Learning from Electromagnetic Emanations — A Case Study for iMDPL

Mario Kirschbaum and Joern-Marc Schmidt

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, 8010 Graz, Austria
{Mario.Kirschbaum, Joern-Marc.Schmidt}@iaik.tugraz.at

Abstract. Efficient countermeasures against side-channel attacks are vital for security-related devices. This is because power-measurements can be carried out at relatively low costs by an adversary that has physical access to the device. In a lot of applications, e.g. pay-TV, the ability of cloning a single device leads already to a significant problem (*i.e.* monetary loss) for the issuer of the device.
While the knowledge that a device leaks information is already important, a detailed image about the nature of the security hole would help the designer to improve the product.
In this paper, we analyze the electromagnetic emanations of the secure logic style iMDPL. We measured the emanations by stepping with an EM probe over an ASIC prototype chip produced in a 180 nm CMOS process technology. By means of data dependency images for each point in time during the computation we deeply investigate security related issues of iMDPL and show that certain data flows within a design can be traced with this technique.

Keywords: EM, iMDPL, stepper, side-channel attacks

1 Introduction

The design of a device that can resist an adversary with physical access to it is a challenging task. This is because the theoretic security in a black-box model of the chosen algorithm is not sufficient to guarantee the resistance of its implementation. In order to implement an algorithm in a secure way, also the physical properties of the underlying device have to be taken into account. An adversary may not only rely on input or output of the device, but also measure its timing [4], its power consumption [5] or its electromagnetic emanations [9].

Quisquater et al. [9] published one of the first articles on practical EM measurements for attacking security-related devices. They showed that EM measurements can be carried out observing local parts of the device instead of obtaining just a global view as it is the case for power measurements. While these attacks target CMOS technology, De Mulder et al. [7] attacked FPGA implementations. Other targets that received attention in the past are RFID tags [2]. Agrawal

et al. [1] used the EM side-channel to attack countermeasures against power analysis.

One possible way to protect a device from such an adversary is using a logic style for the implementation that minimizes the information leakage. During the last years several proposals of such special logic styles have been presented and evaluated. Some variations of dual-rail precharge (DRP) logic styles turned out to be very promising: the DRP principle prevents the occurrence of security threatening glitches ([6], [11]) by introducing a precharge phase and an evaluation phase in each clock cycle. Furthermore, each data signal in a DRP circuit is represented by two complementary wires. During the precharge phase both of the wires are precharged to zero. In the following evaluation phase only one of the two complementary wires switches to one, depending on the value of the data signal. Some of the DRP logic styles depend on balanced complementary wires, *i.e.* the electrical characteristics as well as the length of two related wires need to be identical to provide an appropriate level of security.

One proposal based on the DRP technique was the improved masked dual-rail precharge logic (iMDPL) style by Popp et al. in 2007 [8]. The iMDPL style combines the strength of dual-rail precharge (DRP) logic styles, *i.e.* the non-existence of glitches, and the hiding properties of cell-level masking which supposedly makes the requirement of balanced complementary wires obsolete.

A detailed investigation of iMDPL has shown that the resistance against power analysis attacks has been significantly increased compared to unprotected CMOS implementations [3]. The results also show that there is still an information leakage in the iMDPL style. Previous research indicates that the mask value could be detected due to routing imbalances in the mask tree ([12], [10]).

Our Contribution. In this work we investigate the effects of routing imbalances in a digital circuit with measurements on a self-developed ASIC prototype chip. The chip has been produced in a $180\,nm$ CMOS process technology and it contains an 8051-microcontroller (μC) and an AES module, both implemented in iMDPL and in plain CMOS logic. We measured the EM emanation with a probe that was stepped over the device. For each measurement point we performed a power analysis attack and therefore we received an image of the data dependencies of the whole chip area for each point in time during the computation. Furthermore, we show that this technique may enable the detailed tracking of certain data flows within a digital design.

This paper is organized as follows. Section 2 describes our EM measurement setup. Section 3 describes the results of our detailed investigation of the iMDPL style. Secton 4 discusses the traceability of data flows by means of stepped EM measurements before conclusions are drawn in Section 5.

2 EM Measurement

The main advantage of EM measurements over power measurements is the flexibility regarding the investigation of specifically small areas on a chip die. Tiniest EM probes enable localized measurements of the emanation of single submodules within a digital circuit. Narrowing down the measured area and the involved modules in the circuit implicates a better quality of the measurements in terms of noise. This has a positive effect on the analysis of the measured traces. Power measurements are usually affected by the power supply grid of the chip, which behaves like a higher-order R-L-C network, as well as induced noise in the power lines of the chip and the measurement resistor connected in series to the chip. Nevertheless, in case of EM measurements care has to be taken that surrounding noise sources do not affect the sensitive measurements somehow.

The measurements on the prototype chip have been performed using a LeCroy WP725Zi 2.5GHz oscilloscope and a self-built coil made of copper wire as an EM probe. Before we started our measurements, we did some comparisons with our handmade coil (diameter $\approx 0.5\,mm$) and a professionally crafted and characterized EM probe with a significantly larger diameter ($\approx 5\,mm$). The measurement results have shown a good conformance (*i.e.* the results of the power analysis attacks matched very well), and hence, we proceeded with our handmade coil. The prototype chip has been operated with a clock frequency of $1.8432\,MHz$. The measurements have been performed at a sampling rate of $5\,GS/s$. We used a 3-dimensional stepping motor setup and processed a $3.45 \times 3.45\,mm$ square with a step size of $0.026\,mm$ on the $3.5 \times 3.5\,mm$ chip-die. These parameters resulted in a total of 17 689 measurement positions, with 1 000 measured power traces at each position.

Our investigations are based on power analysis attacks using the Hamming weight (HW) power model on a move (MOV) instruction in the 8051 μC. The MOV operation has been used to store a known byte value in a cleared register in the internal memory. The resulting correlation traces have then been used to produce data dependency images of the whole chip die for each point in time. In order to simplify our analysis the iMDPL circuit has been supplied with a constant mask value $m = 0$.

3 Investigation of Routing Imbalances in iMDPL

Recent research indicates that the single mask bit in an iMDPL circuit can be discovered due to the fact that imbalances in the mask trees (signal trees for the mask m and the inverted mask $\overline{m}$) cause significant differences in the power consumption. On the one hand, imbalances between two complementary wires in a circuit obviously cause signal-dependent differences in the power consumption of a circuit. On the other hand, such imbalances may also influence the timing of the signals in these wires. In a conventional digital design, which contains multi-bit data paths and considerable multiplexer structures, such imbalances are expected to influence the overall power consumption to a certain degree. Variations in the imbalances among the bits of a uniform data path are somehow

randomly distributed, depending on how the place&route tool has processed each wire. Hence, we expect to encounter significant differences in the power consumption of each bit of the processed byte value in the 8051 μC.

In order to verify these assumptions, we performed a bit-wise power analysis of the stored byte value on the measured EM traces for each measurement step. It turned out that each data bit has a distinct characteristic in the electromagnetic emanation over time on the chip area. The results in Figure 1 show the progress of the correlation over the whole chip area for bit 0 (upper two plots) and bit 3 (lower two plots) for two different points in time ($t_0 = 1.5334\,\mu s$, $t_1 = 1.5354\,\mu s$). It can be seen that at time t_0 bit 0 shows a significant leakage around the coordinates $(80, 60)$ whereas bit 3 does not show any leakage. At time t_1 the results are the other way around: bit 0 does not show a distinct leakage whereas bit 3 shows a significant leakage around the same coordinates as bit 0 at time t_0. We obtained similar results for the other bits: different data bits are leaking information in the same area in the circuit but at different points in time. These results show that the information leakage of each data bit of a uniformly structured data bus has its own specific characteristic (in terms of power / EM emanation and timing) due to routing imbalances. This leads us to the conclusion that also imbalances between the two considerably large mask trees within an iMDPL implementation have significant effects on the power consumption and / or the timing behavior of the design. These findings support the assumptions that routing imbalances may reveal information about the mask and other sensitive data in an iMDPL implementation.

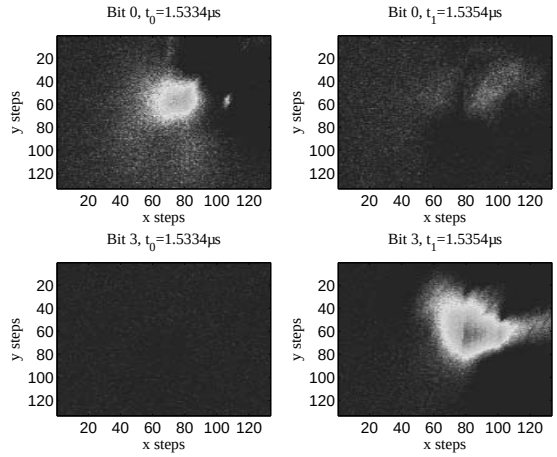

Fig. 1. The progress of the correlation over the whole chip area for bit 0 (upper two plots) and bit 3 (lower two plots) at two different points in time $t_0 = 1.5334\,\mu s$ (left two plots) and $t_1 = 1.5354\,\mu s$ (right two plots); the bright areas indicate a higher correlation.

4 Traceability of the Data Flow within the Circuitry

The investigation of iMDPL has shown that different bits leak information at different moments in time. Further investigations have indicated that each bit is leaking information at different areas in the circuit at different points in time. Figure 2 depicts the correlation results over the whole chip area for bit 0 at four different points in time. It can be seen that the bright leakage spots somehow transform with the advance in the time dimension. This behavior could also be used to track the data flow within a design.

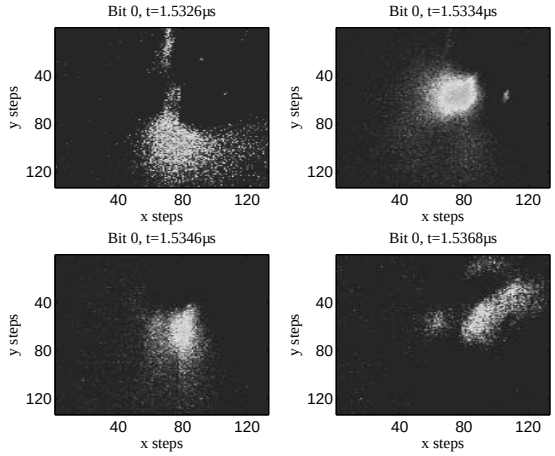

Fig. 2. The progress of the correlation over the whole chip area for bit 0 at four different points in time; the bright areas indicate a higher correlation.

5 Conclusions and Future Work

In this work we have shown that stepped EM measurements are a powerful way to perform detailed and manifold investigations of a device. The analysis of the measurements of an iMDPL implementation supports the assumptions that routing imbalances in a masked DRP logic style harbor the risk of exposing information about the mask value in the circuit. Furthermore, our investigations have shown that it is possible to track certain data flows within the design. There is yet some unexploited potential left in this technique. With a finer-grained stepping in combination with a smaller and more precise EM probe it should be possible to figure out even more profound details about the device under test. Our current work in progress also involves stepped EM measurements on the iMDPL prototype chip supplied with a random mask bit in every clock cycle as well as a finer-grained measurement with different active modules in the μC.

Acknowledgements. Parts of the research described in this paper have been supported by the Austrian Science Fund (FWF) under grant number P22241-N23 ("Investigation of Implementation Attacks").

References

1. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM Side-channel(s). In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*.
2. M. Hutter, S. Mangard, and M. Feldhofer. Power and EM Attacks on Passive 13.56 MHz RFID Devices. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*.
3. M. Kirschbaum and T. Popp. Evaluation of a DPA-Resistant Prototype Chip. In *25th Annual Computer Security Applications Conference (ACSAC 2009), 7-11 December 2009, Honolulu, Hawaii, USA*, 2009.
4. P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In N. Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*.
5. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In M. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*.
6. S. Mangard, T. Popp, and B. M. Gammel. Side-Channel Leakage of Masked CMOS Gates. In A. Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*.
7. E. D. Mulder, S. Örs., B. Preneel, and I. Verbauwhede. Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems. In *Automation Congress, 2006. WAC '06. World*, pages 1—6, 2006.
8. T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard. Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*.
9. J.-J. Quisquater and D. Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In I. Attali and T. P. Jensen, editors, *Smart Card Programming and Security, International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, September 19-21, 2001, Proceedings*.
10. P. Schaumont and K. Tiri. Masking and Dual-Rail Logic Dont Add Up. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*.
11. D. Suzuki, M. Saeki, and T. Ichikawa. Random Switching Logic: A Countermeasure against DPA based on Transition Probability. Cryptology ePrint Archive (`http://eprint.iacr.org/`), Report 2004/346, December 2004.
12. K. Tiri and P. Schaumont. Changing the Odds against Masked Logic. In E. Biham and A. M.Youssef, editors, *Selected Areas in Cryptography, 13th International Workshop, SAC 2006, Montreal, Quebec, Canada, August 17-18, 2006, Revised Selected Papers*.