Influence of Electrical Circuits of ECC Designs on Shape of Electromagnetic Traces measured on FPGA

Christian Wittke, Zoya Dyka, and Peter Langendoerfer
System dept.,
IHP, Im Technologiepark 25,
15236 Frankfurt(Oder), Germany
[wittke| dyka| langendoerfer]@ihp-microelectronics.com

Abstract**—** *Side channel attacks take advantage from the fact that the behavior of crypto implementations can be observed and provides hints that simplify revealing keys. The energy consumption of the chip that performs a cryptographic operation depends on its inputs, on the used cryptographic key and on the circuit that realizes the cryptographic algorithm. An attacker can experiment with different inputs and key candidates: he studies the influence of these parameters on the shape of measured traces with the goal to extract the key. The main assumption is here that the circuit of the attacked devices is constant. In this paper we investigated the influence of variable circuits on the shape of electromagnetic traces. We changed only a part of the cryptographic designs i.e. the partial multiplier of our ECC designs. This part calculates always the same function in a single clock cycle. The rest of the design was kept unchanged. So, we obtained designs with significantly different circuits: in our experiments the number of used FPGAs LUTs differs up to 15%. These differences in the circuits caused a big difference in the shape of electromagnetic traces even when the same data and the same key are processed. Our experiments show that the influence of different circuits on the shape of traces is comparable with the influence of different inputs. We assume that this fact can be used as a protection means against side channel attacks, especially if the cryptographic circuit can be changed before the cryptographic operation is executed or dynamically, i.e. while the cryptographic operation is processed.*

Keywords — countermeasures against side-channel attacks, FPGA, electromagnetic traces

I. Introduction

The side channel attacks are a relevant threat if attacked devices can be accessed physically, for example in wireless sensor networks.

In this paper we investigated the influence of circuits of crypto devices on the shape of electromagnetic traces. We assume that individualizing of electrical circuits can be used as a protection means against side channel attacks. The basic idea of such attacks is that the inputs of cryptographic devices and used cryptographic key causes switching of the gates of the attacked circuit. It means that observing power consumption or electromagnetic radiation of the chip, while the cryptographic operation is calculated, can be used for extraction of the cryptographic key. Usually an attacker collects a lot of traces with different inputs for analyzing them and many traces with the same inputs to decrease the influence of noise. The attacker can separately investigate the influence of different parameter on the shape of measured traces: only the key influence, if different key candidates can be processed; only the data influence, if he can give different inputs that will be processed with the same key; different environment parameters such light, temperature, etc. if all other parameters are constant. The basic assumption of such investigation is that the attacked circuit is the same, i.e. constant.

In this paper we show that the influence of different circuits on the shape of electromagnetic trace is comparable with the influence of other parameters like inputs or cryptographic key. We assume this fact can be used as protection means against side channel attacks.

The rest of this paper is structured as follows. In section II we introduce the idea of our approach and the substantial basics with respect to the cryptographic operations we use for individualizing crypto devices. Section III presents the measurement setup and also discusses the measurement results i.e. the electromagnetic traces of the individualized designs. The paper finishes with short conclusions.

II. Individualizing cryptographic designs

To prevent exploiting the difference of side-channel leakages we propose individualizing of cryptographic designs. The idea is that devices with the same functionality can have a different i.e. individual circuit. Important is that not only the chip topology after place-and-route but also the number of used gates is individual. This results in an individual power consumption, electromagnetic radiation, etc.

A. Individualization of GF(2^n)-ECC designs

Typically an ECC design consists of registers, of the arithmetic-logic unit (ALU) that performs additions and squaring of its operands and of the field multiplication unit (MULT) that calculates the product of its operands. The necessary sequence of these mathematical operations is organized by the controller unit (see Fig. 1). The controller manages each unit when it may read the data from the bus (blue line in Fig. 1) and process these data as inputs and when it may write the result of calculation to the bus.

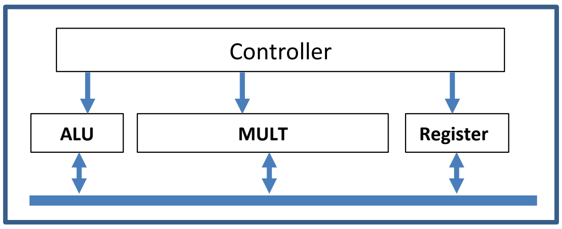

Fig. 1. Typical structure of an ECC design: the ALU performs addition and squaring of its operands; MULT calculates the product of its operands; the Controller organizes the necessary sequence of mathematical operations.

ECC-designs can be individualized using different multiplication methods (MM) for field multiplication. The field multiplication can be performed in two steps. The first step is the multiplication of two polynomials of length *n* that results in their (*2n-1*) bit product. The second step is the reduction of this polynomial product using the so called irreducible polynomial.

The polynomial multiplication (i.e. of the first step of the field multiplication) is an expensive task with respect to time, area and energy since the length of multiplicands is typically large (about 200 bit); therefore many optimizations have been proposed in the past. Many multiplication methods apply segmentation of both multiplicands into the same number of parts. The product then is calculated as a sum of smaller partial products. Historically, the first optimization of the classical multiplication method was the Karatsuba multiplication method published in 1962 [1]. This method uses the segmentation of polynomials into two terms. The next one was proposed by Winograd in 1980 [2]. This method uses the segmentation of polynomials into three terms. At the moment there exist more than 10 different multiplication formulae. Each multiplication formula has its own segmentation of operands, its own number of partial products of these short – only one segment long – operands and its own number of additions of the obtained partial products, i.e. its own complexity.

Moreover the multiplication methods can be combined. Each combination of MMs also has its own complexity. The set of different combinations is very large. This fact can be used for individualizing multiplier designs and so for individualizing ECC designs.

B. Investigated ECC designs

To proof our idea we implemented and compared three different designs of elliptic curve point multiplication or – shortly – the *kP* operation for the NIST EC *B-233* [3]. We implemented the *kP*-operation using the Montgomery elliptic curve point multiplication algorithm in Lopez-Dahab coordinates. The implementation details are given in [4]. All three designs differ only in their partial multiplier. The partial multiplier is a part of the field multiplier and calculates a product of 60-bit long operands in a single clock cycle. The field multiplier needs 9 clock cycles to accumulate all partial products to obtain the product of 233-bit long operands.

Table I gives details of the investigated designs.

TABLE I. IMPLEMENTATION DETAILS OF INVESTIGATED ECC DESIGNS

ECC design	**Used Spartan-6 *FPGA-resources***		**partial multiplier implementing:**
	registers	***LUTs***	
design1	3 283	6 522	the classical MM only
design2	2 997	5 649	selected combination of two MMs: the iterative 4-segment Karatsuba MM [5] and the classical MM
design3	3 274	6 290	random combination of 3 MMs: the iterative 4-segment Karatsuba MM, the iterative 3-segment Winograd MM [6], the classical MM

As explained above we implemented the partial multipliers using the classical (or the school-book) MM for our first design. Our second design is a combination of the classical MM and our 4-segment iterative Karatsuba MM. The combination of MMs used for our 3rd design was selected randomly. We do not give the details here for simplifying the reading. The important fact is that the complexity of these MMs is different. It results in different circuits that use the different FPGA-resources. For example, *design1* uses 15% more LUTs than *design2*.

III. Measurement Results

A. Measurement setup

Fig. 2 shows our measurement setup. All our ECC designs run at 4 MHz in the Spartan-6 FPGA from Xilinx [7] on the Fault Extension Board (FEB) from TU Graz. The FEB was especially designed for the measurement of power and electromagnetic traces of designs running on the FPGA. The red curve on the oscilloscope shows the electromagnetic trace (EMT). We used the shielded high sensitivity Riscure electromagnetic probe 4.0 [8] for the measurement of the electromagnetic traces. Each trace was measured using LeCroy Waverunner 610Zi oscilloscope with a 2.5 GS/s sampling rate, i.e. with about 600 measurement points per clock cycle.

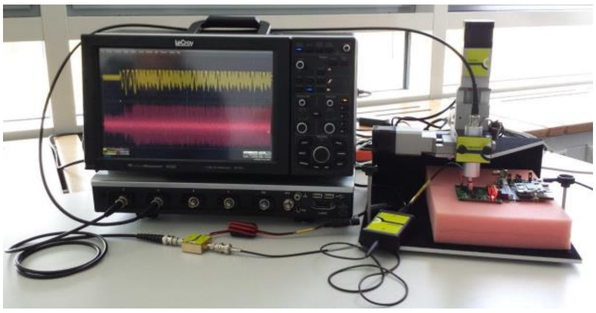

Fig. 2. Measurement setup for collecting electromagnetic traces.

The FPGA was not decapsulated and we decided not make any electromagnetic cartography of the chip surface. Instead we x-rayed a Spartan-6 to detect where the ASIC really is. The chip has a size of 7mm x 7mm and is placed in a 19mm x 19mm BGA package.

For our measurements we placed the electromagnetic probe over the middle of the FPGA close to the package surface. We decided to do our measurements in this way for the following reasons:

- The inner diameter of the shielding of the Riscure probe we used is about 6mm, i.e. it covers almost the complete 7mm x7mm IC of the FPGA
- We wanted to avoid noise stemming from bond wires
- We wanted to have identical conditions for all designs.

Each implemented ECC design has its own complexity and circuit resulting in its – individual – electromagnetic radiation. The measured EMTs are given and discussed in the next section.

B. Individualized electromagnetic Traces

Fig. 3 shows a part of the measured traces. More precisely the shown part of the trace corresponds to the first 3 clock cycles of the processing of the 4th bit of the cryptographic key. The processing of one key bit takes always 57 clock cycles in our implementations. The key is 232 bit long and the whole processing time is about 13000 clock cycles. To investigate the influence of the individualized designs we are using the same inputs for all designs. Thus, the influence of different inputs on the measurement results was excluded. The yellow line in Fig. 3 depicts the EM-trace of the *design1*. The violet line shows the EM-traces of *design2* and the blue line denotes the EM-trace of *design3*. We synchronized the investigated traces using software provided by Riscure.

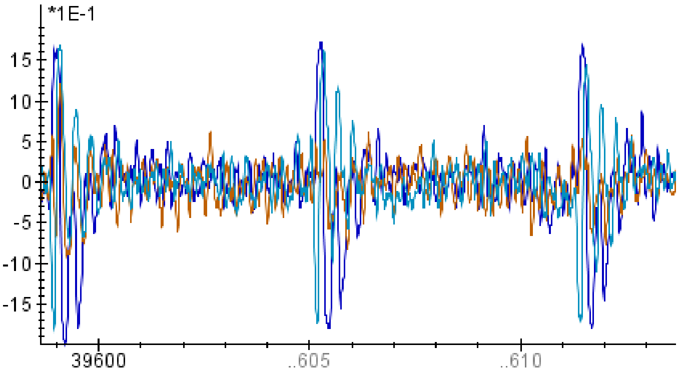

Fig. 3. Measurement results: the same part of the electromagnetic trace of the kP-operation of all three ECC designs: the yellow line depicts the electromagnetic traces of *design1*; the violet line shows the EMT of *design2*; the blue line shows the EMT of *design3*.

The measurement results confirm our idea i.e. the shapes of the electromagnetic traces are different for all three designs (see Fig. 3) even though they all process identical data.

In order to quantify the effect of our idea at least to a certain extend we compared measured traces of different design with each other to show the differences, and we also compared the differences of repeated measurements, i.e. with the same input using the same design to show the noise. We did this for all three designs but are going to present these results only for *design1*.

Fig. 4 shows the absolute differences of the electromagnetic traces for the whole kP operation. The top curve in in Fig. 4, denoted as '*difference 1*', depicts the differences between repeated measurements with the same inputs. The next two curves, denoted as '*difference 2*' and '*difference 3*', show the influence of different inputs on *design1*: the curve *difference 2* displays the differences if only one of 3 large inputs – the key – was changed and the curve *difference 3* corresponds to the case in which all 3 inputs – the key and the both coordinates of EC point – are different. The curves *difference 4* and *difference 5* display the differences if the circuit was different: *design1*-to-*design2* and *design1*-to-*design3* respectively if the same inputs are processed. Note these curves visualize the influence of the individualization of the designs.

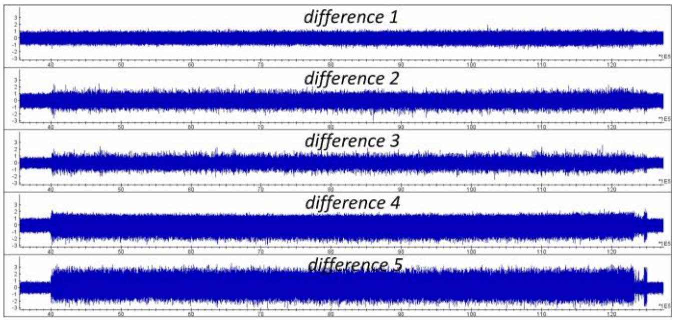

Fig. 4. Differences of measured electromagnetic traces.

Table II shows the list of all curves in Fig. 4 and give a short overview of parameters that we experimented with.

TABLE II. SHORT DESCRIPTION OF INVESTIGATED ECC DESIGNS

Curve in Fig.4	**Changed parameters**			**Cause of the differences**
	key	*EC Punkt P=(x,y)*	*circuit*	
difference 1	*same*	*same*	*same*	noise
difference 2	√	*same*	*same*	influence of the *key*
difference 3	√	√	*same*	influence of the inputs and the *key*
difference 4	*same*	*same*	*design1 -to- design2*	influence of the circuit, example 1
difference 5	*same*	*same*	*design1 -to- design3*	influence of the circuit, example 2

It can be seen, that the differences between two repeated measurements of the same design (the curve *difference 1* in Fig. 4) are comparable with the noise. Compared to that, the influence of the individualized designs however is significant (see curves *difference 4* and *difference 5* in Fig. 4) and comparable with the influence of different inputs (see curves *difference 2* and *difference 3* in Fig. 4).

IV CONCLUSION

In this paper we introduced the idea to use different circuits with the same functionality as a promising means to cope with side channel attacks. The idea of individualizing the circuit can be applied to each design, if its functionality can be implemented in different ways. We selected elliptic curve cryptography, i.e. the implementation of the required field multipliers, as sample application. The advantage of this type of operation is that a plethora of different multiplication methods that provide the same operation are available. By unifying the interfaces we are capable of combining different multiplication methods. These multiplication methods can be selected at will or randomly. The differences in the observable behavior of the resulting multipliers stem from the different complexity of the multiplication methods that influence the resources needed to implement the multipliers as well as the related energy consumption and electromagnetic radiation. We implemented three designs using different combinations of three MMs. Our measurement results show significant variations in resources and electromagnetic traces.

In our next research steps we will investigate whether individualizing circuits can be used as a protection means against side channel analysis.

ACKNOWLEDGEMENTS

The work presented in this paper has been partially funded by LASA under grant number 1389053.

[1] A. Karatsuba, A., Ofman, Y.: *Multiplication of Many-Digital Numbers by Automatic Computers*. Doklady Akad. Nauk SSSR, Vol. 145 (1962), pp: 293–294. Translation in Physics-Doklady, 7 (1963), pp. 595–596.

[2] S. Winograd: *Arithmetic Complexity of Computations*. SIAM (1980)

[3] NIST Digital Signature Standard (DSS), FIPS PUB 186-4, July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[4] S. Peter: *Evaluation of Design Alternatives for Flexible Elliptic Curve Hardware Accelerators*, Diplom Thesis, 2006, http://www.ics.uci.edu/~steffenp/files/da_peter.pdf

[5] Z. Dyka, P. Langendoerfer: *Area efficient hardware implementation of elliptic curve cryptography by iteratively applying Karatsubas method*, Proc. of the Design, Automation and Test in Europe (DATE 2005), 2005, Vol.3, pp: 70-75

[6] Z. Dyka, P. Langendoerfer, F. Vater, S. Peter: *Towards strong security in embedded and pervasive systems: energy and area optimized serial polynomial multipliers in GF(2^k)*, Proc. of IEEE New Technologies, Mobility and Security, 5th International Conference (NTMS-2012), 2012, pp. 1-6

[7] Xilinx Inc.: Spartan-6 Family Overview, Product Specification, DS160 (v2.0) October 25, 2011, http://www.xilinx.com/support/documentation/data_sheets/ds160.pdf

[8] Riscure: Inspector data sheet: EM Probe Station. https://www.riscure.com/benzine/documents/EMProbeStation.pdf