Hindawi Publishing Corporation
International Journal of Reconfigurable Computing
Volume 2012, Article ID 360242, 9 pages
doi:10.1155/2012/360242

Research Article

Blind Cartography for Side Channel Attacks: Cross-Correlation Cartography

Laurent Sauvage, Sylvain Guilley, Florent Flament, Jean-Luc Danger, and Yves Mathieu

Télécom ParisTech, Institut Télécom CNRS LTCI, 46 rue Barrault, F-75634 Paris Cedex 13, France

Correspondence should be addressed to Laurent Sauvage, laurent.sauvage@telecom-paristech.fr

Received 12 July 2011; Revised 20 October 2011; Accepted 27 December 2011

Academic Editor: Kris Gaj

Side channel and fault injection attacks are major threats to cryptographic applications of embedded systems. Best performances for these attacks are achieved by focusing sensors or injectors on the sensible parts of the application, by means of dedicated methods to localise them. Few methods have been proposed in the past, and all of them aim at pinpointing the cryptoprocessor. However it could be interesting to exploit the activity of other parts of the application, in order to increase the attack's efficiency or to bypass its countermeasures. In this paper, we present a localisation method based on cross-correlation, which issues a list of areas of interest within the attacked device. It realizes an exhaustive analysis, since it may localise any module of the device, and not only those which perform cryptographic operations. Moreover, it also does not require a preliminary knowledge about the implementation, whereas some previous cartography methods require that the attacker could choose the cryptoprocessor inputs, which is not always possible. The method is experimentally validated using observations of the electromagnetic near field distribution over a Xilinx Virtex 5 FPGA. The matching between areas of interest and the application layout in the FPGA floorplan is confirmed by correlation analysis.

1. Introduction

Side channel attacks (SCA) and fault injection attacks (FIA) are very efficient techniques to retrieve secret data stored in cryptographic devices such as smartcards. First attacks have been performed globally, for instance by measuring the power consumption (power analysis: PA) [1] of a device under analysis (DUA) or by quickly changing the nominal voltage of its power supply [2]. But best results have then been achieved locally, by using a small EM probe just over the cryptoprocessor (electromagnetic analysis: EMA) [3] or by shooting at it with a laser beam [4, 5]. Indeed, for SCA, such locality permits to solely collect the activity of the cryptoprocessor, instead of gathering the activity of the whole DUA. In the case of FIA, depending on the technology process of the integrated circuit, only one bit of the implementation can be affected. However, the efficiency of these attacks relies on localisation methods which have to pinpoint as accurately as possible the DUA-sensitive areas. Using these localisation methods is mandatory in the case of a cryptographic application embedded in a field Programmable gate array (FPGA) as its regular structure prevents the localisation of sensible modules by optical or electron microscopy. Indeed, the task is easier for most ASICs, where the functional modules stand clearly out from a visual inspection of the layout as rectangular shapes. Some methods have been proposed in the past, illustrated using as observations the near electromagnetic (EM) field radiated by the DUA: an EM probe is moved over the DUA from a position to another one, and for each of them, the temporal variation of the EM field is measured with an oscilloscope. We use once again such cartography procedure in this paper. Furthermore, we note that all previously published localisation methods along with the one in this paper can deal with other physical phenomenons, such as photons emitted by transistors while they commute [6, 7].

Up to now, two strategies have been deployed to locate cryptographic modules within a DUA. They consist in iden-

tifying areas where the physical observations vary according to:

(1) the data processed during an encryption [8, 9] or

(2) the operations performed by the cryptographic module [10], even if this latter is protected against SCA [11].

With the first strategy, two observations are collected for two different plaintexts p_1 and p_2, and their fluctuations are assessed either by looking for the maximum difference in their temporal domain [8] or by calculating the incoherence of the frequency spectrum [9]. The larger the difference is or the lower the incoherence is, the closer to the cryptoprocessor the EM probe is. To improve the accuracy of the method, a third observation but of the same plaintext p_1 can be acquired, with a view to reject the measurement noise [8]. These approaches seem to be the most suitable because statistical tools which are then used, the CPA [12] for example, exploit plaintexts or ciphertexts as well. However, they would be optimal only if and only if the differences in the observations are maximal, which requires that all of the transistors making the datapath of the cryptoprocessor commute. This can happen only if the attacker knows the secret data, obviously the key but also the mask values when the DUA is protected by masking [13, 14], which is possible in the framework of an evaluation but not with a real-world application.

Instead of focusing on the same time slot, that of the encryption, and collecting two observations, the techniques of the second strategy need only one plaintext and take advantage of two or more time slots of a single observation. Typically, if the cryptoprocessor is in idle state, none of its transistors commute and the corresponding activity is at a low level. On the contrary, during an encryption, the activity is expected to be at a high level. Thus, the localisation of the cryptoprocessor can be achieved in the temporal domain by evaluating the difference between these activities [10]. To diminish the impact of the measurement noise, the localisation can be performed in the frequency domain: indeed, the succession of these low and high activity levels yields a special signature in the frequency spectrum [10]. As this succession still occurs for some countermeasures, the second strategy remains valid to localise protected cryptoprocessors. This fact is all the more true with protections using dual-rail with precharge logic (DPL [15]): as they alternate between two phases, namely, precharge and evaluation phases, they "oscillate" at the half of the master clock frequency, a frequential component of great interest for the frequency analysis [11].

Both previous strategies require to identify the time slot of some sensible operations, such as the encryption. This information can be extracted from the implementation netlist or by using simple power analysis (SPA) [1] or simple electromagnetic analysis (SEMA). Nonetheless, exploring the full implementation appears to be complex, at least time consuming and forces it to be partial, focused on few targets. In this paper, we propose a method to *exhaustively* locate the information sources of a DUA, *without preliminary knowledge* about it. This method is described in Section 2. Then, its ability to identify areas of interest, and in particular cryptographic modules, is evaluated in Section 3. Finally, Section 4 concludes this paper and presents some future works and perspectives.

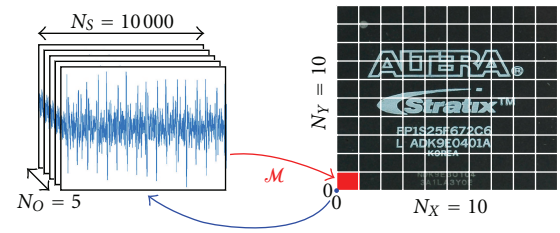

Figure 1: Cartography principle commonly used.

2. Cross-Correlation Cartography

Cartography formally consists in monitoring one or more physical phenomenons at N_P positions over a DUA. Generally, these positions form a 2D grid composed of N_X and N_Y points over, respectively, the X and Y axes. N_X and N_Y could have the same value, for instance 10 as in Figure 1. For each of the $N_P = N_X \times N_Y$ positions, identified by their coordinates (x, y), N_O observations $O^0_{(x,y)}$ of N_S samples n are achieved. They constitute an observations set $\mathcal{O}_{(x,y)} = \{O^0_{(x,y)}, O^1_{(x,y)}, \ldots, O^{N_O-1}_{(x,y)}\}$. In the example of Figures 1 and 4 observations of 10,000 samples are collected per position. To build the final 2D map, each set $\mathcal{O}_{(x,y)}$ has to be reduced to a unique scalar $m_{(x,y)}$. The common usage is to apply a function $\mathcal{M}$ to the corresponding observations $O^0_{(x,y)}, O^1_{(x,y)}, \ldots, O^{N_O-1}_{(x,y)}$. From a "graphical" standpoint, the $m_{(x,y)}$ values, real numbers, are then mapped to colors according to a user-defined scale.

The localisation method we propose in this paper is motivated by the fact that the observation of a physical phenomenon depends on the time and on the space. In the SCA topic, the physical phenomenon we consider is the emanation of a digital integrated circuit. As the state of this circuit changes from a synchronization clock cycle to another one, the observations are made of successive peaks. The amplitude of each one of these peaks

(i) varies in the time according to the data manipulated by its source (see for instance Figure 7);

(ii) decreases when the distance between the source and the observation point increases.

In consequence, sources carrying distinct information generate physical phenomenons whose temporal variations look completely different, that is, *uncorrelated*. At the opposite, observations gathered at positions close to each other, and in particular at positions which are themselves close to a source, look very alike. Thus, to locate these sources, we collect a single observation $O^0_{(x,y)}$ per (x, y) position, then estimate the similarity level between all of these observations. While the methods presented in Section 1 consider (through the $\mathcal{M}$ function, see Figure 1) each observations set $\mathcal{O}_{(x,y)}$ independently from the other, we use conjointly all of them.

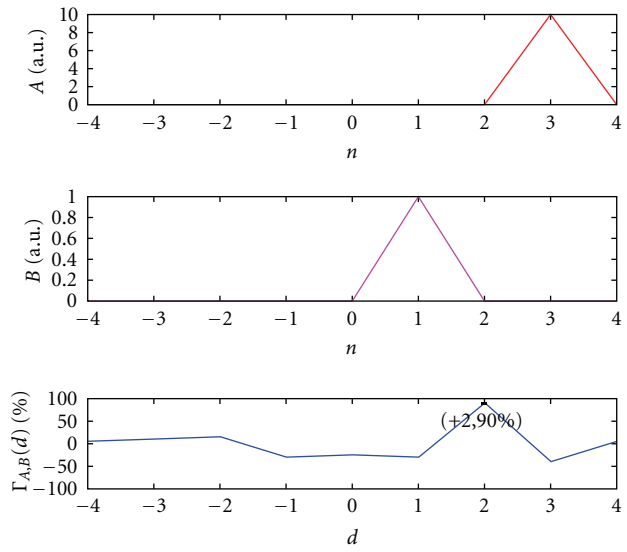

Figure 2: From top to bottom: one reference signal A, the same B but with a lower amplitude and delayed by two samples, and their normalized cross-correlation function $\Gamma_{A,B}(d)$.

The first step of our technique consists in taking each observation $O^0_{(x,y)}$ as a reference, then looking for the maximum of normalized cross-correlation (abridged NXC) between this reference and the other observations. The NXC function is defined as

$$\Gamma_{A,B}(d) = \frac{\operatorname{cov}(A, B_d)}{\sigma_A \cdot \sigma_B} = \frac{\sum_{n=d}^{d+\inf(N_A,N_B)-1} \left(A(n) - \overline{A(n)}\right) \cdot \left(B(n-d) - \overline{B(n)}\right)}{\sqrt{\sum_{n=0}^{N_A-1} \left(A(n) - \overline{A(n)}\right)^2} \cdot \sqrt{\sum_{n=0}^{N_B-1} \left(B(n-d) - \overline{B(n)}\right)^2}}. \quad (1)$$

In (1), $\operatorname{cov}(\cdot,\cdot)$ stands for the covariance, A and B are two observations (at two different points), which, respectively, have N_A and N_B temporal samples, whose mean values are $\overline{A(n)}$ and $\overline{B(n)}$, and whose standard deviations are σ_A and σ_B. B_d means that a delay d belonging to the interval from $-(N_B - 1)$ to $N_A - 1$ is applied to B. From a "graphical" standpoint, the waveform of B is shifted to the right along the temporal X-axis, or in other words the origin $n = 0$ of B is moved to $n = m$. We simply abridge A_0 as A and note that $\sigma_{B_d} = \sigma_B$ because the standard deviation is considered over the complete waveform (and is thus independent of the offset d). Figure 2 shows the variations of the NXC function $\Gamma_{A,B}(d)$ according to the d values, when A and B are two signals with an identical shape, but distinct amplitudes, are delayed by two samples. The maximum value of $\Gamma_{A,B}(d)$ indicates that A and B are 90% similar, while the index of this maximum, 2, provides the sample delay between A and B. The value of $\Gamma_{A,B}(d)$ does not reach 100% because of computational side-effects: the X-axis is not infinite but bounds to $[-4; +4]$.

To briefly illustrate the result of such computation, we provide two NXC maps on Figure 3. The first one, (a), has been obtained considering the center of the map as the reference point. Maximum correlation values are at a very low level, lightly positive in red on the map, or negative in blue, except for the reference point, which by definition is 100% correlated to itself and takes the yellow point in the center. It does not identify a source of interest, because it is insulated. On the second map, (b) of Figure 3, an area of high correlation (in yellow) stands out around the reference point located at $X = -7.90$ mm and $Y = 12.0$ mm and is marked with a white cross. This zone has a size greater than the actual active logic in the FPGA and notably extends outside the silicon chip's boundary, depicted in a white dashed line. The diffusion of the EM field accounts for this extension of a couple of millimeters around the radiating logic. Indeed, in our setup, the distance between the loop sensor and the silicon surface is roughly speaking equal to 2 mm. Above, a second area emerges in blue, with a negative correlation value, as the observations correspond to EM field measurements, these ones, and in turn the correlation values, may be of opposite sign. But in reality, this second blue area contains the same information as the first yellow area does. Therefore, to prevent such artifact, we now consider the *absolute* maximum values of the normalized cross-correlation function.

Each observation gathered at a position of the 2D grid become in turn a reference observation, we finally collect N_P NXC maps. Most of them are alike, as computed at neighbouring points, close to physical sources. The second step of our technique aims at grouping them. For this purpose, we need once again a correlation estimator, but this time, as we manipulate maps, this one should take into account the two dimensions x and y. This bidimensional estimator, namely, $\Gamma^{2D}_{M,N}(p,q)$, is defined as:

$$\Gamma^{2D}_{M,N}(p,q) = \frac{\operatorname{cov}\left(M, N_{(p,q)}\right)}{\sigma_M \cdot \sigma_N}, \quad (2)$$

where

$$\operatorname{cov}\left(M, N_{(p,q)}\right) = \sum_{x=p}^{x_{\max}} \sum_{y=q}^{y_{\max}} \left(M(x,y) - \overline{M(x,y)}\right) \cdot \left(N(x-p, y-q) - \overline{N(x,y)}\right),$$

$$\text{with } x_{\max} = p + \inf\left(N_{X_M}, N_{X_N}\right) - 1$$

$$\text{and } y_{\max} = q + \inf\left(N_{Y_M}, N_{Y_N}\right) - 1,$$

$$\sigma_M = \sqrt{\sum_{x=0}^{N_{X_M}} \sum_{y=0}^{N_{Y_M}} \left(M(x,y) - \overline{M(x,y)}\right)^2},$$

$$\sigma_N = \sqrt{\sum_{x=0}^{N_{X_N}} \sum_{y=0}^{N_{Y_N}} \left(N(x-p, y-q) - \overline{N(x,y)}\right)^2}. \quad (3)$$

In this equation, M and N are two maps, of N_{X_M} and N_{X_N} points on x, N_{Y_M} and N_{Y_N} points on y, whose mean values

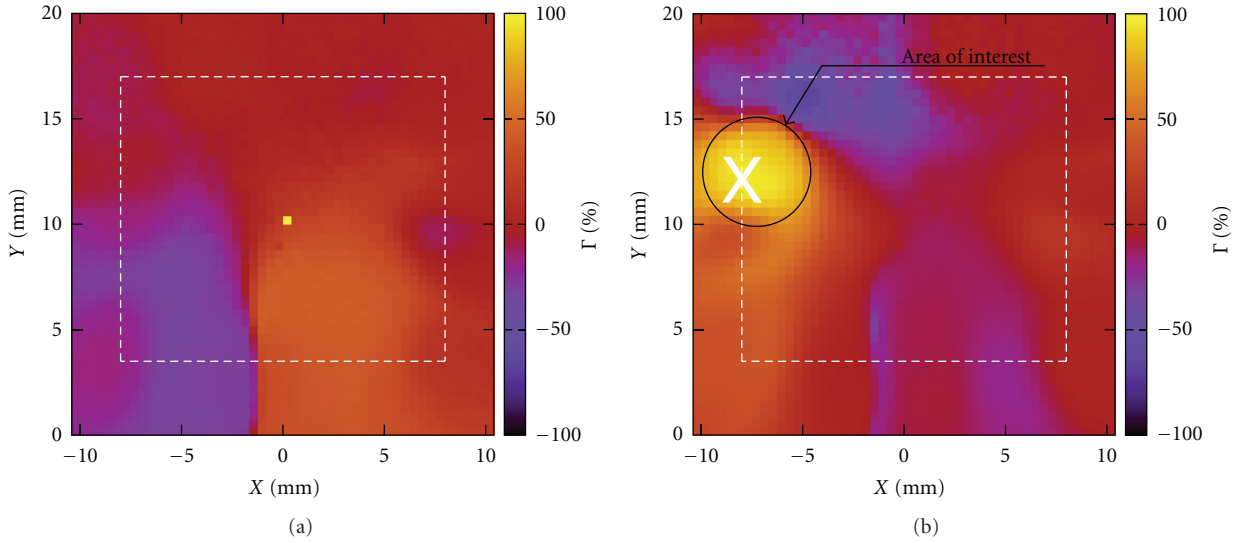

Figure 3: Normalized cross-correlation maps obtained when the reference point, marked with a white cross, is useless (a) or of interest (b).

are $\overline{M(x,y)}$ and $\overline{N(x,y)}$ and standard deviations σ_M and σ_N. $N_{(p,q)}$ means that a spacial offset is applied to the map N, so that its origin point $(0,0)$ is moved to (p,q). This offset is useful when the objective is to find the location of a small pattern within a reference map. In this paper, as we compare maps with identical size, p and q are set to zero. As previously, we fix a reference map, then we look for the maximum of the absolute value of $\Gamma^{2D}_{M,N}(p,q)$. If this maximum is greater than a user-defined threshold, maps are considered as identical and grouped in the same list. Every list is called an area of interest.

To finish the analysis, one map per list has to be extracted. It could be randomly chosen, but we suggest to select the map for which the number of points with a value above under, respectively, a user-defined threshold is the greatest. The corresponding map is the one with the widest, nearest area. The full method is summarized by the Algorithm 1. In this algorithm, the selection of areas of interest is represented by a function called "*extract*."

3. Experimental Results

To evaluate the efficiency of our method, we have used it against an FPGA-based cryptoprocessor performing the simple and triple Data Encryption Standard (3DES) [16], and protected by first-order Boolean masking [13, 14]. In practice, we have implemented the same masking scheme as in [17]. We concur this design is obsolete for at least two reasons. First of all, DES has been replaced by the Advanced Encryption Standard (AES) [18] since the year 2001. Second, the employed masking scheme is not robust against High-Order Side Channel Attack (HO-SCA) [17, 19]. Nonetheless, the objective of this section is not to come up with a new attack to break a still considered invulnerable countermeasure, but to experimentally prove that our method identifies areas of interest, and in particular two sensible 64-bit registers, LR and MASK, carrying respectively the masked value and the mask itself.

To make the experiment easier, we have constrained their placement so that they may fit in rectangular areas, themselves placed at the opposite sides of the FPGA. As depicted by Figure 4, MASK is at the top left hand corner, while LR is at the bottom right hand corner. Splitting these registers in such a way has spread the routing of the 3DES cryptoprocessor datapath all over the FPGA. Therefore, in a view to keep the other components of our implementation visible, for the 3DES datapath, only its logic cells are displayed. They appear as black dots in the upper half part of the floorplan. The KEY scheduling block is at the bottom right of Figure 4, in salmon, while the 3DES CONTROLler, in green, is in the middle, on the left. Close to this latter, we find a 6502 CISC CPU in olive and an UART in turquoise. All previous components share a VCI bus along with its memories, in gold in Figure 4. This real-life application has been programmed into a Xilinx [20] Virtex 5 FPGA, whose metallic lid has been removed with a cutter, as shown in Figure 5. This way, not only we can reduce the analysis area strictly to the FPGA silicon die, but the signal to noise ratio is also greatly improved.

Observations have been acquired using a 2 mm diameter EM probe, a 3 GHz bandwidth 30 dB gain preamplifier, and an Agilent [21] Infiniium 54854 oscilloscope, whose bandwidth and sampling rate have been set up to, respectively, 3 GHz and 10 GSa/s. The EM probe has been moved following a 25×25 points grid, per step of 480 μm along the X-axis, and 400 μm along the Y-axis. The grid is rather rectangular, since we covered the whole silicon die of the Virtex 5 (refer to Figure 5): 12 mm wide and 10 mm high. Then, maps have been grouped together according to a threshold of 90%, that is, two maps whose 2D cross-correlation coefficient is greater than 90% are considered as identical and gathered in the same list. Finally, we have counted for each map the number of points with a correlation level above 90%. From each list,

Require: One observation per point
Ensure: List of identical maps
  For each 2D grid point (x, y) **do** {Fixed reference point A}
    {/* Looping over all fixed reference points A */}
    $x\ ref \leftarrow x$
    $y\ ref \leftarrow y$
    for each 2D grid point (x, y) **do**
      {/* Looping over all mobile points B */}
      $m(x, y) \leftarrow \max_d(|\Gamma_{O(x\ ref, y\ ref), O(x,y)}(d)|)$
    end for
    $map(x\ ref, y\ ref) \leftarrow m$
  end for
  $i \leftarrow 0$ {/* Index of areas of interest */}
  for each 2D grid point (x, y) **do**
    {/* Looping over all fixed reference points A */}
    $x\ ref \leftarrow x$
    $y\ ref \leftarrow y$
    $list[i] \leftarrow map(x\ ref, y\ ref)$
    for each 2D grid point (x, y) **do**
      {/* Looping over all mobile points B */}
      $M_r \leftarrow map(x\ ref, y\ ref)$
      $M_c \leftarrow map(x, y)$
      if $M_c \notin list$ and $\max(|\Gamma^{2D}_{M_r, M_c}(0, 0)|) > threshold$ **then**
        $list[i] \leftarrow map(x, y)$
      end if
    end for
    $i \leftarrow i + 1$
  end for
  for $j = 0$ to i **do**
    $area(j) \leftarrow extract\ (list[j])$
  end for

Algorithm 1: Algorithm for grouping maps per area of interest.

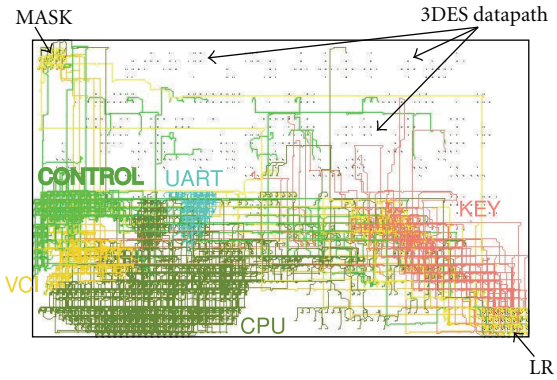

Figure 4: Floorplan of the cryptographic application under ISE floorplanner.

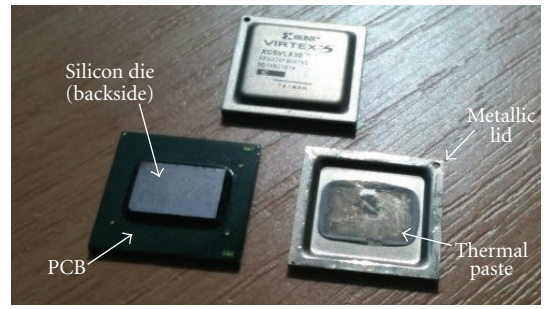

Figure 5: Photograph of the FPGA chip whose cryptographic modules are to be located by cross-correlation cartography.

we have extracted only the map with the greatest number of such points.

Proceeding this way, we have obtained eleven areas of interest. The nine most significant ones are reported on Figure 6, with a disposition in the page that reflects their location within the FPGA. As in Figure 3, reference points are marked with a white cross. The maps (a) and (i) pinpoint two areas in the top left hand and bottom right hand corners. At first sight, they correspond to the two sensible registers LR and MASK. To confirm this, we have conducted large acquisition campaigns of 1,000 observations per point, then computed for each of them the CEMA factor, that is, CPA (Correlation Power Analysis) with electromagnetic waves. We denote by ρ this CEMA factor, to distinguish it from Γ, the NXC coefficient defined in (1). Note that we use data

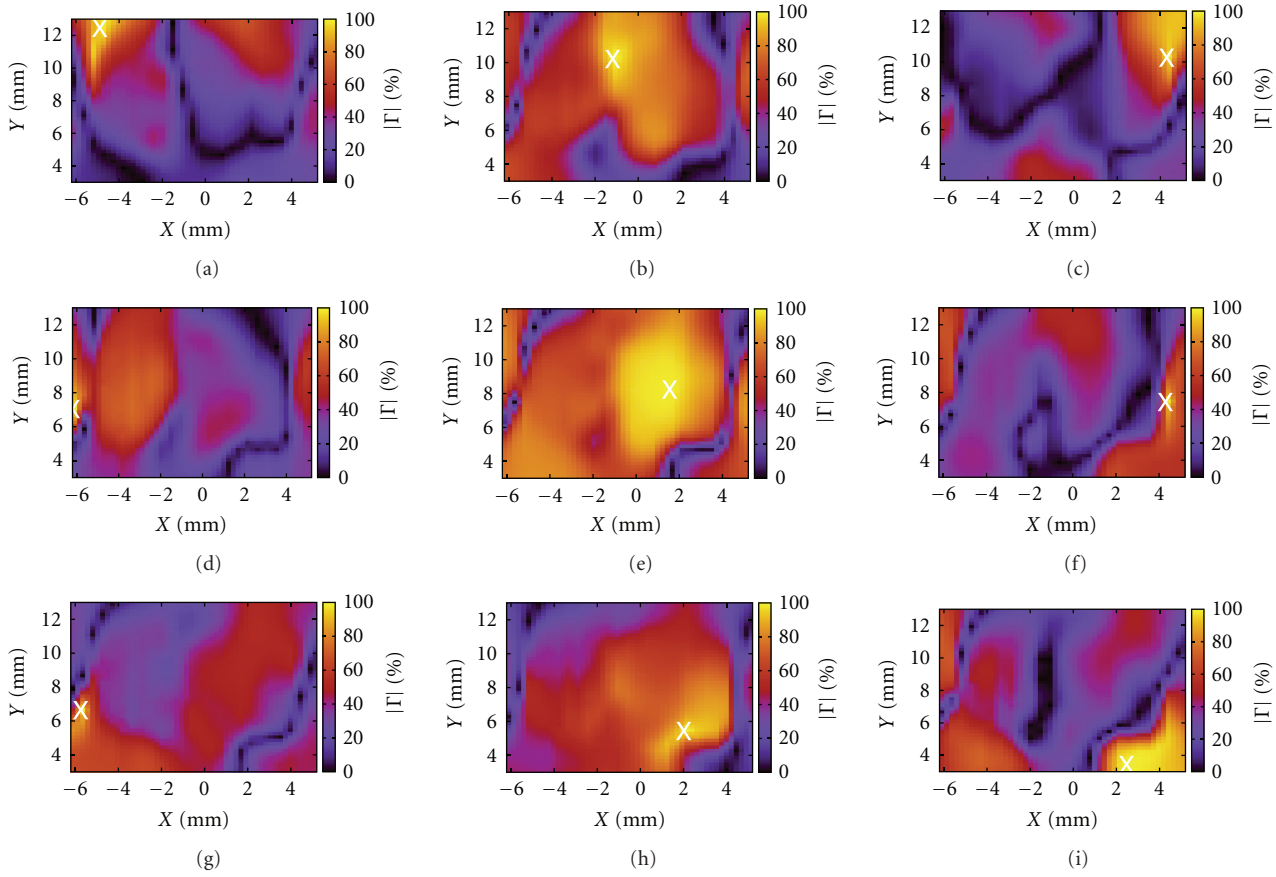

FIGURE 6: Some maps obtained by cross-correlation. The white cross indicates the point of greatest Γ.

normally not accessible to an attacker such as the mask's value: this is, however, possible in an evaluation context. The resulting maps for the MASK and LR registers are depicted by Figure 8. The CEMA clearly identifies that area of interest (a) is correlated with the mask and that area (i) is correlated with the masked data. In these two CEMA maps, the point with the maximum ρ correlation is marked with a white cross. This location coincides almost exactly with that of maximum Γ in the NXC maps. Hence, the proof that the methodology succeeds in insulating areas of consistent activity. Therefore, our main objective has been successfully reached. This result is very precious to continue with a HO-SCA (second order) taking advantage of this spatial diversity: LR is leaking more about the masked data, whereas MASK discloses information more related to the mask. HO-SCA such as those based on correlation reviewed in [22] or the one based on information theory in [23] would advantageously combine observations over these points. Identifying the other areas is not trivial as their shapes do not fit the arrangement of Figure 4. Indeed, EM radiations are generally more likely due to the power grid and the clock tree of the FPGA [10] than to its logic cells and routing paths.

To complement the analysis, Figure 7 delivers the output voltage of the EM probe when this latter is just over the points of interest. Except for the map (f), the 16 rounds of the DES encryption are neatly visible in the right hand part of the observations. The 16 peaks amplitude varies in time, but not in the same way from a position to another one, which confirms that we observe the activity of distinct elements. We guess that the observation that coincides with the locations:

(i) (e) and/or (h) may be due to the key scheduling;

(ii) (d) and/or (g) to some reads/writes on the VCI bus;

(iii) (b) and/or (c) and/or (f) to some combinatorial functions in the 3DES datapath, such as exclusive logical OR.

We insist that our blind cartography method does not actually distinguish cryptographic blocks from the others. But still, the method has the following interests.

(i) It highlights "equivalent areas" for EMA. Once those areas of interest are localized, the attacker can focus her measurements on them. In our example, this reduces the number of positions from $25 \times 25 = 625$ to only 11.

(ii) Applied to the second-order attack of a first-order masking scheme, the number of combinations to be tested to match the mask and the masked data activity is only $\binom{11}{2} = 55$. Without NXC, the number of couples to test would be equal to $\binom{25 \times 25}{2} \approx 200,000$, which is deterrent for an attacker, but the computational workload is too high.

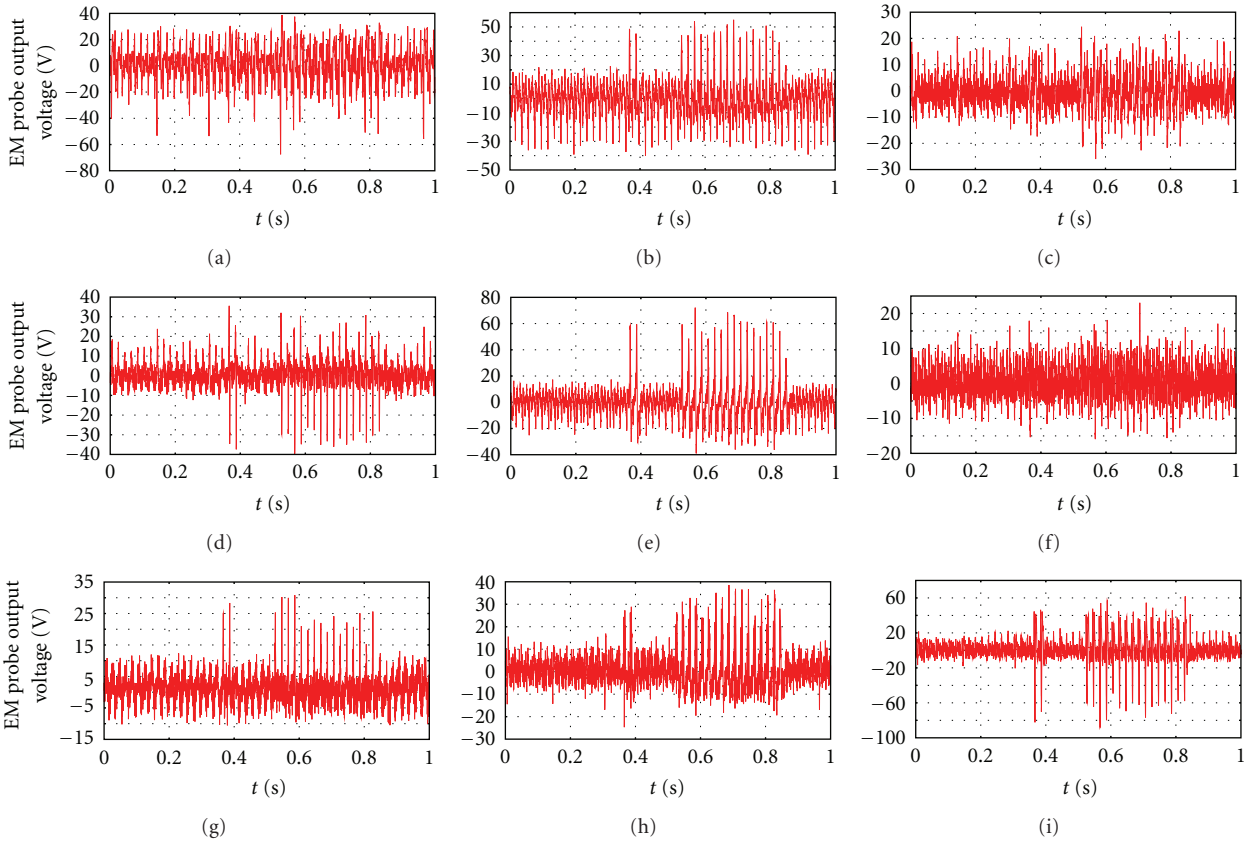

Figure 7: Output voltage of the EM probe when positioned over the points of interest.

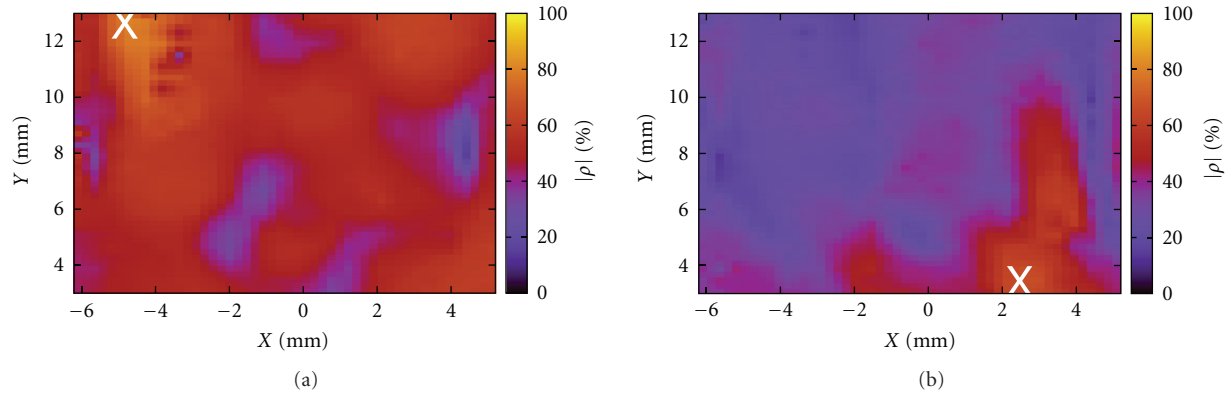

Figure 8: CEMA maps obtained knowing the activity of the MASK (a) and LR (b) registers. The white cross indicates the point of greatest ρ.

4. Conclusion and Future Works

Many implementation-level attacks can be enhanced if the floorplan of the application is known by the attacker. For instance, side-channel measurements can be made less noisy if focused on the most leaking zone, and fault injection attacks (by electromagnetic waves or laser shots) have indeed more chance to succeed in perturbing the adequate resource if positioned well in a vicinity of the zone of influence. As far as ASICs are concerned, the location of each module can be guessed by an optical analysis of chip photographs. Modern ASICs (such as modern smartcards) have their logic dissolved so as to make its analysis intractable. Now, regarding FPGAs, the problem is the same, since the fabric is extremely regular and does not show the location of the user design. In addition, FPGA chips are wider than ASICs, thus the research for sensitive regions is *a priori* more complex.

In this paper, we introduce a novel location method based on cross-correlation of electromagnetic cartographies. It is indeed able to reveal the position of blocks. This shows that the structure of the floorplan shall not be considered confidential in FPGAs, even if the bitstream is confidential

(e.g., encrypted). Then, we experimentally demonstrate that the cross-correlation location method is efficient to pinpoint areas of interest in the context of a protected cryptographic application. This methodology illustrates a new aspect of the wealth of the information carried out by the electromagnetic field leaked by electronic devices. The floorplan reverse-engineering method presented in this paper is an algorithm-agnostic preliminary step that enables the further realization of well-focused electromagnetic analysis attacks aiming this time at extracting secrets. We have exemplified this method with the successful localization of the registers that hold the mask and the masked data that are manipulated concomitantly. Being able to record traces from both locations allows for second-order attacks by combination of the twain measurements [24]. Also, the same method could be used to record traces selectively from one half of separable dual-rail logic styles (such as SDDL [25, Section 3.1], DWDDL [26], divided backend duplication [27], partial DDL [28], or PA-DDL [29]) thereby defeating the complementation property of those "hiding" countermeasures.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference Advances in Cryptology (CRYPTO '99)*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397, Springer, Santa Barbara, Cali, USA, 1999.

[2] R. Anderson and M. Kuhn, "Tamper resistance—a cautionary note," in *Proceedings of the 2nd USENIX Workshop on Electronic Commerce (WOEC'96)*, pp. 1–11, USENIX Association, Berkeley, Calif, USA, 1996.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," in *Proceedings of the 3rd International Workshop Cryptographic Hardware and Embedded Systems (CHES'01)*, C. K. Koc, D. Naccache, and C. Paar, Eds., vol. 2162 of *Lecture Notes in Computer Science*, pp. 251–261, Springer, Paris, France, 2001.

[4] M. Agoyan, J.-M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta, and A. Tria, "Single-bit DFA using multiple-byte laser fault injection," in *Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST'10)*, pp. 113–119, 2010.

[5] G. Canivet, J. Clédière, J. B. Ferron, F. Valette, M. Renaudin, and R. Leveugle, "Detailed analyses of single laser shot effects in the configuration of a Virtex-II FPGA," in *14th IEEE International On-Line Testing Symposium, (IOLTS '08)*, pp. 289–294, Rhodes, Greece, 2008.

[6] S. P. Skorobogatov, "Using optical emission analysis for estimating contribution to power analysis," in *Proceedings of the 6th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC '09)*, pp. 111–119, IEEE Computer Society, Lausanne, Switzerland, 2009.

[7] J. Di-Battista, J.-C. Courrège, B. Rouzeyre, L. Torres, and P. Perdu, "When failure analysis meets side-channel attacks," in *Proceedings of the 12th International Workshop Cryptographic Hardware and Embedded Systems (CHES '10)*, Santa Barbara, Calif, USA, 2010.

[8] D. Réal, F. Valette, and M. Drissi, "Enhancing correlation electromagnetic attack using planar near-field cartography," in *Proceedings of the Design, Automation and Test in Europe, (DATE '09)*, pp. 628–633, IEEE, Nice, France, April 2009.

[9] A. Dehbaoui, V. Lomne, P. Maurine, and L. Torres, "Magnitude squared incoherence em analysis for integrated cryptographic module localisation," *Electronics Letters*, vol. 45, no. 15, pp. 778–780, 2009.

[10] L. Sauvage, S. Guilley, and Y. Mathieu, "ElectroMagnetic radiations of FPGAs: high spatial resolution cartography and attack of a cryptographic module," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 2, no. 1, pp. 1–24, 2009.

[11] L. Sauvage, S. Guilley, J.-L. Danger, Y. Mathieu, and M. Nassar, "Successful attack on an FPGA-based WDDL DES cryptoprocessor without place and route constraints," in *Proceedings of the Design, Automation and Test in Europe (DATE'09)*, pp. 640–645, IEEE, Nice, France, April, 2009.

[12] É. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proceedings of the 6th International Workshop Cryptographic Hardware and Embedded Systems (CHES'04)*, vol. 3156 of *Lecture Notes in Computer Science*, pp. 16–29, Springer, Cambridge, Mass, USA, August, 2004.

[13] L. Goubin and J. Patarin, "DES and differential power analysis (The "Duplication" Method)," in *Proceedings of the 1st International Workshop Cryptographic Hardware and Embedded Systems (CHES'99)*, vol. 1717 of *Lecture Notes in Computer Science*, pp. 158–172, Worcester, Mass, USA, August, 1999.

[14] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Proceedings of the 19th Annual International Cryptology Conference Advances in Cryptology (CRYPTO '99)*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 398–412, Springer, Santa Barbara, Calif, USA, August, 1999.

[15] J.-L. Danger, S. Guilley, S. Bhasin, and M. Nassar, "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors," in *Proceedings of the 3rd International Conference on Signals, Circuits and Systems (SCS'09)*, pp. 1–8, IEEE, Jerba, Tunisia, November 2009.

[16] National Institute of Standards and Technology, "Data Encryption Standard (DES): FIPS PUB 46-3," 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. .

[17] E. Peeters, F.-X. Standaert, N. Donckers, and J.-J. Quisquater, "Improved higher-order side-channel attacks with FPGA experiments," in *Proceedings of the 7th International Workshop Cryptographic Hardware and Embedded Systems (CHES '05)*, vol. 3659 of *Lecture Notes in Computer Science*, pp. 309–323, Springer, Edinburgh, UK, 2005.

[18] National Institute of Standards and Technology, "Advanced Encryption Standard (AES): FIPS PUB 197," 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[19] T. S. Messerges, "Using second-order power analysis to attack DPA resistant software," in *Proceedings of the 2nd International Workshop Cryptographic Hardware and Embedded Systems (CHES'00)*, vol. 1965 of *Lecture Notes in Computer Science*, pp. 238–251, Springer, Worcester, Mass, USA, August, 2000.

[20] "Xilinx FPGA designer," http://www.xilinx.com/.

[21] "Agilent Technologies," http://www.home.agilent.com/.

[22] E. Prouff, M. Rivain, and R. Bévan, "Statistical analysis of second order differential power analysis," *IEEE Transactions on Computers*, vol. 58, no. 6, pp. 799–811, 2009.

[23] B. Gierlichs, L. Batina, B. Preneel, and I. Verbauwhede, "Revisiting higher-order DPA attacks: multivariate mutual information analysis," in *Proceedings of the The Cryptographer's Track at RSA Conference (CT-RSA'10)*, vol. 5985 of *Lecture Notes in Computer Science*, pp. 221–234, Springer, San Francisco, Calif, USA, March 2010.

[24] E. Prouff, M. Rivain, and R. Bévan, "Statistical analysis of second order differential power analysis," *IEEE Transactions on Computers*, vol. 58, no. 6, pp. 799–811, 2009.

[25] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'04)*, pp. 246–251, IEEE Computer Society, Paris, France, February 2004.

[26] P. Yu and P. Schaumont, "Secure FPGA circuits using controlled placement and routing," in *Proceedings of the 5th IEEE/ACM international conference on Hardware/software codesign and system synthesis (CODES+ISSS'07)*, pp. 45–50, ACM, New York, NY, USA, 2007.

[27] K. Baddam and M. Zwolinski, "Divided Backend duplication methodology for balanced dual rail routing," in *Proceedings of the Cryptographic Hardware and Embedded Systems (CHES '08)*, vol. 5154 of *Lecture Notes in Computer Science*, pp. 396–410, Springer, Washington, DC, USA, 2008.

[28] J.-P. Kaps and R. Velegalati, "DPA Resistant AES on FPGA Using Partial DDL," in *Proceedings of the 18th IEEE Annual International Symposium on Field-Programmable Custom Computing Machine (FCCM'10)*, pp. 273–280, IEEE Computer Society, Charlotte, NC, USA, May, 2010.

[29] W. He, E. D. L. Torre, and T. Riesgo, "A precharge-absorbed DPL logic for reducing early propagation effects on FPGA implementations," in *Proceedings of the ReConFig*, IEEE Computer Society, Quintana Roo, México, 2011.