A Simulation Methodology for Electromagnetic Analysis and Testing on Synchronous and Asynchronous Processors

Huiyun Li, Simon Moore, A. Theodore Markettos
Computer Laboratory, University of Cambridge
Huiyun.Li@cl.cam.ac.uk

Abstract

A systematic simulation methodology is proposed to identify and assess electromagnetic (EM) leakage characteristics of secure processors. This EM simulation methodology involves current simulation, chip layout parasitics extraction, then data processing to simulate direct EM emissions or modulated emissions. We demonstrate that differential EM analysis (DEMA) of direct emissions and DEMA of envelope detection based amplitude demodulated emissions reveal the same level of leakage as in differential power analysis, while DEMA of product detection based amplitude demodulated emissions reveals increased leakage. A comparison is also made between the EMA on synchronous and asynchronous processors, which indicates that the synchronous processor has data dependent EM emission, while the asynchronous processor has data dependent timing which is visible in DEMA.

1 Introduction

Electromagnetic analysis (EMA) has become an important side channel attack on many cryptographic implementations. EMA could compromise information by analysing the electric and/or magnetic fields emanating from a device. The ability to examine EM emissions of processors through simulation can help identify design flaws, develop countermeasures and assess their effectiveness. This paper presents a systematic simulation methodology to identify EM leakage characteristics of secure processors. We first investigate the types of EM emissions and field sensors in EMA attacks. Then we present our simulation methodology incorporating different types of EM emissions and different field sensors. Finally, we demonstrate simulation results for two processors on our Springbank test chip to compare the EM characteristics of synchronous and asynchronous logic operations.

1.1 Types of EM emissions

There are two categories of EM emissions [1]: **Direct emissions** and **Unintentional emissions**.

Direct emissions are caused by current flow with sharp rising edges. If a current I flows through a long wire, the resultant magnetic field B is defined by Biot-Savart's law to be:

$$B = \frac{\mu_0 I}{2\pi r} \tag{1}$$

where r denotes the distance from the wire and μ_0 is Permeability of a vacuum, a constant equal to $4\pi \times 10^{-7} \frac{H}{m}$. To measure direct emissions from a signal source isolated from interference from other signal sources, one needs to use tiny field probes positioned very close the signal source and use special filters to minimize interference. To get good results may require decapsulating the chip.

Unintentional emissions occur when the current flow of a data signal modulates carrier signals which then propagate into the space. A strong source of carrier signals are the harmonic-rich square-wave signals such as a clock, which may

then be modulated in amplitude, phase or some other manner. The recovery of the data signals requires a receiver tuned to the carrier frequency with a corresponding demodulator.

Exploiting unintentional emissions can be easier and more effective than working with direct emission [1]. Some modulated carriers could have substantially better propagation than direct emission, which may sometimes be overwhelmed by noises. The unintentional emission sensing does not require any intrusive/invasive techniques or fine grained positing of probes.

- Amplitude Modulation

  In a circuit, the data signal couples to a carrier signal (e.g. clock harmonics), due to E field capacitive coupling, H field magnetic coupling, which generates a sum of the two signals. Once these two coupled signals go through a square-law device, such as a transistor, the product of the two signals is generated.

  For instance, an *n*-channel transistor operates in the saturation region where $V_{DS} > V_{GS} - V_{Tn}$, its drain current remains approximately constant as: $I_{DSn(sat)}$ [2]:

$$I_{DSn(sat)} = \frac{\beta_n}{2}(V_{GS} - V_{Tn})^2 \qquad (2)$$

  where the constant β_n denotes the *n*-channel transistor gain factor, V_{GS} denotes the gate-source voltage and V_{Tn} denotes the threshold voltage.

  If the input V_{GS} is a clock signal with a coupled data signal ($V_{GS} = V_{data} + V_{clock}$), in which the square-wave clock signal V_{clock} can be represented as a Fourier series with the fundamental frequency f and all the odd harmonics:
  $V_{clock} = \sum_{n=1,3,5...}^{\infty} \frac{4}{n\pi} \sin(2\pi nft)$.
  The saturation current $I_{DSn(sat)}$ becomes:

  $\frac{\beta_n}{2}[V_{data} + (\sum_{n=1,3,5...}^{\infty} \frac{4}{n\pi} \sin(2\pi nft)) - V_{Tn}]^2$

  Expanded, $I_{DSn(sat)}$ contains items of interest as the product of sinusoidal signals and the coupled data signal: $\sum_{n=1,3,5...}^{\infty} \frac{4}{n\pi} \sin(2\pi nft)V_{data}$.
  This process is amplitude modulation (AM). The coupled data signal V_{data} modulates clock harmonics with diminishing magnitude. When the current $I_{DSn(sat)}$ is picked up by an EM sensor and fed into a bandpass filter tuned to a certain clock harmonic frequency, the signal V_{data} can be recovered. This process is amplitude demodulation.

  AM modulation can also occur in a transistor when the input V_{GS} is itself a square-wave, harmonic-rich signal. For example, if V_{GS1} is 00111100..., while V_{GS2} is 01010101..., then their Fourier series expressions are different. If a demodulator is tuned to one of these carrier frequencies, the difference of the coefficients in the Fourier series can be detected and viewed as a manifestation of the difference in V_{GS1} and V_{GS2}. This type of AM modulation mechanism is dominant for deep-submicron technologies[1] where the saturation current $I_{DSn(sat)}$ and the source-drain voltage V_{GS} follows a linear law rather than the square law.

- Angle Modulation (phase or frequency modulation)

  Coupling of circuits can also result in changes in the angle (frequency or the phase) of the carrier signals. If there is a coupling between a data line and the internal clock circuitry, e.g. its VCO (voltage controlled oscillator), this coupling can affect the output clock frequency by affecting the VCO control voltage. The resulted clock frequency variation may be visible as data-dependent timing in differential EM analysis.

[1] Gate lengths below 0.35 μm are considered to be in the deep-submicron region

1.2 Measurement equipment

A number of sensors can be used to detect electromagnetic fields. They are divided into those detecting electric fields and those detecting magnetic fields in near-field[2], or those detecting far-field EM-field. In EM analysis attacks on small devices with weak EM emissions such as a smart card, near-field sensors are more appropriate.

1.3 Near-field electric field sensors

An example of electric field sensors is a monopole antenna. It generally measures the near-field electric component around a current carrying conductor where $\mathbf{E} \propto I$.

1.4 Near-field magnetic field sensors

Near-field Magnetic field sensors generally measure the near-field magnetic component around a current carrying conductor where $\mathbf{B} \propto I$. There are several types of magnetic field sensors based on different mechanisms as follows.

- Magnetic loop (also referred to as inductive loop)

  The simplest magnetic field sensor is a loop of wire. An EM field is induced in the loop due to a change in magnetic flux through the loop caused by a changing magnetic field produced by an AC current-carrying conductor. This is the transformer effect. The induced voltage is:

  $$V = -\int_S \frac{\partial \mathbf{B}}{\partial t} \cdot d\mathbf{s} \tag{3}$$

  over surface S using area element $d\mathbf{s}$. We can rewrite it into the following equation, saying the measurement output is proportional to the rate of change of the current which causes the magnetic field.

  $$V = M\frac{dI}{dt} \tag{4}$$

  where M denotes the mutual inductance in the loop of wire.

  Hard disk drive write heads are mainly inductive loops.

- Magnetoresistive sensors

  They are used in hard disk drives for reading, made of materials that have resistance linear to the magnetic field ($\mathbf{H}$) [3]. The magnetoresistive probe output is proportional to the magnitude of the field, rather than the rate of change of the magnetic field as in inductive probes.

- Hall probe

  A Hall probe works by way of the Hall effect. Any charged particle moving perpendicular to a magnetic field will have a Lorentz force upon it, given by $F = q(\mathbf{v} \times \mathbf{B})$. However the moving electrons observe an electric field which gives the electrons an electric force in the other direction by $F = q\mathbf{E}$, where $\mathbf{E} = V_{measured}/d$. Thus, $V_{measured} \propto B$. The detectable field range of Hall-effect sensors are above 10 gauss [7], too large to discern EM emission from a chip through ambient noise.

There are also far-field electromagnetic field sensors such as log-periodic antennas. They generally measure far-field electromagnetic fields and often work with other equipment to harness unintentional emissions. For example, an AM receiver tuned to a carrier frequency can perform amplitude demodulation and extract useful information leakage from electronic devices [1].

The above list of field sensors is not exhaustive, but it provides a view that different types of sensors measure different types of field, so that require different means of EM simulations.

[2]Near-field refers to a distance within one sixth of the wavelength from the source ($r < \lambda/2\pi$), while far-field refers to a distance beyond that

2 Simulation for EM analysis

A full 3D nonlinear[3] full-wave simulator incorporating characterised semiconductor behaviour is not available. Our simulation approach is in two parts. The first part is the chip, simulated in **circuit simulators** like SPICE, which is fundamentally flawed because wave coupling is not accurately represented even if transmission lines are used for the interconnects. However, the chip is small enough (compared to the wavelength) to tolerate the errors.

The second part is the package and the printed circuit board (PCB), which can be represented accurately by using a (3D or planar) **EM simulator**. The numerical simulation of full-wave electromagnetic involves solving Maxwell's equations for the electric and magnetic vector fields. Generally speaking, full-wave EM simulations are required when the wavelength is similar to or smaller than the geometric dimensions of the structure. However for a device running at moderate speed, such as a smartcard running at several MHz, with edge rates around several hundred MHz (wavelength at meter or tenth of a meter level), the package size is considered small enough to be modelled with lumped components (R, L or C).

2.1 Simulation methodology

The procedure to perform an EMA simulation on a chip design is shown in Figure 1. The EM analysis simulation flow is similar to that of power analysis which measures the global current of a device. However EM analysis may focus on a smaller block such as the ALU or the memory. A Verilog/Spice co-simulation is chosen to perform the functional/power analysis and to collect current data for later EMA simulation. VCS/Nanosim from Synopsys^{TM} is used in this paper to implement the simulation in which various instructions can be easily executed and modified through testbench files as in Verilog. Accurate current simulation can be achieved in the Spice-deck of Nanosim. The partitioning function of the mix-signal simulator provides an easy means to select the desired block(s) to test.

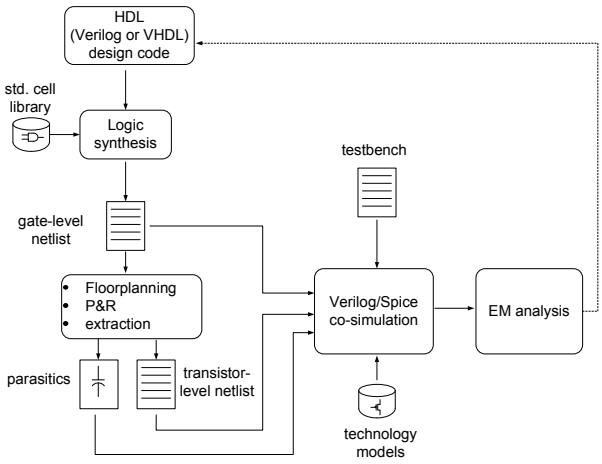

Figure 1: Digital design flow with EM analysis

The collected current data ($Idd(t)$) for the desired block(s) or a whole processor is then processed with Matlab^{TM} to implement DEMA. The data process procedure shown in Figure 2 includes synchronizing and re-sampling that are similar to those in DPA data process. But it also involves steps to perform simulation for EM direct or unintentional emissions. Since EM emissions captured by inductive sensors are proportional to the rate of change of current, the EM simulation involves data manipulation such as differential calculus. If it is a simulation for unintentional EM emissions, other manipulation techniques such as amplitude demodulation are required.

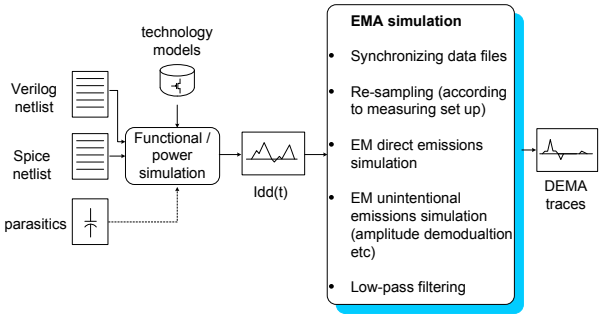

Figure 2: EM analysis simulation procedure

[3] A component is linear if its current is a linear function of the controlling voltage(s), e.g. R. Some examples of nonlinear components are Diode, BJT and MOSFET.

2.2 Low-pass filtering effect of EM sensors

Considering the inductance in inductive sensors and the load resistance from connected instruments (e.g. an amplifier or an oscilloscope), an RL low-pass filterer is formed as shown in Figure 3. Its 3dB cutoff[4] frequency can be calculated as $f_{cutoff} = R/2\pi L$.

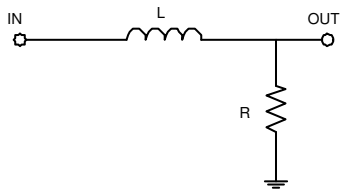

Figure 3: RL low-pass filter

3 Results

3.1 EM measurement results

DEMA measurement has been carried out using the Springbank test chip, fabricated as part of the G3Card project [4, 5]. This contains five processors based on the 16-bit Cambridge Consultants' XAP each in a different design style. The synchronous and secure dual-rail asynchronous XAP processors were used in the following tests.

Two different programs were run on the XAP - the core loop of which was:

```
; positive trigger on IOM[0] output pin
    st      ah,@(0,x)
; load value from memory
    ld      al,@val
; negative trigger on IOM[0] output pin
    st      y,@(0,x)
```

By modifying the data section of the program, the value loaded was set to be 0xFFFF in one program, `LoadFFFF`, and 0x0000 in the other, `Load0`.

[4]The frequency at which the output voltage is 70.7% of the input volatge

For each run, electromagnetic emission is measured and then differential electromagnetic analysis is applied to the traces. Figure 4 shows the results of collecting traces for each operation, averaging the traces over 5000 runs to average out the noise power received, and then subtracting one averaged trace from the other. On the graphs that follow we plot the EM traces of the whole core for `Load0` and `LoadFFFF` (overlapped as the top trace), as well as differential EM (DEM) plot of `1:LoadFFFF-2:Load0` (the middle trace). The lowest curve is I/O signal triggering the oscilloscope.

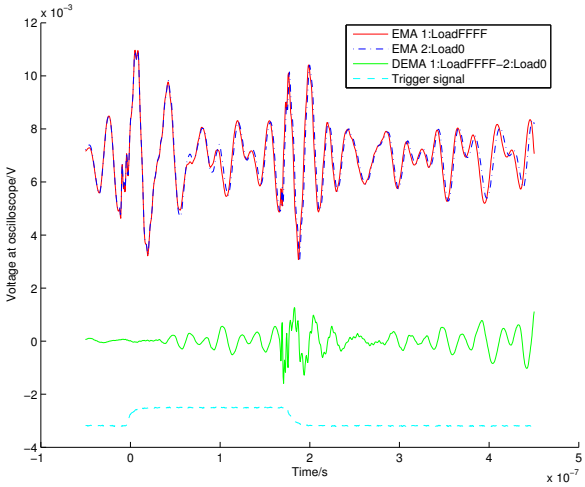

Figure 4: Inductive sensor over secure XAP (dual-rail asynchronous) processor (experimental graph)

The inductive head in use has R = 5.42Ω, L = 9.16μH. When delivering power into a 4KΩ load, the 3dB cutoff is calculated as 70MHz. The measurement results demonstrate the EM traces are around 50MHz, complying to the explanation of the RL low-pass filtering effect in EM sensing.

3.2 EM simulation results

Due to the lack of a Spice model for the memory on the Sprinbank chip, we do not simulate the EMA analysis with `load` instructions as in the above measurement, but use a small `XOR` instruction program to solely test the processors executing logic operations. The `XOR` instruction

program runs twice with different operands:

```
        nop
        nop
        xor       al, @(0,x)
; On first run:  #H'11 xor #H'22
; On second run: #H'33 xor #H'55
        nop
        nop
```

On the first run, H'11 is XORed with H'22. While on the second run, the operands change to H'33 and H'55.

3.2.1 EM simulation on an asynchronous processor

Figure 5 shows the simulated differential power analysis over the DRXAP (dual-rail asynchronous) processor. Figure 6 shows the simulation of EMA with an inductive sensor. Figure 7 shows the simulation of EMA with an inductive sensor plus the amplitude demodulation by the 21st harmonic of the natural operating frequency (The asynchronous XAP executes at a natural speed around 10 to 50MHz. Here we take a carrier whose fundamental is 20MHz).

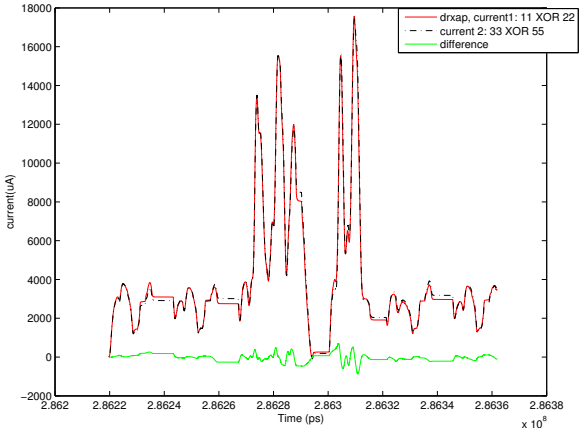

Figure 5: Power simulation: Asynchronous XAP executing XOR

Amplitude demodulation shown in Figure 7 is envelop detection based demodulation and gives the magnitude of differential signals at a similar

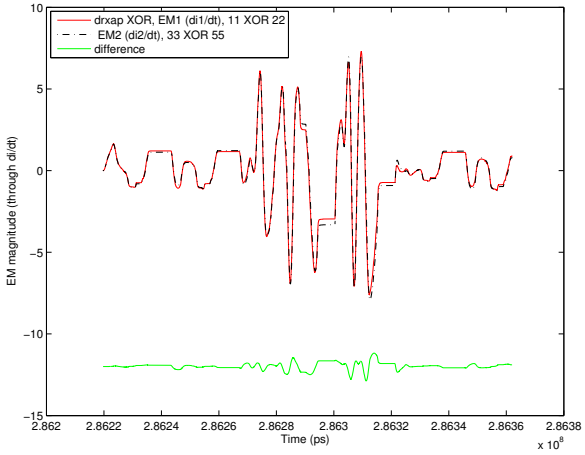

Figure 6: EMA simulation of direct emissions with an inductive sensor: Asynchronous XAP executing XOR

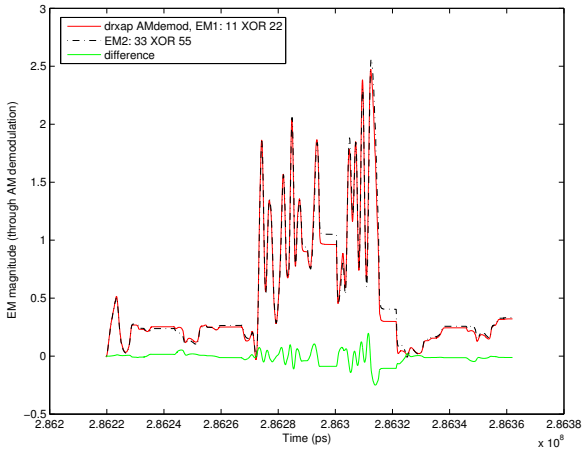

Figure 7: EMA simulation of unintentional emissions, amplitude demodulated by a harmonic of the natural operating frequency of the asynchronous XAP executing XOR

level as in power analysis or in direct emission analysis.

If we do not use an envelop detector, but use a product detector for amplitude demodulation which takes the product of the modulated signal and a tuned frequency, then both the positive and negative going sides of the modulated signal are kept. This *product detection based amplitude demodulation* will reveal greater level of differential signals. The shape and magnitude of the demodulated signals largely rely on the carrier frequency, if the frequency of the modulating signal is close to that of the carrier. A simple example is shown in Figure 8. The top subplot is the modulating signal. The middle subplot is the AM modulation and its product detection based demodulation with a sinusoidal carrier. The pulse appears on the negative side of the modulation, and demodulated as a negative pulse. The bottom subplot in Figure 8 uses another sinusoidal carrier at a higher frequency, and pulse recovered is positive.

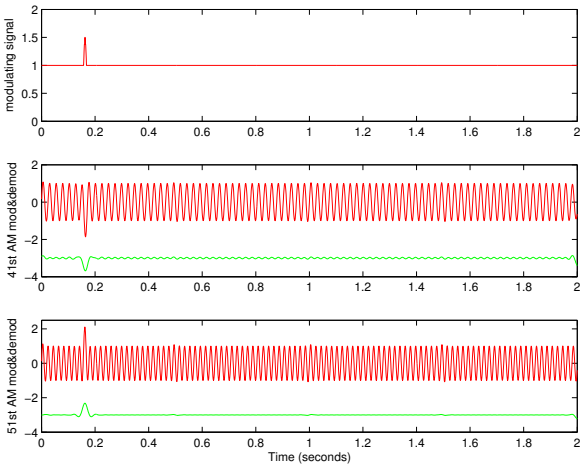

Figure 8: Amplitude modulation and its demodulation based on product detection. The shape and magnitude of the demodulated signal depend on the carrier frequency.

Applying the product detection based amplitude demodulation to the DRXAP processor, we get very different EMA results. Figure 9 demonstrates the demodulation result with the 21st harmonic of the natural operating frequency. The highest peak of the differential trace appears when the EM trace of '`11 XOR 22`' is positive while the EM trace of '`33 XOR 55`' is negative. This indicates a data-dependent timing in asynchronous operations, and the timing shift for the two operations is about odd times of the harmonic half period. Figure 10 shows the demodulation result with the 31st harmonic of the natural operating frequency. The peaks of differential traces in Figure 10 appear in different places compared to Figure 9. It indicates the two operations ('`11 XOR 22`' and '`33 XOR 55`') have different EM emissions (most likely in time rather than in magnitude). When modulating different carriers, different information is magnified or omitted. The product detection based demodulation reveals a larger ratio of differential signals to original signals, which suggests better chances of success in DEMA attacks.

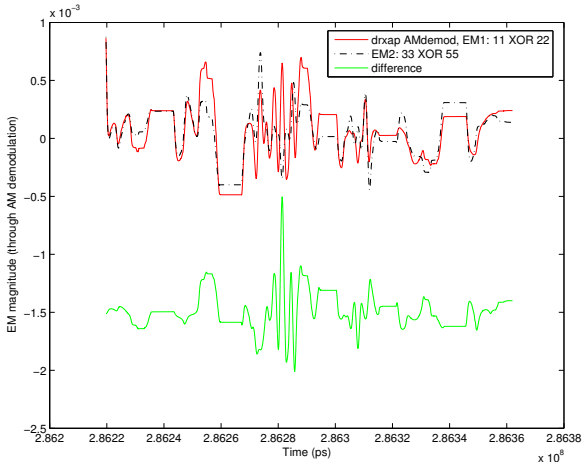

Figure 9: EM simulation of product detection based amplitude demodulation by the 21st harmonic of the natural operating frequency of the asynchronous XAP executing `XOR`

3.2.2 EM simulation on a synchronous processor

Similar simulation flow is applied to the synchronous XAP processor. Figure 11 shows the simulated power analysis. Figure 12 shows the simulation of EMA with an inductive sensor. Figure 13 shows the simulation of EMA with an inductive sensor plus amplitude demodulation

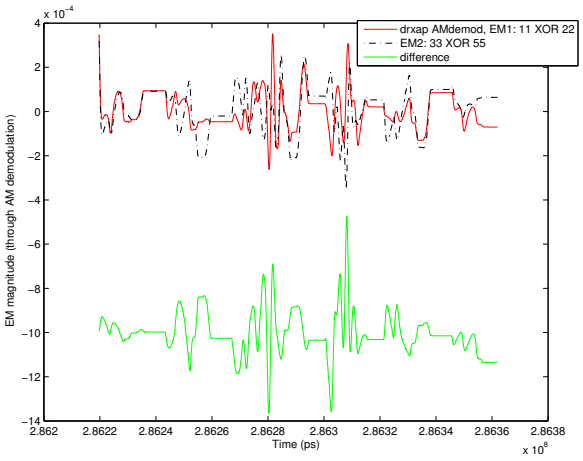

Figure 10: EM simulation of product detection based amplitude demodulation by the 31st harmonic of the natural operating frequency of the asynchronous XAP executing `XOR`

(through envelop detection) by the 19th clock harmonic.

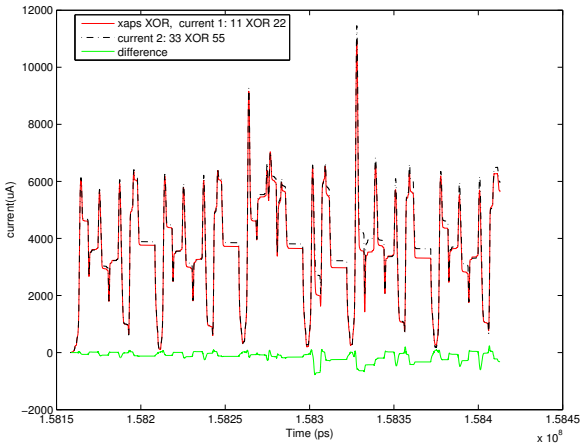

Figure 11: Power simulation: Synchronous XAP executing `XOR`

The magnitude of differential signals in Figures 11 - 13 are shown at similar levels. So we turn to explore the product detection based amplitude demodulation as we do with the asynchronous DRXAP processor. Figure 14 shows the result with the 17th clock harmonic. The highest peak of the differential trace appears when both EM traces of '`11 XOR 22`' and '`33 XOR 55`' are negative or both are positive. This indicates the synchronous processor has data-dependent EM

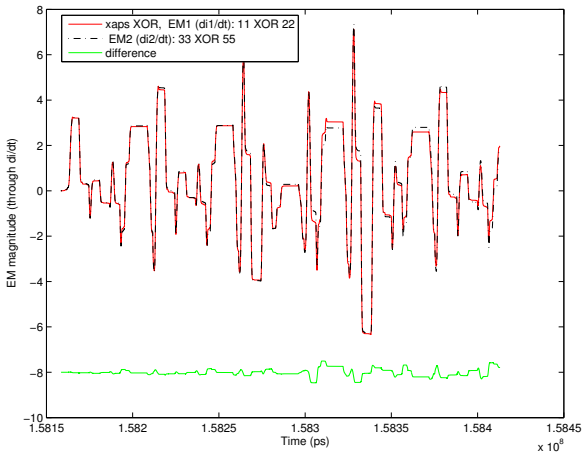

Figure 12: EM simulation of direct emissions with an inductive sensor: Synchronous XAP executing `XOR`

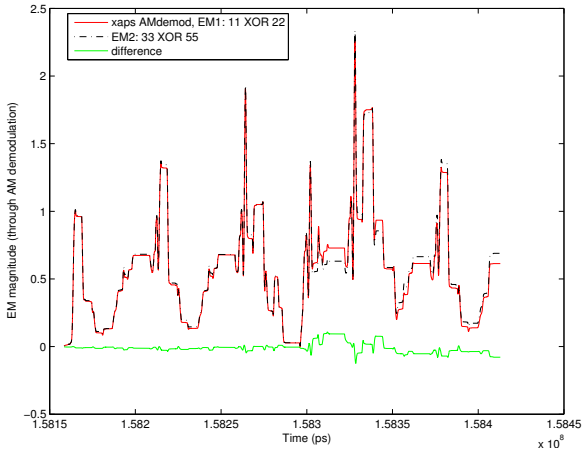

Figure 13: EM simulation of unintentional emissions, amplitude demodulated by a clock harmonic: Synchronous XAP executing `XOR`

emissions varying in magnitude rather than in time. Figure 15 shows the simulation with the 19th clock harmonic. The peaks of differential traces in Figure 14 and Figure 15 appear in different places, which means the two operations ('`11 XOR 22`' and '`33 XOR 55`') have different EM emissions. When modulating different carriers, different information is magnified or omitted.

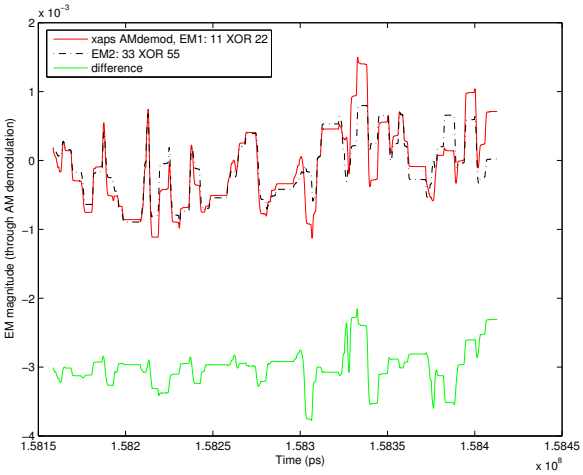

Figure 14: EM simulation of product detection based amplitude demodulation with the 17th clock harmonic: Synchronous XAP executing `XOR`

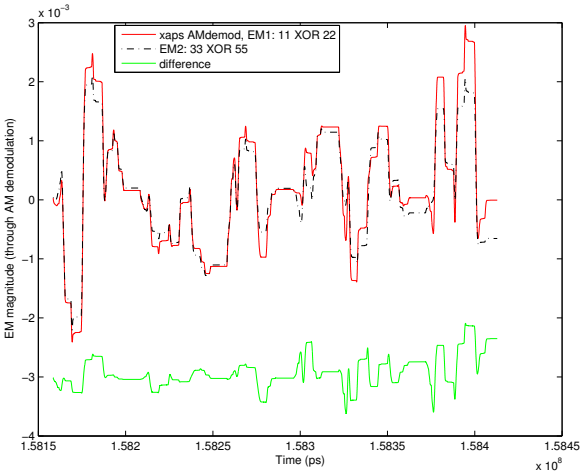

Figure 15: EM simulation of product detection based amplitude demodulation with the 19th clock harmonic: Synchronous XAP executing `XOR`

4 Conclusion

A simulation methodology for EMA has been proposed and a testing has been performed on synchronous and asynchronous processors to identify their EM leakage characteristics. This simulation methodology involves current simulation with circuit simulators such as VCS and Nanosim, IC layout parasitics extraction with extraction tools such as Mentor xCalibre. Once collected, the data of current assumption is processed with Matlab to simulate EMA. It is demonstrated that differential power analysis, differential EM analysis of direct emissions, and differential EM analysis of AM demodulated emissions (through an envelop detector) reveal almost the same level of leakage. While differential EM analysis of AM demodulated emissions (through a product detector) reveals greater leakage, where the magnitude of differential traces is comparable to that of the traces themselves. A comparison between a synchronous and an asynchronous processor indicates that synchronous processors have data dependent power and EM emissions, while asynchronous processors have data dependent timing which is visible in differential power or EM analysis.

References

[1] D. Agrawal, B. Archambeault, J. Rao, P. Rohatgi, "The EM Side-Channel(s):Attacks and Assessment Methodologies", `http://www.research.ibm.com/intsec/emf-paper.ps`

[2] Michael J.S. Smith, *Application-Specific Integrated Circuits*, Addison Wesley, 2001.

[3] M. M. Parish, P. B. Littlewood, "Non-saturating magnetoresistance in heavily disordered semiconductors", in *Nature*, Vol. 426, pp. 162 - 165 (13 November 2003)

[4] G3Card Consortium, "3rd Generation Smart

Card Project", http://www.g3card.org/

[5] Jacques J.A. Fournier, Simon Moore, Huiyun Li, Robert Mullins, George Taylor, "Security Evaluation of Asynchronous Circuits", in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES2003*, Germany, 2003.

[6] D. M. Pozar, *Microwave Engineering*, 2nd ed., John-Wiley, 1998.

[7] Michael J. Caruso, Tamara Bratland, Carl H. Smith and Robert Schneider, "A New Perspective on Magnetic Field Sensing", in *Sensors*, Dec, 1998.

[8] Maxwell and HFSS at CERN, http://wwwce.web.cern.ch/wwwce/ae/Maxwell/ansoft_si.html

[9] Isidor Straus, "Near and Far Fields - From Statics to Radiation", http://www.conformity.com/0102reflections.html

[10] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in proceedings of *Cryptographic Hardware and Embedded Systems (CHES 2001)*, LNCS 2162, 2001.

[11] IBM research news, http://www.research.ibm.com/resources/news/20020507_simcard.shtml

[12] Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards, http://www.research.ibm.com/intsec/gsm.html