fields.

B. Forward Model

The forward electromagnetic model is used to calculate the magnetic field of a given set of magnetic dipoles, which are sources of this field. The number of dipoles and their phasor magnetic moments, locations, and orientations are known. The resulting magnetic field (magnetic-flux density) vector is evaluated at a set of field (test) points. We assume that the field is quasi-stationary. We take into account the currents induced in the PEC plane by introducing images of the magnetic moments.

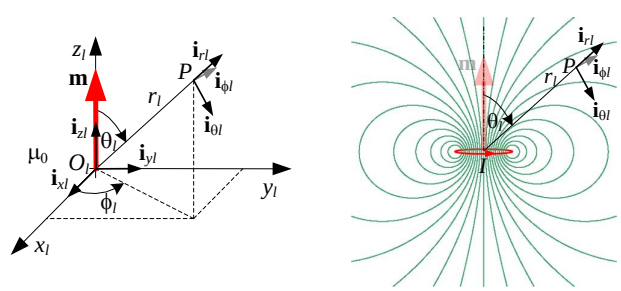


Fig. 3. (left) Local Cartesian coordinate system attached to a magnetic dipole with the corresponding spherical system; (right) magnetic field lines of a small loop.

Figure 3 (left) shows the local Cartesian and spherical coordinate systems attached to a magnetic dipole, which is located at the coordinate origin and whose momentum is oriented along the z-axis. (The index "l" points out that this is the local coordinate system, which is different from the global system.) Figure 3 (right) shows a small current-carrying loop, which is a realistic counterpart of a magnetic dipole, with the lines of the magnetic field and the local spherical coordinate system.

Assuming the magnetic dipole to be located in a vacuum, its magnetic-flux density at the field point P is given by

$$\begin{aligned} \mathbf{B} &= -\frac{\mu_0}{4\pi}\mathrm{grad}\left(\frac{\mathbf{m}\cdot\mathbf{r}_{0l}}{r_l^2}\right) \\ &= \frac{\mu_0}{4\pi}\frac{m_{zl}}{r_l^3}\left(2\mathbf{i}_{rl}\cos\theta_l + \mathbf{i}_{\theta l}\sin\theta_l\right), \end{aligned} \tag{1}$$

where $\mathbf{m} = m_{zl}\mathbf{i}_{zl}$ is the magnetic moment of the dipole, $\mathbf{i}_{\mathrm{x}l}$, $\mathbf{i}_{\mathrm{y}l}$, and $\mathbf{i}_{\mathrm{z}l}$ are the unit vectors of the local Cartesian coordinate system, whereas $\mathbf{r}_{0l} = \mathbf{i}_{\mathrm{r}l}$, $\mathbf{i}_{\theta l}$, and $\mathbf{i}_{\phi l}$ are the unit vectors of the local spherical coordinate system attached to the dipole. Alternatively, we can obtain the local Cartesian components of the vector $\mathbf{B}$ by noting that $\mathbf{m}\cdot\mathbf{r}_{0l} = zm_{zl}/r$, as

$$\begin{aligned} \mathbf{B} &= -\frac{\mu_0}{4\pi}m_{zl}\mathrm{grad}\left(\frac{z_l}{r_l^3}\right) \\ &= \frac{\mu_0}{4\pi}\frac{m_{zl}}{r_l^3}\left(\frac{3z_l}{r_l^2}(x_l\mathbf{i}_{xl} + y_l\mathbf{i}_{yl} + z_l\mathbf{i}_{zl}) - \mathbf{i}_{zl}\right) \\ &= \frac{\mu_0}{4\pi}\frac{m_{zl}}{r_l^3}\left(\frac{3z_l}{r_l}\mathbf{r}_{0l} - \mathbf{i}_{zl}\right). \end{aligned} \tag{2}$$

If the magnetic moment $\mathbf{m}$ has an arbitrary orientation in the global system, its Cartesian components can be found. For each component, we can design a local coordinate system as in Fig. 3, find the components of the vector $\mathbf{B}$ in that system, and then translate them to the Cartesian components in the global Cartesian system.

The resulting vector $\mathbf{B}$, due to all magnetic dipoles, is obtained by summing the global Cartesian components of the field due to the individual dipoles as well as to their images.

C. Optimization Procedure

In the optimization process, we assume that the number of magnetic dipoles is known, but can be equal, smaller, or greater to the actual number of loops. For each dipole, except for the last one, seven optimization variables are used with the following restrictions:

- the magnitude of the dipole moment, m;
- the Cartesian x-coordinate of the dipole center with respect to the global system, $-a_\mathrm{s} \leqslant x \leqslant a_\mathrm{s}$;
- the Cartesian y-coordinate of the dipole center with respect to the global system, $-b_\mathrm{s} \leqslant y \leqslant b_\mathrm{s}$;
- the Cartesian z-coordinate of the dipole center with respect to the global system, $0 \leqslant z \leqslant h_\mathrm{s}$;
- the spherical θ-coordinate of the dipole moment vector, $-2\pi \leqslant \theta \leqslant 2\pi$;
- the spherical ϕ-coordinate of the dipole moment vector, $-2\pi \leqslant \phi \leqslant 2\pi$;
- the initial phase of the dipole moment, $-2\pi \leqslant \alpha \leqslant 2\pi$.

The initial phase for the last dipole is assumed to be 0; hence, the last variable is omitted for this dipole. Thus, the total number of optimization variables is $N = 7n - 1$

(where $N \leqslant P$), where n is the total number of dipoles. The restrictions for the angles θ, ϕ, and α are extended beyond the respective basic ranges necessary for their definition in order to enable a flexible optimization which may dwell around the boundaries of the basic ranges. The cost-function used in all optimization algorithms has the following form:

$$F = \frac{4\pi}{\mu_0 P} \left(||B_{x\mathrm{f}}| - |B_{x\mathrm{m}}|| + ||B_{y\mathrm{f}}| - |B_{y\mathrm{m}}|| + ||B_{z\mathrm{f}}| - |B_{z\mathrm{m}}||\right), \quad (3)$$

where the index f denotes the values from the forward model, and the index m denotes the measured values.

We use simplex optimization [14] or particle-swarm optimization (PSO) [15] to solve this optimization problem. For the simplex algorithm, the cost function is set to a large value (100) if a boundary for any variable is exceeded. Additionally, the simplex algorithm is combined with a random search. These algorithms were implemented in our own proprietary software, written in FORTRAN and C.

The lengthiest algorithm randomly selects a point within the allowed space for the optimization variables, launches a simplex search from the the point and then records the results. The algorithm repeats this procedure many times before selecting the best solution. This algorithm results in thousands and even millions of evaluations of the cost function, but has an increased chance of finding the global optimum. Most runs were of this kind, and they are used to prove the concept and tailor the cost function. A more sophisticated approach is to run a random search, find the optimal point, and then launch a simplex search from the optimal point. Finally, the PSO algorithm is launched within the allowed space for the optimization variables.

IV. Model Verification and Robustness

In this section, we first test the proposed localization model using AWAS simulation results as a proxy for measurements. The reason for this verification is to have a benchmark, with a full control of the location and moments of magnetic field sources. The second step in validation is to add white Gaussian noise and check the accuracy of the localization model. Furthermore, we investigate how the model behaves if the number of sources is unknown (which is typical for practical applications). Finally, we use measurement results around FPGA and IoT devices, as described in Section V, to validate the model.

A. Verification of Localization Algorithm Via Simulated Data

Our first step in validating the localization model is to use simulated data as a proxy for real measurements. We use AWAS [16] to compute the magnetic-flux density of a known set of sources at the test points.

The operating frequency in the simulations is $f = 154.5$ kHz. The dimensions of the rectangle where the test points are located are $a = 50$ mm and $b = 40$ mm, whereas its elevation above the ground plane is $h = 30$ mm. The numbers of spacings along a and b are $n_\mathrm{a} = 10$ and $n_\mathrm{b} = 8$. Hence, the total number of test points is $P = 36$. The dimensions of the source space are defined by $a_\mathrm{s} = 0.975a$, $b_\mathrm{s} = 0.975b$, and $h_\mathrm{s} = h$.

We have generated models with one, two, and three loops. Each loop is a small square, whose side is $s = 1$ mm, centered at a point (within the source space), whose Cartesian coordinates are (x_i, y_i, z_i), $i = 1, 2, 3$. Hence, each loop can be regarded as a magnetic dipole. Each loop is fed by an ideal current generator, whose RMS current is I_i. The magnetic moment of a loop is $m_i = I_i S^2$, where $S = 1$ mm^2 is the surface area of the loops. The currents of the loops are $I_1 = 1$ mA, $I_2 = 2$ mA, and $I_3 = 0.25$ mA. The reference directions of the vectors $\mathbf{m}_\mathrm{i}$ are different for the three loops: $\mathbf{m}_1$ is directed along the y-axis, $\mathbf{m}_2$ along the x-axis, and $\mathbf{m}_3$ along the z-axis. The data for the three loops are summarized in Table I, where the magnetic moments are defined in terms of their Cartesian components, which are phasors, i.e., complex representatives of the time-domain counterparts. Alternatively, the magnetic moment vector can be defined in terms of spherical coordinates as (m, θ, ϕ) , where m is the RMS phasor, θ is the zenith angle (the angle with respect to the z-axis, $0 \leqslant \theta \leqslant \pi$), and ϕ is the azimuth angle (the angle between the projection of the vector onto the Oxy-plane and the x-axis, $-\pi \leqslant \phi \leqslant \pi$).

TABLE I

Summary of parameters used to simulate loops.

i	x_i [mm]	y_i [mm]	z_i [mm]	m_x [nA m^2]	m_y [nA m^2]	m_z [nA m^2]	m [nA m^2]	θ [rad]	ϕ [rad]
1	30.5	20	5.5	0	−1	0	1	$\frac{\pi}{2}$	$-\frac{\pi}{2}$
2	0	−10.5	2.5	−2	0	0	2	$\frac{\pi}{2}$	π
3	−40.5	20.5	15	0	0	0.25	0.25	0	0

In the first model, only the loop 1 from Table I is present. The second model comprises the loops 1 and 2, and the third model has all three loops. Note that the considered electromagnetic system is quasi-stationary: the dimensions of the system are much smaller than the wavelength (which is close to 2 km). Hence, the retardation of the electromagnetic fields is negligible, and the field points (test points) are in the near-field zone of the sources (loops, i.e., magnetic dipoles). In AWAS, the near-field is computed at a uniform rectangular grid of $(n_x+1)(n_y+1) = 99$ points, spanned by the test points. This grid is parallel to the Oxy-plane at the height h above this plane. The computed field is used to create a visualization of the intensity of the magnetic field at this height. Also, the data for the field at the test points are extracted and used to estimate the field sources.

Figure 4 shows contour plots for the total field (more precisely, the intensity of the magnetic-flux density vector normalized to its maximal value on the grid) for 1, 2, and 3 loops, obtained using AWAS. Dark blue square markers denote the positions of the magnetic dipoles. White lines represent the moments of the dipoles. The moments are plotted in a single direction to stress their initial phases. The moment of the third dipole (positioned in the upper-left corner) is perpendicular to the plot and directed outwards. Light blue square markers denote positions of the test points.

Note that the local maxima of the field need not be exactly above each loop. There are two reasons for this. First, for an arbitrarily positioned loop, the maximum may be shifted

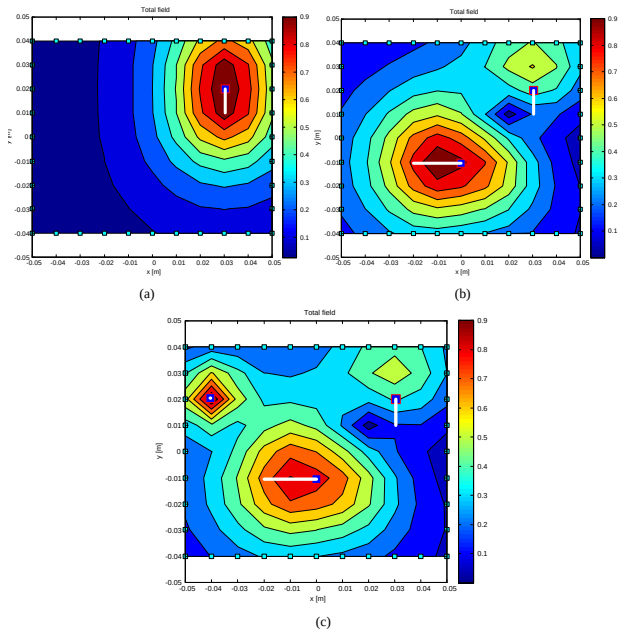


Fig. 4. Normalized intensity of the magnetic field for (a) one loop, (b) two loops, and (c) three loops.

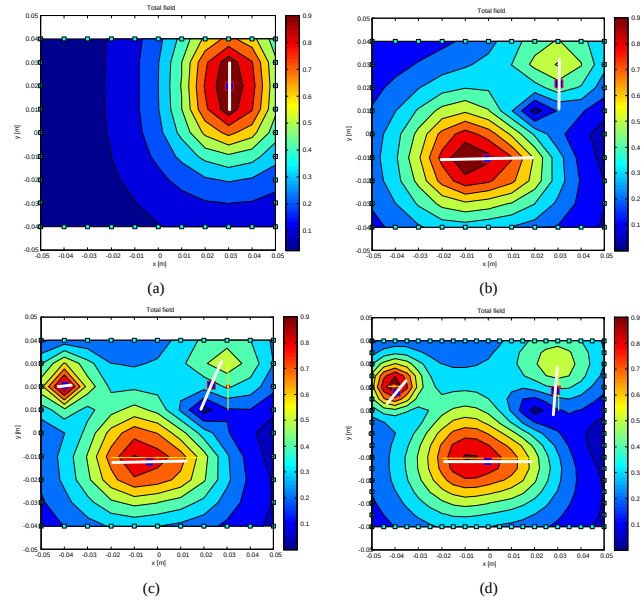


Fig. 5. Results of simplex optimization launched from randomly selected points for (a) one loop, (b) two loops, (c) three loops, and (d) three loops with an increased number of test points.

because the intensity of the magnetic field, at a fixed distance from the loop, varies with spherical angles defined with respect to the local coordinate system attached to the loop. Second, the fields due to the loops are synchronized; hence, they interfere, creating a complicated pattern in the plane of the plot. Also note that the magnetic fields of the loops are strongly affected by the presence of the ground plane: far away from the loops, the fields of the first two loops are enhanced, whereas the field of the third loop is reduced.

Now, we run the simplex optimization with the following data: $10,000$ randomly selected points, the initial step of 0.05, the maximal number of simplex iterations 2000, and the prescribed accuracy for function values and optimization variables of 10^{-12}. The same data is used for the other examples, unless stated otherwise. The results are shown in Fig. 5.

In Fig. 5, the exact solutions for the magnetic dipoles are shown by smaller square markers and yellow lines. These lines go in both directions to point out that we are not interested in the phases anymore. The solutions of the optimization procedure are shown by bigger square markers and white lines. The lengths of these lines are proportional to the estimated moments. The directions of these lines correspond to the estimated azimuth angle, but the estimated zenith angle does not influence the plots.

We can observe that with just one loop, the problem is solved almost perfectly. However, the quality of the solution deteriorates with increasing the number of loops. The quality of the solution for the system with three loops is acceptable, but far from being perfect. In complicated systems, the improvement of the optimization function is relatively small, just one order of magnitude. The optimization function is multimodal, i.e., it has a lot of local minima. Hence, the simplex optimization almost always terminates prematurely in a local minimum and the global minimum (optimum) is very rarely found. The problem which we consider is ill-posed. Increasing the number of test points (P) may improve the quality of the solution, as illustrated on Fig. 5 (d). However, note that this is not the major limitation for the applications such as side-channel analysis or hardware Trojan detection where one reliable location to collect EM signals is sufficient.

B. Localization with Unknown Number of Sources

In this section we illustrate what happens if we do not know the number of sources, but rather set it arbitrarily. This is a realistic assumption because we often do not know the number of sources a priori. Fig. 6 (a) presents results for the case of one loop when we suppose that there are three dipoles present. The algorithm finds two additional, parasitic sources, indicating the ill-posedness of the problem, which is typical for inverse problems as the one we are solving here.

Figure 6 (b) presents results for the system of three loops when we suppose that there is one magnetic dipole, whereas Fig. 6 (c) presents the same system, but with five dipoles. When only one magnetic dipole is assumed, the algorithm finds the dominant source. When we take more dipoles than the number of loops, parasitic solutions exist, as for the system with one loop. However, the parasitic dipoles have small moments in this case which is a good indicator that they are parasitic solutions and can be neglected.

C. Localization Using Simulated Data with Noise

The second step in the verification of the localization results was to test the localization algorithm against simulated data with added white Gaussian noise. In the simulations, the signal-to-noise ratio (SNR) was calculated as the ratio of the intensity of the strongest field at the test points and the standard deviation of the Gaussian noise added to each field component at these points. We consider the case of three loops when there is no added noise, when the SNR is 30 dB, 20 dB,

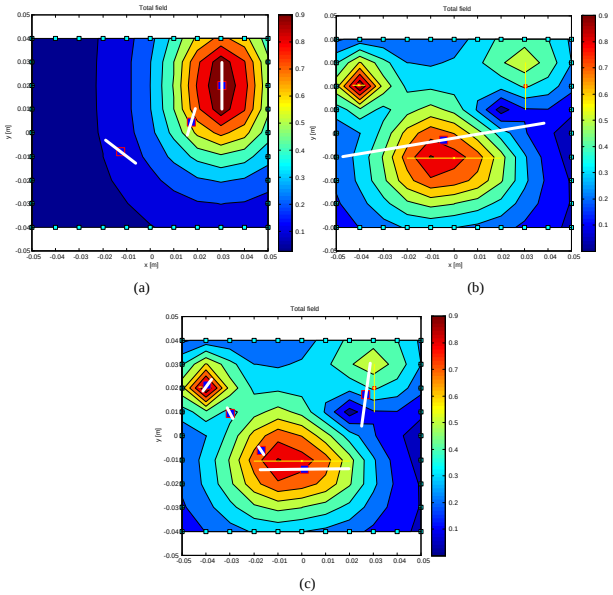


Fig. 6. Results of simplex optimization when the number of assumed dipoles does not match the number of loops: (a) one loop and three dipoles, (b) three loops and one dipole, and (c) three loops and five dipoles.

and 10 dB. The results are shown in Fig. 7 and they should be compared with the results in Fig. 5 (c), which shows results of localization of three loops without added noise. The results

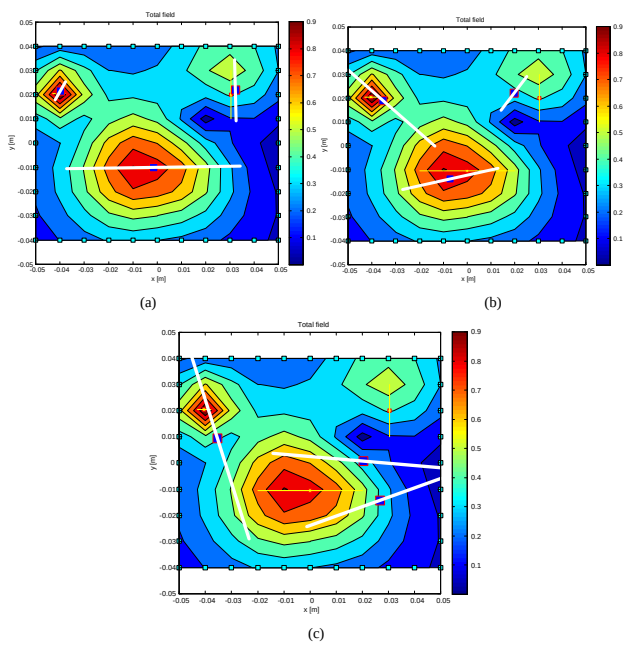


Fig. 7. Optimization for the case of three loops when the signal-to-noise ratio is (a) 30 dB, (b) 20 dB, and (c) 10 dB.

show that the algorithm is robust against noise: the results without noise and for $\mathrm{SNR} = 30$ dB do not differ significantly. Even for $\mathrm{SNR} = 20$ dB, the results are acceptable. The quality of the results is significantly deteriorated only for $\mathrm{SNR} = 10$ dB.

V. Experimental Results

In the following subsections, we first describe a measurement setup that has been developed for accurately and consistently measuring the magnetic fields generated by an electronic device and devices used in testing. Then, we test the proposed localization model by comparing modeled with measured data from real devices. Finally, we present localization results obtained for several different pairs of instructions on different devices.

A. Measurement Setup

The measurement setup is shown in Fig. 8. To collect measured data around the board, we use the MakeBlock XYPlotter Robot Kit v2.0 (the large, light blue device in Fig. 8) which has step motors (with an x-y accuracy of 0.1 mm) for positioning. This setup has a significantly lower cost compared to professional 2-D scanners. We use a hand-made 33-turn coil magnetic field probe with a radius of 5 mm and attach it to the plotter for collecting power measurements. At all times, the probe remain 3 cm above the PCB of the device being tested. The magnitude of the power across the loop probe is measured by a spectrum analyzer (MXA N9020A). Any cables connected to the device being tested are shielded (i.e., wrapped by copper tape) to minimize the influence on the measurements, as shown in Fig. 8.

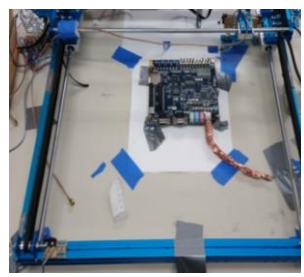


Fig. 8. Photo of the measurement setup.

To approximate an isotropic receiver, three sets of measurements are taken for each pair of instructions. In each set, the probe is oriented parallel to the x-axis, y-axis, or z-axis, respectively. Taking separate measurements with the probe in the three different orientations is equivalent to taking measurements using a set of collocated loops. During a set of measurements, the magnetic probe moves with a step size of 0.5 cm across the entire area of the device. Using this setup, it takes 15 hours to measure the magnetic field over the entire area of the FPGA board. However, the model only needs the measurements around the edge of the device. The rest of the measurements are for demonstrating the accuracy of the model. Taking measurements only around the edges of the device decreases the measurement time to one hour.

B. Devices Under Test

In the follow subsections, measurements are collected for two system boards: a Cyclone II FPGA development board from Altera and an A13-OLinuXino-MICRO IoT board from Olimex. The FPGA board implements a Nios-II soft processor while the Olimex board has an ARM A13 Cortex-A8 processor. The accuracy of the model is first confirmed on the FPGA board and then used on the Olimex board to demonstrate its effectiveness on more complicated devices. These devices are convenient for testing and representative of a wide variety of embedded and IoT computer systems, giving confidence that the same measurement process can be applied to most programmable devices.

In this work, measurements are taken across each device while the device is executing an alternating pair of instructions. We classify these instructions into two categories: *on-chip* and

off-chip instructions. On-chip instructions are those executed exclusively on the processor chip, without interacting with other chips such as system memory. In our experiments, addition, subtraction, division, multiplication, on-chip load, and on-chip store are examples of such instructions. For the rest of this work, these instructions are referred to as ADD, SUB, DIV, MUL, LDL1, and STL1 respectively. For consistency, the same operands are used for all the instructions, and the same registers are used for storage.

The off-chip instructions used in the experiments are off-chip load and off-chip store (LDM and STM). To ensure the off-chip instructions require the processor to interact with the external memory, the addresses used for the LDM and STM are specified to be located on the external memory. For consistency, the same addresses are used for all off-chip instructions.

C. Localization of Sources Created by On-Chip and Off-Chip Instructions on the FPGA Board

In this subsection, we present localization results for FPGA board when it executes DIV/ADD, MUL/ADD, and LDM/DIV. The alternating frequency for all measurements in this and the following subsections is 156 kHz. DIV/ADD and MUL/ADD use only on-chip instructions, while LDM/DIV uses one off-chip and one on-chip instruction.

The last step in the verification of our localization algorithm is to verify if the estimated locations of sources are physically meaningful. While the magnetic dipoles identified by our technique are only approximations of the actual time-varying components of currents, the equivalent dipoles and the actual ac currents need to produce similar magnetic fields not only along the perimeter of the PCB (where the test points are located), but also anywhere above the PCB (except extremely close to the affected chips, their pins, and decoupling capacitors).

To demonstrate that the sources determined by the localization are good approximations of actual ac currents, we compare measured fields when the FPGA executes DIV/ADD with simulated magnetic fields (obtained in ANSYS Maxwell and confirmed by AWAS) when small loops are positioned in the locations found by the localization algorithm.

The total measured magnetic field of DIV/ADD is shown in Fig. 9 (left), and the physical locations of the sources on the FPGA board are shown in Fig. 10 (right). The locations of the

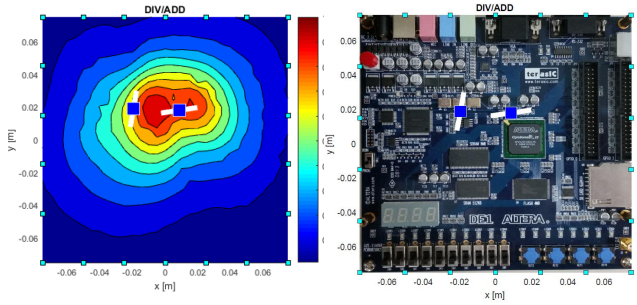


Fig. 9. (left) Total measured magnetic field for DIV/ADD with locations of the sources; (right) locations of the sources for DIV/ADD on the FPGA board.

sources are represented by the dark blue markers, while the white lines represent the orientation of the dipoles' moments. The light blue squares indicate the number and positions of the measurement points used by the algorithm. Before discussing the sources themselves, it should be noted that the magnetic field in Fig. 9 is strongest around the FPGA. This result supports the assumption that the instruction-dependent current will be limited to the area around the chip or chips executing the instructions. Similar results can be seen in the measurements taken for the other pairs of instructions.

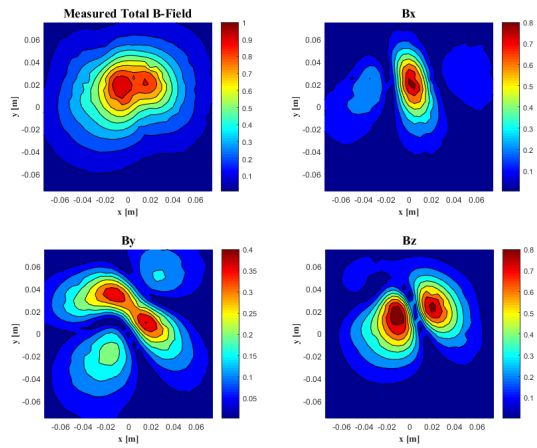


Fig. 10. The measured total magnetic field and the x, y, and z components of the magnetic field generated by DIV/ADD on the FPGA board.

As Fig. 9 illustrates, the algorithm determined two sources for DIV/ADD. Both sources are located near the FPGA's decoupling capacitors. These sources are likely caused by variations in the current being drawn by the FPGA as it switches between executing DIV and ADD. The results for DIV/SUB were nearly identical to the results for DIV/ADD (two sources located at the same locations). This similarity is unsurprising since, on the Cyclone II, SUB is a pseudo-instruction for ADD. To demonstrate the accuracy of the

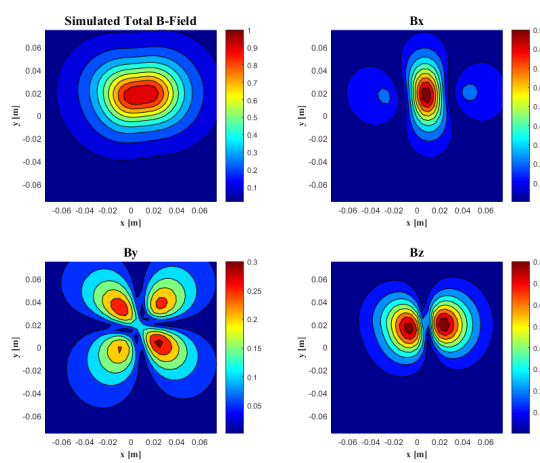


Fig. 11. The simulated total magnetic field and the x, y, and z components of the magnetic field generated by DIV/ADD on the FPGA board using the optimal location of the sources found by the algorithm.

results for DIV/ADD, magnetic field of the sources located by the algorithm is simulated using ANSYS Maxwell. If the algorithm is accurate, the simulated magnetic fields will be similar to the measured fields. In the simulation, the sources are represented by small loops positioned at the locations and

in the orientations indicated by the algorithm. For simplicity, the board is represented by a finite metallic foil having the same dimensions as the board. To match the measurements, the magnetic field is simulated 3 cm above the board. The total measured magnetic field and the measured x, y, and z components of the magnetic field are shown in Fig. 10, while the simulated total magnetic field and its components are shown in Fig. 11. Comparing the simulated and measured fields illustrates that shape and magnitudes of the fields are very similar. This similarity indicates that the sources found by the algorithm produce a similar magnetic field over the entire area of the board and not only at the points used by the algorithm.

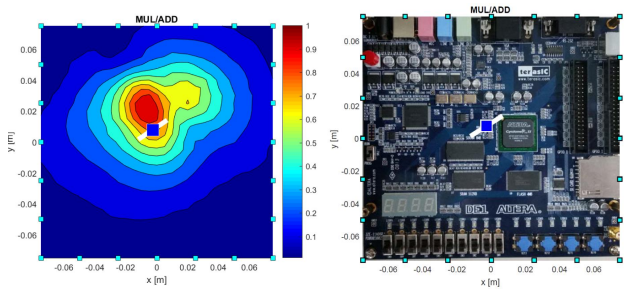


Fig. 12. (left) Total measured magnetic field for MUL/ADD with the location of the source; (right) the location of the source for MUL/ADD on the FPGA board.

Next, the measurements taken when the FPGA executes MUL/ADD are evaluated. As shown in Fig 12 (left), the algorithm identified one dominant source. This result contrasts with the two sources found for DIV/ADD, but it is not surprising: in [7], we have shown that DIV instruction has much higher power consumption compared to ADD, SUB, and MUL. Fig 12 (right) shows that the physical location of the source found for MUL/ADD is near one of the FPGA's decoupling capacitors.

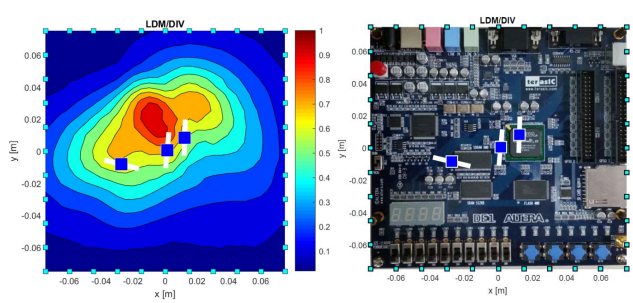


Fig. 13. (left) Total measured magnetic field for LDM/DIV with locations of the sources; (right) locations of the sources for LDM/DIV on the FPGA board.

Next, we evaluate the measurements taken for LDM/DIV. The measured magnetic fields and the sources determined by the algorithm are shown in Fig. 13. Comparing LDM/DIV to DIV/ADD highlights both the similarities and differences between the on- and off-chip instructions. Like the findings for the on-chip pairs of instructions, the localization algorithm identified two sources near the decoupling capacitors at the upper left corner of the FPGA. This result is expected since DIV is still being executed on the FPGA. However, unlike findings for the on-chip instructions, the algorithm found a third source located much further away from the FPGA, near the SDRAM chip that serves as the FPGA's external memory. This source is caused by the FPGA communicating with the SDRAM when executing the off-chip store.

D. Localization of Sources Created by Instructions Modulated onto FPGA Processor Clock

As discussed in Section II, the processor clock signal can be modulated by periodic activity in an executed program. To generate the modulated emanations, the FPGA is again programmed to execute an alternating pair of instructions. However, instead of measuring the emanations at the alternation frequency, measurements are taken near the frequency of the FPGA's clock. Since the signal at the clock frequency is modulated, there are upper and lower side-bands at frequencies $+f_{alt}$ and $-f_{alt}$ away from the clock frequency. Measurements of the side-bands are used by the algorithm to determine the source locations. For all the following measurements, the FPGA's processor clock operates at 50 MHz, and f_{alt} is 20 kHz.

It should be noted that for the following section the algorithm did not use the measurements taken along the outer edge of the board to determine the source locations. Instead the algorithm used points located along a smaller 10 cm by 10 cm square contained within the area of the FPGA. This change was made because the magnitude of the magnetic field along the edges was too low to distinguish from noise. As a result, points closer to the sources need to be used.

The first pair of instructions evaluated is DIV/ADD. The measured magnetic fields and source locations are shown in Fig. 14 (left) and Fig. 14 (right). From the measurements, the algorithm determined that DIV/ADD has two sources at the decoupling capacitors along the top edge of the FPGA.

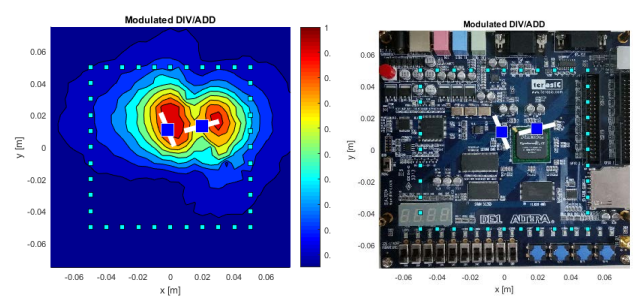


Fig. 14. (left) Total measured magnetic field for modulated DIV/ADD with locations of the sources; (right) locations of the sources for modulated DIV/ADD on the FPGA board.

The next instruction pair measured is LDM/LDL1. The measured magnetic field and the source locations are shown in Fig. 15. As the figure demonstrates, the algorithm has identified two sources, one at the decoupling capacitors near the right edge of the SDRAM and the other at the decoupling capacitors in between the FPGA and SDRAM.

E. Localization of Sources on the Olimex Board

In this subsection, the localization results when the Olimex board executes MUL/ADD and MUL/SUB are presented. The DIV instruction is not used because the device does not have a division instruction. The alternation frequency for all measurements is again 156 kHz. Here, we illustrate how our localization algorithm works on a more complex board that

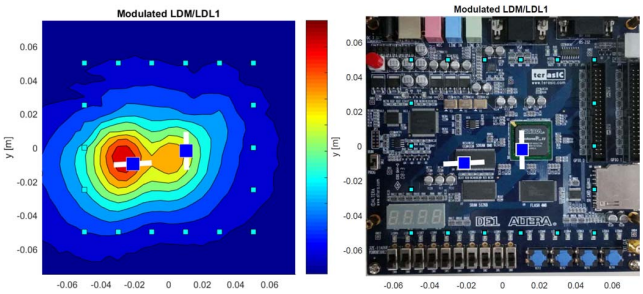


Fig. 15. (left) Total measured magnetic field for modulated LDM/LDL1 with locations of the sources; (right) locations of the sources for modulated LDM/LDL1 on the FPGA board.

not only runs our application, but also has an operating system active. The results again demonstrate that the model is able to locate the sources of instruction-dependent emanations.

The measured total magnetic field of the MUL/ADD instruction and the sources found by the localization algorithm are shown in Fig. 16 (left). From Fig. 16 (right) we can see that one source is located at the bottom left part of the board, near the power supply circuitry. A second source is located near the center of the board, between the processor and its decoupling capacitors.

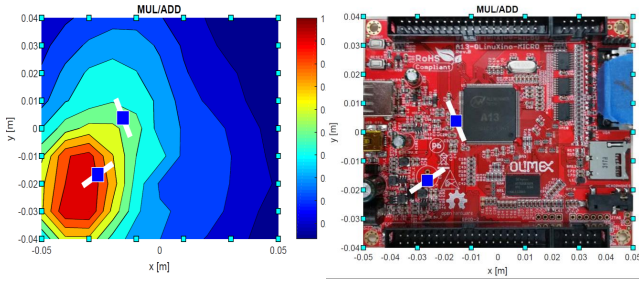


Fig. 16. (left) Total measured magnetic field for MUL/ADD with locations of the sources; (right) locations of the sources for MUL/ADD on the Olimex board.

Next, the magnetic field when the Olimex board executes MUL/SUB is shown in Fig. 17 (left). The sources determined from the measurements are shown in Fig 17 (right). Comparing the source locations in Fig. 17 (right) to Fig 16 (right) demonstrates that the locations of the sources for MUL/SUB are close to the sources for MUL/ADD, near the processor's decoupling capacitors and the power supply circuitry.

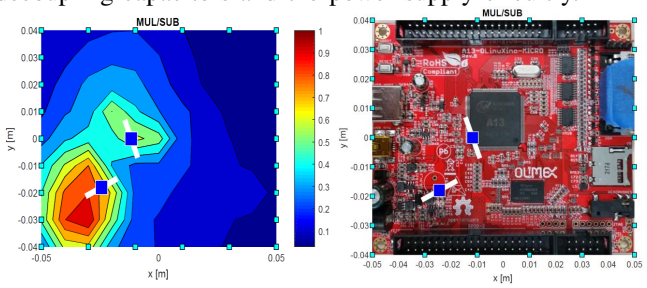


Fig. 17. (left) Total measured magnetic field for MUL/SUB with locations of the sources; (right) locations of the sources for MUL/SUB on the Olimex board.

VI. Conclusions

This paper proposes a method for efficient identification of instruction-dependent sources on a printed-circuit board (PCB) by localizing magnetic field sources from a limited number of measurements around the PCB. The localization results are first verified using simulations, then tested when noise is added to the simulation results, and finally verified against measurements on FPGA and IoT development boards. The results show that the number of strong magnetic field sources on a board depends on the instructions used to excite the board. Furthermore, the results show that the proposed localization algorithm can accurately identify those sources, regardless of the frequency at which the measurements are conducted and the instruction pairs that are executed. Finally, in comparison with the scanning all over the PCB, our method achieves a 15-fold decrease of the overall measurement time.

References

[1] M. G. Kuhn, "Compromising emanations of lcd tv sets," *IEEE Trans. on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 564–570, June 2013.

[2] Y. I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J. L. Danger, "Analysis of electromagnetic information leakage from cryptographic devices with different physical structures," *IEEE Trans. on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 571–580, June 2013.

[3] H. Sekiguchi and S. Seto, "Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage," *IEEE Trans. on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 547–554, June 2013.

[4] D. Agrawal, B. Archambeult, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2002*, 2002, pp. 29–45.

[5] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," in *2010 IEEE International Symposium on Electromagnetic Compatibility*, July 2010, pp. 121–126.

[6] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2001*, 2001, pp. 251–261.

[7] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *IEEE Trans. on Electromagnetic Compatibility*, vol. 56, no. 4, pp. 885–893, Aug 2014.

[8] HINT-PROJECT, "Holistic Approaches for Integrity of ICT- Systems," 2012. [Online]. Available: http://cordis.europa.eu/project/rcn/105381_en.html

[9] J. Balasch, B. Gierlichs, and I. Verbauwhede, "Electromagnetic circuit fingerprints for hardware trojan detection," in *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Aug 2015, pp. 246–251.

[10] P. Maheshwari, V. Khilkevich, D. Pommerenke, H. Kajbaf, and J. Min, "Application of emission source microscopy technique to emi source localization above 5 GHz," in *Electromagnetic Compatibility (EMC), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 7–11.

[11] P. Maheshwari, H. Kajbaf, V. V. Khilkevich, and D. Pommerenke, "Emission source microscopy technique for emi source localization," *IEEE Trans. on Electromagnetic Compatibility*, vol. 58, no. 3, pp. 729–737, 2016.

[12] A. Gorbunova, A. Baev, M. Konovalyuk, and Y. Kuznetsov, "Localization of cyclostationary emi sources based on near-field measurements," in *Electromagnetic Compatibility (EMC), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 450–455.

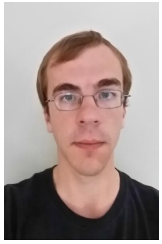
[13] M. Prvulovic, A. Zajic, R. L. Callan, and C. J. Wang, "A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems," *IEEE Trans. on Electromagnetic Compatibility*, vol. 59, no. 1, pp. 34–42, Feb 2017.

[14] J. A. Nelder and R. Mead, "A simplex method for function minimization," *The Computer Journal*, vol. 7, no. 4, pp. 308–313, 1965.

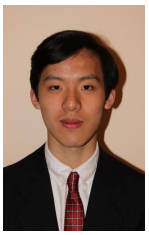
[15] J. Robinson and Y. Rahmat-Samii, "Particle swarm optimization in electromagnetics," *IEEE Trans. on Antennas and Propagation*, vol. 52, no. 2, pp. 397–407, Feb 2004.

[16] A. R. Djordjević, M. B. Baždar, V. V. Petrović, D. I. Olćan, T. K. Sarkar, and R. F. Harrington, *AWAS for Windows: Analysis of Wire Antennas and Scatterers, Software and User's Manual*. Boston:Artech House, 2002.

[17] M. I. Montrose, "How decoupling capacitors may cause radiated emi," in *Electromagnetic Compatibility Symposium-Perth (EMCSA), 2011*. IEEE, 2011, pp. 1–4.



Frank Werner received his B.S. degree (2013) and his M.S. (2016) in electrical engineering from Auburn University, Alabama. Currently, he is completing his PhD in electrical engineering are Georgia Institute of Technology. His research interests include electromagnetic compatibility and applied electromagnetics.



Derrick Albert Chu was born in Albany, NY, in 1993. He received his B.S. degree in electrical engineering from the University of California Los Angeles (UCLA) in 2015 and his M.S degree in electrical engineering from Georgia Institute of Technology in 2017. He is currently working towards the Ph.D. degree at Georgia Institute of Technology. His research interests include wireless communications and applied electromagnetics.

Antonije R. Djordjević was born in Belgrade, Serbia, on April 28, 1952. He received the B.Sc., M.Sc., and Ph.D. degrees from the School of Electrical Engineering, University of Belgrade, in 1975, 1977, and 1979, respectively. In 1975, he joined the School of Electrical Engineering, University of Belgrade, as a Teaching Assistant. He was promoted to an Assistant Professor, Associate Professor, and Professor, in 1982, 1988, and 1993, respectively. In 1983, he was a Visiting Associate Professor at Rochester Institute of Technology, Rochester, NY. In 1997, he became a Corresponding Member of the Serbian Academy of Sciences and Arts, and he became a full member in 2006. His main area of interest is numerical electromagnetics, in particular applied to fast digital signal interconnects, wire and surface antennas, microwave passive circuits, and electromagnetic-compatibility problems.

Dragan Olćan (S'05-M'09) is an Associate Professor at the School of Electrical Engineering, University of Belgrade, Serbia. At the same school he received his B.Sc. (5 years), M.Sc., and Ph.D. degrees in 2001, 2004, and 2008, respectively. He is a coauthor of three commercial electromagnetic software codes, fifteen journal papers, more than seventy conference papers, and seven university textbooks. His main research interests are: numerical electromagnetic analysis, optimization algorithms applied to electromagnetic design, and electromagnetic compatibility testing.

Milos Prvulovic (S'97-M'03-SM'09) received the B.Sc. degree in electrical engineering from the University of Belgrade in 1998, and the M.Sc. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 2001 and 2003, respectively. He is a Professor in the School of Computer Science at the Georgia Institute of Technology, where he joined in 2003. His research interests are in computer architecture, especially hardware support for software monitoring, debugging, and security.

Dr. Prvulovic is recipient of the following awards/honors: NSF CAREER Award (2005), Best Paper Award at the 49th Annual IEEE/ACM International Symposium on Microarchitecture, 2016, Distinguished Alumni Educator Award, 2012, from the Department of Computer Science at the University of Illinois at Urbana-Champaign, Hesburgh Teaching Fellowship, 2010-2011, Intel PhD Fellowship, 2002, and W.J. Poppelbaum Memorial Award, 2001.

Alenka Zajić (S'99-M'09-SM'13) received the B.Sc. and M.Sc. degrees form the School of Electrical Engineering, University of Belgrade, in 2001 and 2003, respectively. She received her Ph.D. degree in Electrical and Computer Engineering from the Georgia Institute of Technology in 2008. Currently, she is an Associate Professor in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Her research interests span areas of electromagnetics, wireless communications, signal processing, and computer engineering.

Dr. Zajić is the recipient of the following awards: NSF CAREER Award (2017), Best Paper Award at the 49th Annual IEEE/ACM International Symposium on Microarchitecture, 2016, 2012 Neal Shepherd Memorial Best Propagation Paper Award, the Best Student Paper Award at the IEEE International Conference on Communications and Electronics 2014, the Best Paper Award at the International Conference on Telecommunications 2008, the Best Student Paper Award at the 2007 Wireless Communications and Networking Conference, LexisNexis Dean's Excellence Award 2016, and Richard M. Bass/Eta Kappa Nu Outstanding Teacher Award 2016. She has been an editor for IEEE Transactions on Wireless Communications 2012-2017.