A SECURITY EVALUATION METHODOLOGY FOR SMART CARDS AGNAIST ELECTROMAGNETIC ANALYSIS

Huiyun Li, A. Theodore Markettos, Simon Moore

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

ABSTRACT

Cryptographic processors can be vulnerable in electromagnetic analysis (EMA) attacks due to their EM side-channel leakage. A design-time security evaluation methodology has been proposed to assess the security level of cryptographic processors against EMA attacks. This EM simulation methodology involves current flow simulation, chip layout parasitics extraction, then data processing to simulate direct EM emissions or modulated emissions. 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.

1. INTRODUCTION

Smart cards are used in a multitude of security applications, ranging from personal identification and wireless communication to bank payment cards and computer security. Their cryptographic operations are based on cryptographic algorithms and protocols. However, even if these algorithms and protocols are provably secure, the system could be broken if the keys can be extracted from smart cards or terminals by side-channels analysis attacks, such as timing analysis [1], power consumption analysis [2], as well as electromagnetic radiation analysis [3] attacks. In an EM side-channel analysis attack, some sophisticated statistical techniques such as differential electromagnetic analysis (DEMA) [3, 4, 5] are used to analyse the EM emission of a smart card during operation. DEMA involves hypothesising a secret key (often part of the key bits), taking a large number of measurement of EM traces, dividing these traces into two partitions according to the intermediate results, averaging each partition to remove noise, and finally computing the differential trace (the difference between the average of the two partitions). If the hypothetic secret key is false, the differential trace is close to zero. If the hypothetic secret key is true, the differential trace exhibits peaks, indicating points where the key bits were manipulated. By this means, DEMA can detect variations in EM emission so small that individual key bits can be identified.

A huge amount of research has been undertaken to keep smart cards secure against the DEMA attacks. The countermeasures generally endeavour to hide or avoid the correlation between the data being manipulated and the side-channel information. However, in common industrial practise, the security evaluation of the secure device designs could only be 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.

To simulate EM waves propagating in a circuit generally requires a 3D or planar EM simulator, which involves solving Maxwell's equations for the electric and magnetic vector fields in either the frequency or the 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.

This paper presents a security evaluation methodology for smart cards against EM analysis attacks. This design-time security evaluation methodology first partitions the 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.

We organise the rest of the paper as follows. In Section 2, we present our simulation methodology of system partitioning and simulation procedures. In Section 3, we demonstrate the simulation result for our test chip from which data dependent EM characteristic is successfully identified and verified by the measurement result. Section 4 presents a brief conclusion.

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

2. SIMULATION METHODOLOGY FOR EM ANALYSIS

2.1. System partitioning

As described earlier, 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 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

Figure 1 demonstrates the procedure of EMA simulation based on a typical digital IC design flow. The EM analysis is similar to power analysis which measures the global current of a device [6], except that 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.

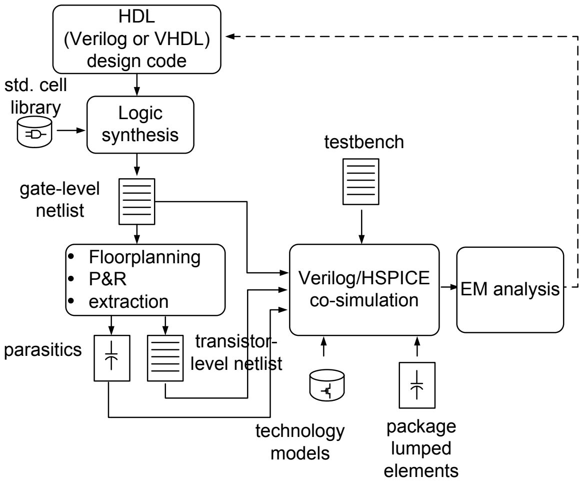

Fig. 1. Digital design flow with EM analysis

The blocks of *Verilog/HSPICE co-simulation* and *EM analysis* in Figure 1 are zoomed in and shown in Figure 2. In particular, *EM analysis* is shown in the shadowed box, including synchronising and re-sampling of two sets of current consumption data when the processor under test is computing with different operands. We then perform signal processing on each set of current consumption data according to the types of field sensors to measure and according to the types of EM emissions to be measured. For example, using differential calculus, if we wish to simulate direct EM emissions, or using amplitude demodulation to simulate amplitude modulated EM emissions.

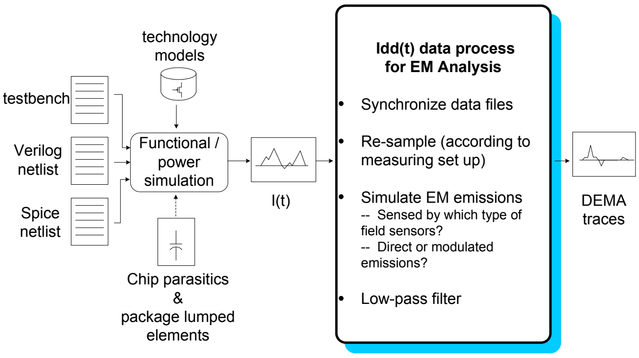

Fig. 2. EM analysis simulation procedure

2.2.1. *EM field measurement equipment*

The field sensors used in EMA attacks are divided into those detecting electric and those detecting magnetic fields in near-field[3], 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 $E \propto I$.

Near-field magnetic field sensors generally measure the near-field magnetic component around current-carrying conductor where $B \propto I$. 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 Alternate Current (AC) current-carrying conductor. This is the transformer effect. The induced voltage is:

$$V = -\int_S \frac{\partial \mathbf{B}}{\partial t} \cdot d\mathbf{s} \tag{1}$$

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.

$$V = M\frac{dI}{dt} \tag{2}$$

where M denotes the mutual inductance between the sensor and the concerned circuit.

[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. Smart card chips are typically $< 5mm$, so wires are never longer than 10mm, but even this is unlikely.

[3] 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.

2.2.2. 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.

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.

2.2.3. 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[4] 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.

Finally, the DEMA trace 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.

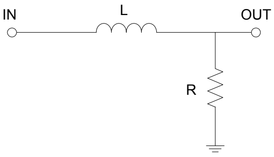

Fig. 3. RL low-pass filter

3. EVALUATION RESULTS OF THE SIMULATION METHODOLOGY

3.1. EM simulation setup

We perform DEMA simulation on a test chip fabricated in UMC 0.18μm six metal CMOS process as part of the G3Card project [7, 8]. The test chip contains five 16-bit microcontroller processors with different design styles. This paper addresses the synchronous processor (S-XAP) on the top left corner.

The aim of the test is to examine data-dependent EM characteristics of the processors, so as to assess their security against EM side-channel analysis attacks. 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

Figure 4 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 plot of EMA1 - EMA2 (DEMA). The EM traces (EMA1 and EMA2) are superposed and appear as the top trace in Figure 4. 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 2.2.1, thus has units of $\mu A/s$.

The measurement of EM emissions on the same processor performing the same code is shown in Figure 5. 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 = 5.4 , inductance L = 9µH. When delivering power into a 4K 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 2.2.3, and the parameters have been used in the EMA simulation shown in Figure 4.

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 4 are lower

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

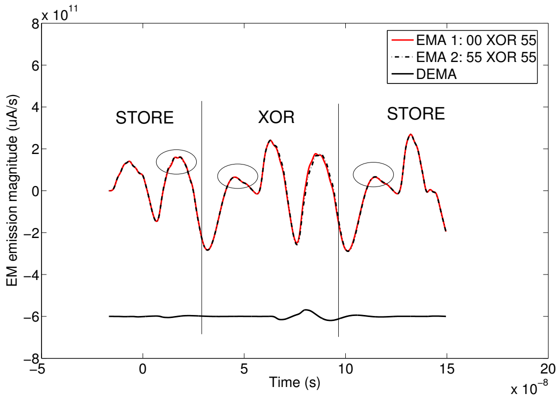

Fig. 4. EMA simulation over S-XAP processor executing `XOR` with different operands

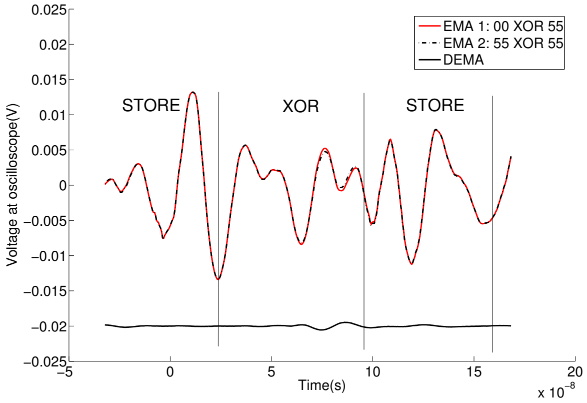

Fig. 5. EMA measurement over S-XAP processor executing `XOR` with different operands (experimental graph)

in shape compared to those measured around the circled places, as the simulation includes no power contribution from memory accesses.

4. CONCLUSION

A security evaluation methodology has been proposed to assess the cryptographic processor designs against EM emission analysis attacks at design time. This methodology involves the partitioning of the system under test, simulation of its current flow, IC layout parasitic extraction, and data processing.

Simulation implemented on a test processor identifies its data dependent EM characteristics which is verified by measurements.

The proposed simulation methodology can be easily employed in the framework of an integrated circuit design flow. 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 and fault-injection attacks.

References

[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. Bucci, M. Guglielmo, R. Luzzi, and A. Trifiletti. A Power Consumption Randomization Countermeasure for DPA-Resistant Cryptographic Processors. In *PATMOS*, pages 481–490, 2004.

[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.

Acknowledgements

The authors would like to thank the Engineering and Physical Sciences Research Council (EPSRC) for funding this research as part of the project: GR/S16805/01. We also thank Jacques Fournier, Scott Fairbanks, Petros Oikonomakos and Simon Hollis for their valuable comments on this paper.