Security Evaluation Against Electromagnetic Analysis at Design Time

Huiyun Li, A. Theodore Markettos, and Simon Moore

Computer Laboratory, University of Cambridge
JJ Thomson Avenue, Cambridge CB3 0FD, UK
Huiyun.Li@cl.cam.ac.uk

Abstract. Electromagnetic analysis (EMA) can be used to compromise secret information by analysing the electric and/or magnetic fields emanating from a device. It follows differential power analysis (DPA) becoming an important side channel cryptanalysis attack on many cryptographic implementations, so that constitutes a real threat to smart card security. A systematic simulation methodology is proposed to identify and assess electromagnetic (EM) leakage characteristics of secure processors at design time. This EM simulation methodology involves current flow simulation, chip layout parasitics extraction, then data processing to simulate direct EM emissions or modulated emissions. Tests implemented on synchronous and asynchronous processors indicates that the synchronous processor has data dependent EM emission, while the asynchronous processor has data dependent timing which is visible in differential EM analysis (DEMA). In particular, DEMA of amplitude demodulated emissions reveals greater leakage compared to DEMA of direct emissions and DPA. The proposed simulation methodology can be easily employed in the framework of an integrated circuit (IC) design flow to perform a systematic EM characteristics analysis.

Keywords. EM side-channel analysis; smart card; design time security evaluation

1 Introduction

Smart cards are widely used for authentication and securing transactions. Their cryptographic operations are based on symmetrical or asymmetrical cryptographic algorithms such as triple DES, AES or RSA. But even if the cryptographic algorithms and the protocols are secure, information about secret data may leak through side-channels such as timing of computation [1], power consumption [2], as well as electromagnetic radiation [3]. In the EM side-channel, a smart card emits different amounts of EM emission during the computation depending on the instructions and data being executed. Some sophisticated statistical techniques such as differential electromagnetic analysis (DEMA) [3, 4, 5] can detect variations in EM emission so small that individual key bits can be identified. This means secret key information can be recovered from the secure devices.

To keep these devices secure against the EM side-channel attacks, a huge amount of research has been undertaken. However, in common industrial practise, the security evaluation of the secure device designs is only performed after chips are manufactured. This post-manufacture analysis is time consuming, error prone and very expensive. This has driven the study of the design-time security evaluation which aims to examine data-dependent EM characteristics of secure processors, so as to assess their security level against EM side-channel analysis attacks.

The most straightforward way to simulate EM waves propagating in a circuit is to use a 3D or planar EM simulator, which involves solving Maxwell's equations for the electric and magnetic vector fields in either the frequency or time domain. However a full-wave 3D simulator incorporating characterised nonlinear[1] semiconductor devices is too time consuming to be practical for chip-level analysis. Various types of field sensors, namely electric or magnetic field sensor measuring in near or far field, used by attackers also increase the challenges in EMA simulation. Different types of sensors measure different types of field, so they require different simulation methods. Furthermore, the modulated EM emissions [4] have begun arousing attention in the cryptanalysis community as well as the direct EM emissions that are normally exploited in EM analysis attacks [5]. Modulated emissions occur when a data signal modulates carrier signals which then generate EM emissions propagating into the space. Different modulation mechanisms require different demodulation manners.

In this paper, we present a design time security evaluation methodology for EM side-channel analysis. It first partitions an electronic system under test into two parts: the chip and the package. The package is simulated in an EM simulator and modelled with lumped parameters R, L and C. The chip incorporating the package lumped parameters is then simulated in circuit simulators. This mixed-level simulation obtains current consumption of the system under test accurately and swiftly. Next, the security evaluation methodology involves a procedure of data processing on the current consumption to simulate EM emissions. Different methods of data processing are required to target corresponding types of sensors. Furthermore, to simulate modulated EM emissions, demodulation in amplitude or angle is incorporated into the simulation flow.

The rest of the paper is organised as follows. In Section 2, we present our simulation methodology of system partitioning and simulation procedures incorporating different types of EM emissions and different field sensors. In Section 3, we demonstrate simulation results for two processors on our test chip from which data dependent EM characteristic is successfully identified and verified by measurement results. Section 4 presents a brief conclusion.

2 Simulation Methodology for EM Analysis

2.1 System partitioning

As described in Section 1, a 3D full-wave field simulator incorporating large number of semiconductor devices is too time consuming to be practical for chip-level analysis. Our simulation approach is to partition an electronic system into two parts. The first part

[1] Some examples of nonlinear components are Diode, BJT and MOSFET.

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 dimensions are small enough (compared to the wavelength) to tolerate the errors[2]. The second part is the package and even the printed circuit board (PCB), which can be accurately simulated by a (3D or planar) **EM simulator** and be modelled with lumped components (R, L and C). The lumped elements will then be incorporated into the same circuit simulator to achieve the response of the entire system.

2.2 Simulation procedure

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. In this case, a Verilog/SPICE co-simulation can be used where the partitioning function provides an easy means to select the desired block(s) to test. With Verilog/SPICE co-simulation, various instructions are easily executed and modified through testbench files written in Verilog. Accurate simulation of current consumption is achieved in the SPICE-like simulation. Once the current data $Idd(t)$ for the desired block(s) or a whole processor is collected, it is passed to MATLAB™ and is processed to implement DEMA according to the sensor types and emission types.

The data process procedure for EM analysis is shown in the shadowed box in Figure 2. It includes synchronising and re-sampling of two sets of current consumption data when the processor under test is computing with different operands. We perform signal processing on each set of current consumption data according to the types of EM emissions to be measured and according to the types of field sensors to measure the EM emissions.

Direct vs modulated EM emissions EM emissions can be generally categorised into two types: direct emissions and modulated emissions [4]. *Direct emissions* are caused directly by current flow with sharp rising/falling edges. To measure direct emissions from a signal source isolated from interference from other signal sources, one uses tiny field probes positioned very close to the signal source and special filters to minimise interference. To get good results may require decapsulating the chip.

Modulated emissions occur when a data signal modulates carrier signals which then generate EM emissions propagating 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.

[2] The velocity of electromagnetic propagation is limited by the laws of nature, and in silicon-dioxide it is approximately 1.5×10^8 m/s . Fast signal edges in smart card chips with an edge rate of under 1ns have to be considered as “high speed” only when the longest chip dimension is beyond 50mm, as a rule of thumb.

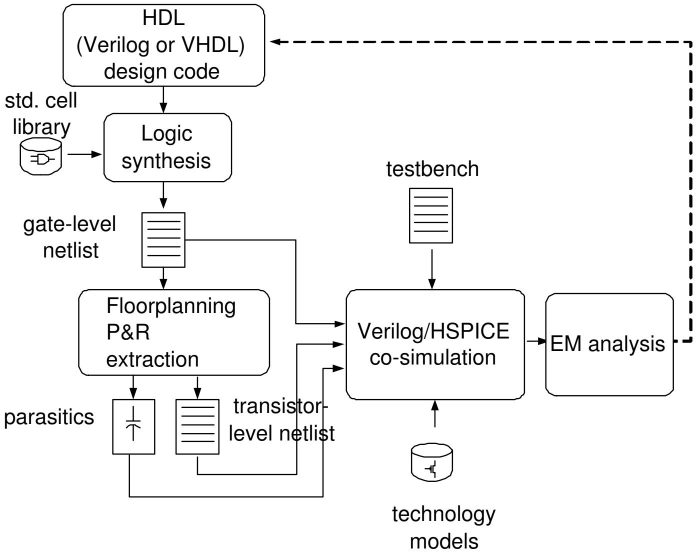


Fig. 1. Digital design flow with EM analysis

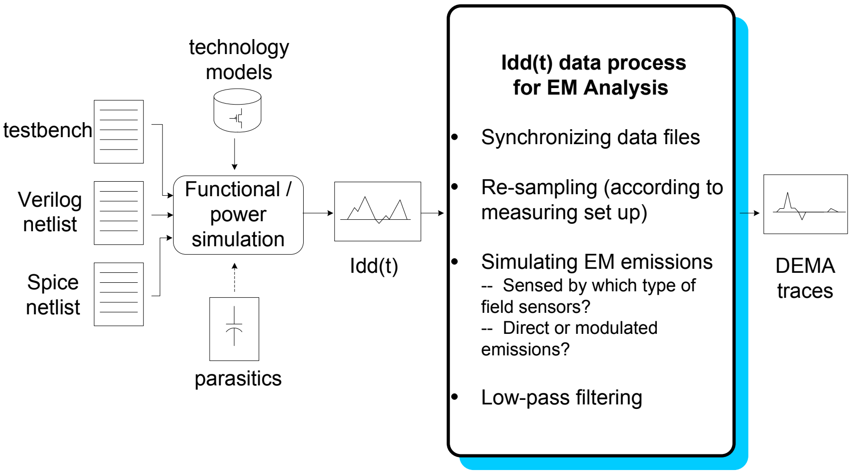

technology
models
testbench
Verilog
netlist
Spice
netlist
Functional /
power
simulation
parasitics
Idd(t)
Idd(t) data process
for EM Analysis
• Synchronizing data files
• Re-sampling (according to measuring set up)
• Simulating EM emissions
-- Sensed by which type of field sensors?
-- Direct or modulated emissions?
• Low-pass filtering
DEMA
traces

Fig. 2. EM analysis simulation procedure

- Amplitude Modulation
  In a circuit, the data signal may couple to a carrier signal (e.g. clock harmonics) due to E field capacitive coupling or H field magnetic coupling, which generates a sum of the data signal and the carrier signal. Once these two coupled signals go through a square-law device (e.g. a transistor), the product of the two signals is generated.
  For instance, an n-channel transistor operates in the saturation region when $V_{DS} > V_{GS} - V_{Tn}$, its drain current remains approximately constant as: $I_{DSn(sat)}$ [6]:

  $$I_{DSn(sat)} = \frac{\beta_n}{2}(V_{GS} - V_{Tn})^2 \tag{1}$$

  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 (V_{clock}) coupled with a data signal (V_{data}): $V_{GS} = V_{data} + V_{clock}$, 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: $\sum\limits_{n=1,3,5...}^{\infty} \frac{4}{n\pi}\sin(2\pi nft)$.
  The saturation current $I_{DSn(sat)}$ becomes:

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

  Expanded, $I_{DSn(sat)}$ contains items of interest as the product of sinusoidal signals and the coupled data signal: $\beta_n \sum\limits_{n=1,3,5...}^{\infty} \frac{4}{n\pi}\sin(2\pi nft)V_{data}$.
  This process is amplitude modulation (AM), where the coupled data signal V_{data} modulates clock harmonics with diminishing magnitude. If 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.
  Amplitude modulation can also occur in a transistor when the digital gate input V_{GS} is itself a square-wave, harmonic-rich signal. For example, in one cryptographic execution run, the input V_{GS1} is 00111100..., while in another run, the input at the same gate becomes V_{GS2} as 01010101.... Then V_{GS1} and V_{GS2} have Fourier series expressions different at some carrier frequencies. 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[3]. In deep submicron processes, the dependence of saturation drain current $I_{DSn(sat)}$ on gate source voltage V_{GS} is better modelled by a linear rather than a quadratic relationship.

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

- 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 voltage controlled oscillator (VCO), 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.

Exploiting modulated emissions can be easier and more effective than working with direct emission [4]. Some modulated carriers could have substantially better propagation than direct emission, which may sometimes be overwhelmed by noise. The modulated emission sensing does not require any intrusive/invasive techniques or fine grained positioning of probes.

Depending on the types of EM emissions in EMA attacks: direct emissions or modulated emissions, EMA simulation may require demodulation of corresponding manners of the modulation.

EM field measurement equipment A number of sensors can be used to detect the EM signals in EMA attacks. They are divided into those detecting electric and those detecting magnetic fields in near-field[4], 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.

An example of **near-field electric field sensors** is a monopole antenna. It generally measures the near-field electric component around current-carrying conductor where electric field magnitude $E \propto I$. **Near-field magnetic field sensors** generally measure the near-field magnetic component around current-carrying conductor where magnetic field magnitude $B \propto I$.

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, which says 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 between the sensor and the concerned circuit.

[4] 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 it ($r > \lambda/2\pi$).

This type of field sensor senses the change of magnetic flux, so we use the rate of change of the current dI/dt to track EM emission. Simulation for this type of sensor involves differential calculus on current consumption data.

There are also **far-field electromagnetic field sensors** such as log-periodic antennas. They generally measure far-field electromagnetic field and often work with other equipment to harness modulated emissions. For example, an amplitude modulation (AM) receiver tuned to a clock harmonic can perform amplitude demodulation and extract useful information leakage from electronic devices [4].

This is not an exhaustive list of field sensors, but provides a view that different types of sensors measure different types of field, so that require different approaches in EM simulations.

Low-pass filtering effect of EM sensors The last step of data processing procedure as shown in the shadowed box in Figure 2 is the low-pass filtering. Considering the inductance in field sensors, and the load resistance from connected instruments (e.g. an amplifier or an oscilloscope), an RL low-pass filter is formed as shown in Figure 3. Its 3dB cutoff [5] frequency is calculated as $f_{cutoff} = R/2\pi L$. Due to this RL low-pass filtering effect, the two sets of processed current consumption data have to be low-pass filtered at the end of the EMA data processing procedure.

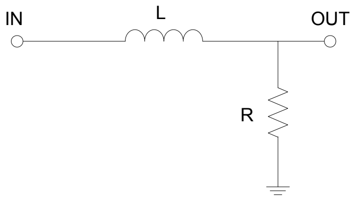


Fig. 3. RL low-pass filter

Finally, DEMA is performed by subtracting one EMA trace from another. Security weakness will be manifested as pulses in the DEMA trace, revealing data-dependent EM characteristics of the tested design. The term DEMA here (and further in this paper) refers to the variation (difference) in the EM emissions, instead of statistical treatment correlating the variation to hypothetical data being manipulated as in a real DEMA attack [3]. This is because the proposed methodology is to evaluate data-dependent EM characteristics of secure processor designs, which are the fundamental weakness a real DEMA attack exploits and can be identified with deterministic data.

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

3 Evaluation Results of The Simulation Methodology

3.1 EM simulation setup

DEMA simulation has been carried out on a test chip, fabricated in UMC 0.18μm six metal CMOS process as part of the G3Card project [7, 8]. Figure 4 shows a picture of the test chip which contains five 16-bit microcontroller processors with different design styles. This paper addresses the synchronous processor (S-XAP) on the top left corner and the dual-rail asynchronous processor (DR-XAP) in the middle.

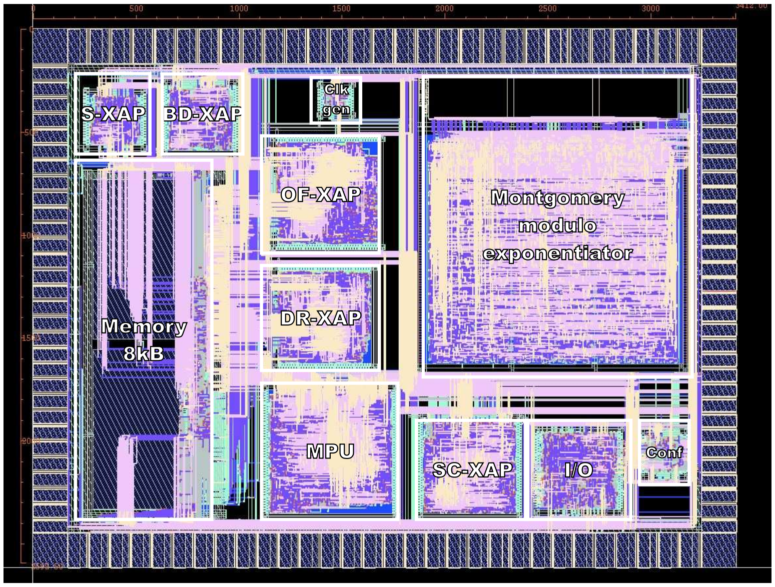


Fig. 4. The microcontroller processors (S-XAP, DR-XAP) on the chip are under EMA simulation test.

We target simple instructions (e.g. XOR (exclusive OR), shift, load, store etc) which can give a good indication of how the hardware reacts to operations of cryptographic algorithms. A short instruction program runs twice with operands of different Hamming weight. The first run sets the I/O trigger port high by storing '1' into memory, computes '00 XOR 55', and sets the I/O trigger port low by storing '0' into memory, while the second run sets the I/O port high, computes '55 XOR 55', and sets the I/O port low.

3.2 EM simulation of a synchronous processor

Figure 5 shows the EMA simulation over the S-XAP processor. We simulate direct EM emission picked up by an inductive sensor. On the graph we plot the EM traces of the processor for '00 XOR 55' and '55 XOR 55', as well as the differential EM

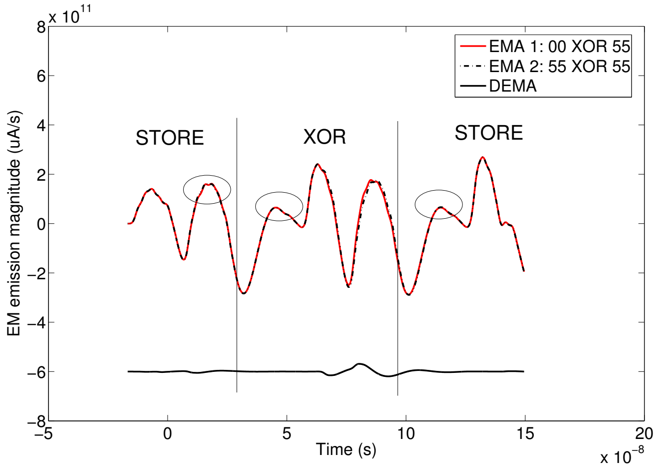


Fig. 5. EMA simulation over S-XAP processor executing XOR with different operands

plot of EMA1 - EMA2 (DEMA). The EM traces (EMA1 and EMA2) are superposed and appear as the top trace in Figure 5. The differential EM trace (DEMA) is shifted down from the centre by 6×10^{11} unit to clearly show its relative magnitude. The EM emission magnitude is computed through dI/dt as discussed in Section 2.2, thus has units of $\mu A/s$.

The measurement of EM emissions on the same processor performing the same code is shown in Figure 6. The EM emissions are picked up by an inductive sensor over 5000 runs to average out the ambient noise (although 200 runs are enough), then are monitored on an oscilloscope. The inductive head in use has resistance R = 5.42Ω, inductance 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 Section 2.2, and the parameters have been used in the EMA simulation shown in Figure 5.

Both the measurement and the simulation results observe the differential trace peaks when the processor is executing XOR logic operations. This means data dependent EM emission is leaking information related to key bits at those instances, thus means vulnerability in EMA attacks. The agreement in the measurement and the simulation results verified the validity of the proposed EMA simulation approach. The simulated EM traces in Figure 5 are lower in shape compared to those measured around the circled places, as the simulation includes no power contribution from memory accesses.

To gain a perception of the DPA attack versus the DEMA attack, Figure 7 demonstrates DPA measurement over S-XAP processor performing the same code. Although only 4 measurement runs to average out noise, data dependent power consumption can clearly identify when the processor is executing XOR logic operations. The peak to peak in the differential trace (DPA) is about 6% of the peak to peak of the original signals (Power Analysis 1 and Power Analysis 2). As a comparison, the peak to peak

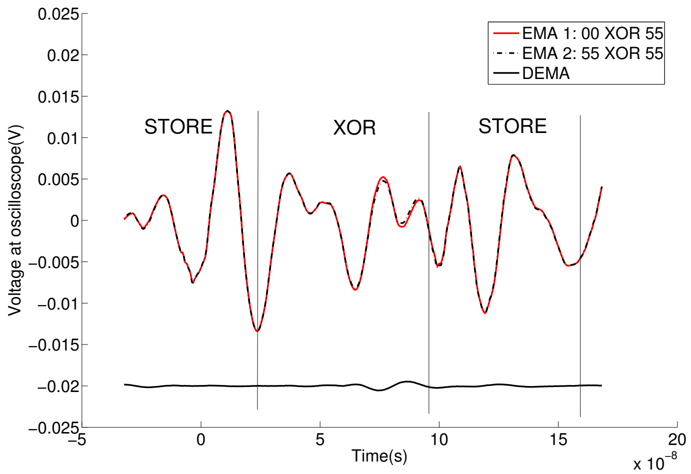


Fig. 6. EMA measurement over S-XAP processor executing XOR with different operands (experimental graph)

DEMA is about the same level of the peak to peak of the original signals (EMA 1 and EMA 2) in Figures 5 and 6, indicating the same level of information leakage in the EM side-channel and in the power channel.

3.3 EM simulation of an asynchronous processor

We then perform EMA simulation on processor DR-XAP which is designed in a dual-rail asynchronous style with return-to-zero handshaking protocol. This balanced asynchronous circuitry was believed to be secure since power consumption should be data independent [8]. Figure 8 shows the EMA simulation result. On the graph we superpose the EM traces of the processor for '00 XOR 55' and '55 XOR 55', and put the DEMA trace at the bottom. The DEMA trace exhibits a wobble at only about 1% magnitude of that of the original traces (EMA1 and EMA2). This matches with the projection that asynchronous design with dual-rail coding and return-to-zero handshaking is much more secure against side-channel analysis attacks.

The measurement result in Figure 9 also indicates no information leakage along the logic operation. Comparing Figure 8 and 9, we observe again lower magnitude in shape around the circled places in simulation, resulted from no memory accesses power consumption in simulation.

Performing EMA simulation on *modulated emissions* on the asynchronous processor, we achieved more intriguing results. We collected the current consumption data as we did in direct emission simulation, then we processed the data with amplitude demodulation. The carrier used to demodulate the EM signal is the 17th clock harmonic (The asynchronous XAP executes at a speed around 10 to 50MHz. Here take a carrier whose fundamental is 20MHz). From the simulation results shown in Figure 10, we

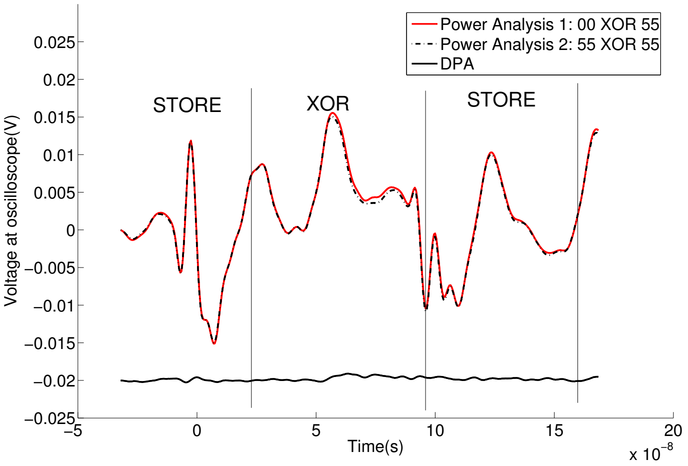


Fig. 7. DPA measurement over S-XAP processor executing `XOR` with different operands (experimental graph)

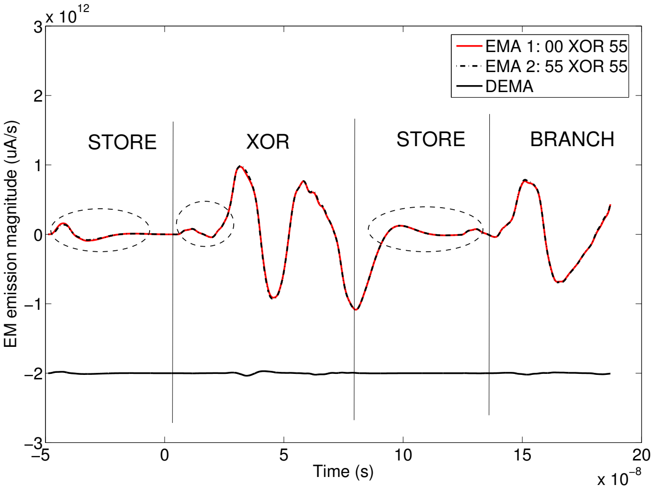


Fig. 8. EMA simulation over DR-XAP (asynchronous dual-rail) processor executing `XOR` with different operands

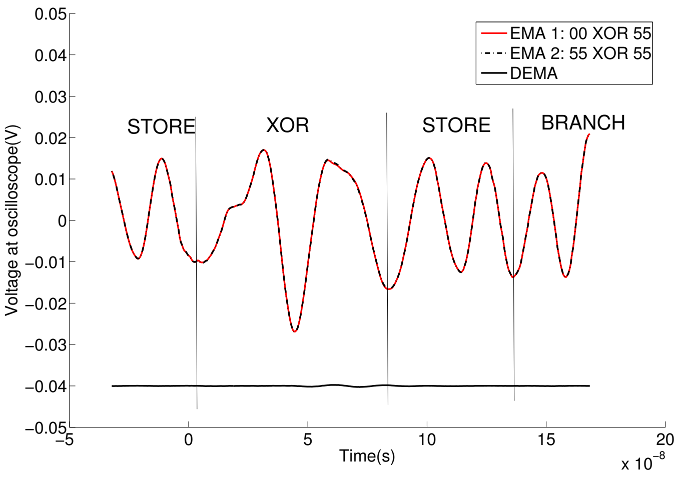


Fig. 9. EMA measurement over DR-XAP (asynchronous dual-rail) processor executing `XOR` with different operands (experimental graph)

observed greater level of differential signals compared to Figure 8. The peak to peak of the differential trace (DEMA) is about 32% of the peak to peak of the original signals (EMA 1 and EMA 2).

The reason why the amplitude demodulated EMA reveals stronger differential signals is demonstrated in a simple example shown in Figure 11. The pulse in subplot (a) is a modulating signal. Subplot (b) shows the AM modulation with a sinusoidal carrier and its product detection based demodulation [9]. The pulse appears on the negative side of the modulation, and demodulated as a negative pulse. Subplot (c) shows the modulating signal with same magnitude and period, but time shifted a bit. Subplot (d) shows its AM modulation with the same sinusoidal carrier as in (b). The pulse appears on the positive side of the modulation, and demodulated as a positive pulse. The sign opposition in the raw traces can result in large peaks in their difference.

In a similar way, data dependent timing in the program execution caused significant peaks in the differential trace shown in Figure 10, although no obvious time shift is observed in the raw traces (AM demodulated EMA 1 and 2), because low-pass filtering has obscured the time shift. We however see higher peaks in Figure 10 around the second STORE operation, as a result of the time shift accumulated in previous operation. This data dependent timing caused EM information leakage is much higher in the tested asynchronous design than the synchronous design, as a result of the lack of clock i.e. synchronisation. The amplitude demodulated EMA simulation reveals an unexpected weakness in the tested asynchronous design against EM side-channel attacks, which provides a good example of usefulness of the design-time evaluation in the secure processor design flow.

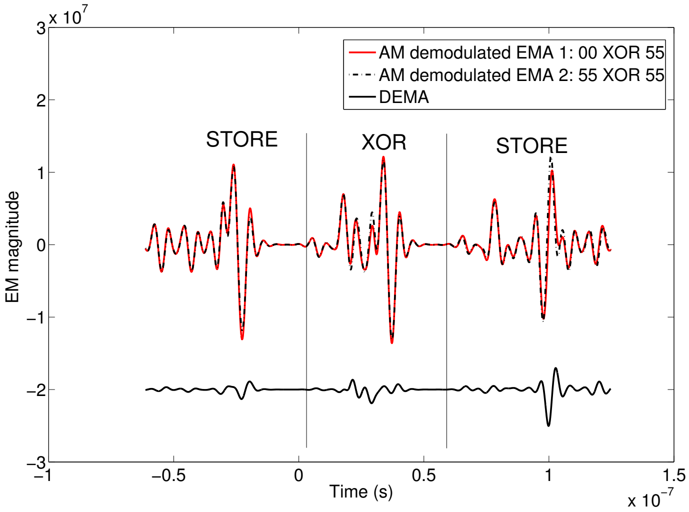
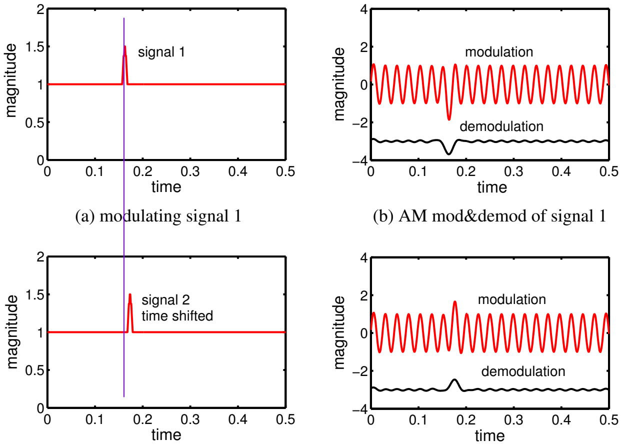


Fig. 10. EMA simulation over DR-XAP (asynchronous dual-rail) processor executing `XOR` with different operands, examining modulated emissions



(a) modulating signal 1

(b) AM mod&demod of signal 1

(c) modulating signal 2

(d) AM mod&demod of signal 2

Fig. 11. Amplitude modulation and demodulation on time shifted signals

4 Conclusion

A simulation methodology for EMA has been proposed on the basis of an analytical investigation of EM emissions in CMOS circuits. This simulation methodology involves simulation of current consumption with circuit simulators and extraction of IC layout parasitics with extraction tools. Once collected, the data of current consumption is processed with MATLAB to simulate EMA.

Testing has been performed on synchronous and asynchronous processors and the results have demonstrated that DPA and DEMA of direct emissions reveal about the same level of leakage. While DEMA of amplitude demodulated emissions reveals greater leakage, suggesting better chances of success in differential EM analysis attacks. The comparison between the EMA on synchronous and asynchronous processors indicates that the synchronous processor has data dependent EM emissions, while the asynchronous processor has data dependent timing which is visible in DEMA.

The proposed simulation methodology can be easily employed in the framework of an integrated circuit design flow. To the best of our knowledge, the proposed simulation methodology for EMA is the first available assessment of EM leakage characteristics of cryptographic processors at design time. It moves one step closer to a complete security-aware design flow for cryptographic processors which aims to cover all known side-channel analysis attacks.

Acknowledgements

The authors would like to thank the Engineering and Physical Sciences Research Council (EPSRC) for funding this research project. We also thank Jacques Fournier, Scott Fairbanks, Petros Oikonomakos and Simon Hollis for their valuable comments on this paper.

Bibliography

[1] P. Kocher. Cryptanalysis of Diffie-Hellman, RSA, DSS, and other cryptosystems using timing attacks. In *Proceedings of 15th International Advances in Cryptology Conference – CRYPTO '95*, pages 171–183, 1995.

[2] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proceedings of 19th International Advances in Cryptology Conference – CRYPTO '99*, pages 388–397, 1999.

[3] J-J. Quisquater and D. Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *E-smart*, pages 200–210, 2001.

[4] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi. The EM side-channel(s). In *Proceedings of Cryptographic Hardware and Embedded Systems - CHES2002*, pages 29–45, 2002.

[5] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In *Proceedings of Cryptographic Hardware and Embedded Systems - CHES2001*, pages 251–261, 2001.

[6] M.J. Smith. *Application-Specific Integrated Circuits*. Addison-Wesley, 1997.

[7] G3Card Consortium. 3rd generation smart card project. `http://www.g3card.org/`.

[8] J. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor. Security evaluation of asynchronous circuits. In *Proceedings of Cryptographic Hardware and Embedded Systems - CHES2003*, pages 137–151, 2003.

[9] H.L. Van Trees. *Detection, Estimation, and Modulation Theory: Radar-Sonar Signal Processing and Gaussian Signals in Noise*. Krieger Publishing Co., Inc., 1992.