ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards

Jean-Jacques Quisquater and David Samyde

Université catholique de Louvain, UCL Crypto Group,
Laboratoire de microélectronique (DICE),
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium.
E-mail: {jjq,samyde}@dice.ucl.ac.be
URL: http://www.dice.ucl.ac.be/crypto

Abstract. A processor can leak information by different ways [1], electromagnetic radiations could be one of them. This idea, was first introduced by Kocher, with timing and power measurements. Here we developed the continuation of his ideas by measuring the field radiated by the processor. Therefore we show that the electromagnetic attack obtains at least the same result as power consumption and consequently must be carefuly taken into account. Finally we enumerate countermeasures to be implemented.

Keywords: electromagnetic and power analysis, tamper resistance, SEMA, DEMA, SPA, DPA, smartcard.

1 Introduction

The measurement of the consumption of a cryptographic processor (smartcard) provides data on its activities. Handling of a bit with 1 and a bit with 0 involves different energy, so the electromagnetic field can be another vector of information. Any movement of electric charges is accompanied by an electromagnetic field. The currents going through a processor can characterize it according to its spectral signature.

This idea is a generalization of Kocher's idea presented in 1996. His idea laid the foundations of the power analysis. Actually power analysis includes Simple Power Analysis (SPA) and Differential Power Analysis (DPA) [2,3]. However the electromagnetic analysis wants to be more general. The Timing attack developed by Kocher and its practical implementation by Koeune, are limited in the analysis to mono-dimensional data processing. In the same way the DPA attacks or second order DPA use a two-dimensional matrix to visualize the correlation during the treatment [4]. The results from the Electromagnetic Analysis can be treated as the previous ones, but they also hold a three-dimensional information linked to the volume.

I. Attali and T. Jensen (Eds.): E-smart 2001, LNCS 2140, pp. 200-210, 2001.

Smart cards are particularly concerned [5]. They are protected against many non intrusive attacks but they cannot detect a listening material. Moreover, they emit a lot of information because memory accesses are frequent. The dimensions of the chip are directly linked to the emissions of all kind, and a lot of noises are generated by calculations and processor's actions.

For example, the Haming weight can be deducted during the loading time of the data bus. Each " 0 " implies the use of a specific quantity of energy, it is then possible to calculate the number of " 1 " in the data and to deduce the weight. SPA can allow such a measurement, and so does EMA.

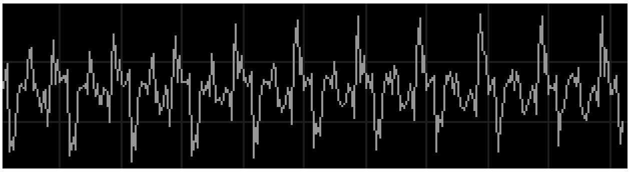

Fig 1 : Few rounds of a DES execution.

In a synchronous processor, the modifications linked to the evolution of the clock characterize the system [6]. The transfers on the bus have a consumption proportional to the number of bits which change between two cycles. So the electromagnetic analysis is strongly dependent on the architecture of the chip, and the knowledge of the internal circuitry of the processor facilitates the work.

2 Context

For a few years the electromagnetic radiation of the electric devices has been taken into account. The standards for electromagnetic radiation are present in order to at least allow the peaceful coexistence of various devices at the same place.

All the electronic devices containing electronic components are sensitive to outside disturbances [7]. However they are themselves disturbing elements in some cases. Thus an office computer can interferer with a radio receiver. We decided to base on this idea to investigate the study of the electromagnetic field emitted by processors during their work.

It appears that this radiation is directly connected to the current consumption of the processor. The electromagnetic field lets informations on the activities of the chip flee. The spectral signature is architecture dependant. However some behaviors are identical from a processor to another. For example an access memory that activates the load pump results in a specific peak in the electromagnetic spectrum and is directly linked to the control of the oscillator.