# FPGA-based Testing Strategy for Cryptographic Chips: A Case Study on Elliptic Curve Processor for RFID Tags

Junfeng Fan, Miroslav Knežević, Duško Karaklajić, Roel Maes,
Vladimir Rozić, Lejla Batina and Ingrid Verbauwhede
Katholieke Universiteit Leuven, ESAT/SCD-COSIC,
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee, Belgium
{firstname.lastname}@esat.kuleuven.be

## Abstract

*Testing of cryptographic chips or components has one extra dimension: physical security. The chip designers should improve the design if it leaks too much information through side-channels, such as timing, power consumption, electric-magnetic radiation, and so on. This requires an evaluation of the security level of the chip under different side-channel attacks before it is manufactured. This paper presents an FPGA-based testing strategy for cryptographic chips. Using a block-based architecture, a testing bus and a shadow FPGA, we are able to check information leakage of each block. We describe this strategy with an Elliptic Curve Cryptosystem (ECC) for RFID tags.*

## 1 Introduction

Public Key Cryptosystems (PKC) such as Elliptic Curve Cryptosystem (ECC) are used in RFID tags [7] to provide chip authentication to the reader. Implementing ECC on such a small device with limited power budgets is a challenge. Side-channels attacks, such as Timing Analysis (TA) [5], Power Analysis (PA) [6] and Fault Analysis (FA) [2], have been studied extensively in recent years. As a result, the designers of cryptographic chips/components need to evaluate how much information is leaked though the side-channels, and improve the design if necessary. In this paper, we propose a strategy of testing cryptographic chips/components using FPGAs. Though the term "testing" normally means on-line testing of the manufactured chip, here we also use it to denote estimation of physical security in the design phase. It is also because that the proposed strategy enable a FPGA-based environment for on-line testing of the manufactured chip. The strategy mainly consists of (1) block-based design for testing, (2) shadow implementation and (3) attack-based security check. We will present the details with a case study on an ECC implementation for RFID tags.

The rest of the paper is organized as follows. Section 2 describes the general strategy for testing of cryptographic chips. In Section 3 we present a case study on testing ECC implementations. We conclude the paper in Section 4.

## 2 A general testing strategy for cryptographic chips

For cryptographic hardware, there are mainly two types of testing: functionality and security. While functionality can be tested with traditional methods, such as a scan-chain, the security testing requires specific knowledge about the cryptosystem and related attacks. Figure 1 shows the front-end design flow of cryptographic hardware. Here functionality verification is to check the output of circuit with the reference model, while the security estimation is to check how much information is leaked through side-channels and how likely it will be broken by known attacks. If the test results indicate vulnerabilities, the design must be modified to eliminate it.

With the proposed method, all the blocks are connected to a testing bus, which can make the ports of each block external. The testing bus consists of only combinational logic and should not increase the critical path delay. A shadow of a block, say block X, is the complete implementation except block X. Using two FPGA boards, we could do fast testing on any block. For instance, in order to test block X, the design is configured so that looking from outside the whole design is just block X. X's shadow is implemented on FPGA2. These two FPGAs are connected with testing bus, making a complete implementation. With this method, we avoid generating waveform for testing circuitry and comparing the output with reference data. When the chip is

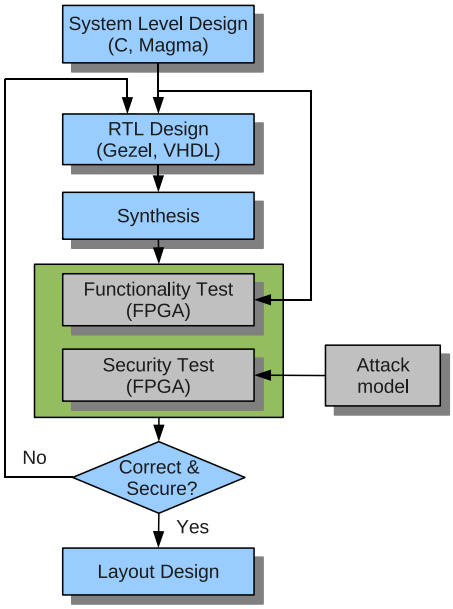


**Figure 1. Cryptographic hardware design flow**

taped out, we can simply replace FPGA1 with the chip, and start testing each block immediately.

## 3 A case study on ECC implementation

We present the test strategy in detail with a case study. An ECC processor is designed for RFID tags. We will test the functionality and security of the ECC implementation with the method described above.

### 3.1 ECC processor

In ECC based cryptographic protocols, the curve $\mathbb{E}$ is defined over a finite field $\mathbb{K}$. A nice mathematical background of ECC can be found in [3]. Given a point P on $\mathbb{E}$ and an integer $k$, the ECC engine calculates Q=$k$P. It is believed that finding out $k$ from P and Q is a $hard$ problem in mathematics. Using this feature, ECC supports data encryption/decryption, key agreement and identity authentication. Alg. 1 describes a method to compute $k$P.

Figure 2 shows block diagram of the ECC implementation with a shadow. It consists of a microprocessor, Elliptic Curve Processor (ECP) which contains a Modular Arithmetic Logic Unit (MALU) and a register file, a True Random Number Generator (TRNG) and a ROM to store the curve parameters. All the blocks are connected to a BUS. A testing bus is inserted in the ECC processor such that each block is accessible from outside. Here the module under test is ECP, which is the main source of area and power consumption. On FPGA1, the ECP is selected, and all the rest is shut down. On FPGA2, ECP's shadow implementation is downloaded. The components implemented on FPGA2 (shadow) are carefully verified and now serve as a testing environment after the chip is manufactured.

**Algorithm 1** Compute $k$P Using Montgomery Ladder [4].

**Input:** $P = (x_p, y_p)$, $k = (k_{l-1}k_{l-2}\cdots k_0)_2$
**Output:** $Q = (x_q, y_q) = kP$

1: $P_1 \leftarrow P$, $P_0 \leftarrow 2P$
2: **for** $i$ from $l-2$ downto 0 **do**
3: $\quad P_{[k_i]} \leftarrow P_1 + P_0$, $P_{[1-k_i]} \leftarrow 2P_{[1-k_i]}$
4: **end for**
5: Return $P_1$

### 3.2 Security test

Security test is driven by attack models. Successful attacks on ECC with different methods, i.e. TA,PA and FA have been reported. In this paper we present the preliminary results of TA/SPA on this ECC implementation.

**Timing Analysis (TA)**

TA on ECC scalar multiplication is usually based on the fact that the delay of operations when key bit is 1 might be different from that of key bit 0. The algorithm used in this chip, the Montgomery Ladder, is supposed to be secure against TA. However, in practice it can still be vulnerable if

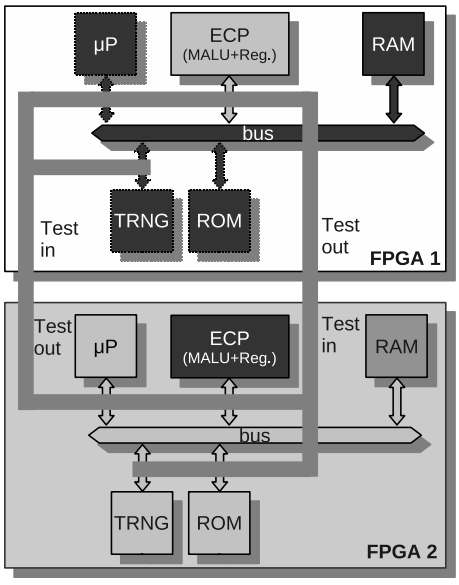


**Figure 2. Testing methods for ECC processor**

it is not carefully implemented.

**Simple Power Analysis (SPA)**

Simple Power Analysis on ECC scalar multiplication is based on the fact that power consumption may differ when key bit is 1 or 0. Note that even if the same number of clock cycles are used for each key bit, different patterns in the power trace can reveal key bit.

### 3.2.1 On board test

The design shown in Figure 4 is implemented and tested. We choose the SASEBO board [1] as the platform. The SASEBO board is designed for the purpose of side-channel attack evaluation. It has two FPGAs, a control FPGA and a target FPGA. We put the ECC processor on the target FPGA and the shadow on the control FPGA. The power consumption of ECP during a scalar multiplication is measured. Both FPGAs work on a clock frequency of 1 MHz. Figure 3 shows the power trace of the first 4000 clock cycles. One can clearly see parameter loading in the beginning and 10 iterations of Algorithm 1 afterwards.

Figure 3 shows that each iteration takes the same time. This means that Algorithm 1 was carefully balanced for key bit being 1 and 0, and attackers can hardly reveal the key stream using Timing Analysis. A preliminary inspection on the the power trace shows no obvious patterns repeating for $k_i = 1$ or $k_0 = 0$, which means the implementation of ECC is SPA resistant to a certain degree.

Since ASIC has different layout from FPGA implementations, the security estimation on FPGA can only serve as an indication but not a guarantee. The security of a design against side-channel attacks can only be evaluated after the chip is produced. However, the approach described above enables an early estimation of information leakage in the design phase. Besides, as shown in Fig 3, the block-based testing allows a more precise measurement on the information leakage.

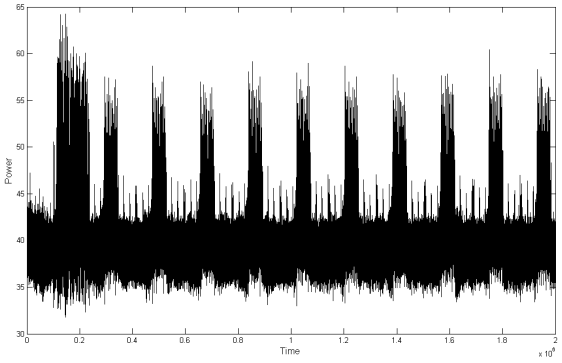


**Figure 3. Averaged power trace of the ECP component during point multiplication**

## 4 Conclusions

We propose a strategy for testing cryptographic designs with FPGA boards. Using block-based architecture and shadow implementation, the functionality of each component can be easily tested. Moreover, this strategy gives an early estimation of physical security. Each component of the chip can be tested alone, giving a more accurate estimation of information leakage than measuring the whole design.

## Acknowledgements

This work was supported in part by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), by FWO projects G.0475.05, and G.0300.07, by IWT-Vlaanderen under grant number 71369, by the European Comission through the IST Programme under Contract IST-2002-507932 ECRYPT NoE, and by the K.U. Leuven-BOF.

The author also want to thank Akashi Satoh (National Institute of Advanced Industrial Science and Technology, Japan) and designers of SASEBO.

## References

[1] *Side-channel Attack Standard Evaluation Board*. http://www.rcis.aist.go.jp/special/SASEBO/SASEBO-G-en.html.

[2] D. Boneh, R. DeMillo, and R. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In W. Fumy, editor, *Advances in Cryptology: Proceedings of EUROCRYPT'97*, number 1233 in Lecture Notes in Computer Science, pages 37–51. Springer-Verlag, 1997.

[3] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curves Cryptography*. Springer-Verlag, 2004.

[4] M. Joye and S. ming Yen. The montgomery powering ladder. In *CHES 2002, LNCS*, pages 291–302. Springer-Verlag, 2003.

[5] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. In N. Koblitz, editor, *Advances in Cryptology: Proceedings of CRYPTO'96*, number 1109 in Lecture Notes in Computer Science, pages 104–113. Springer-Verlag, 1996.

[6] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology: Proceedings of CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 388–397. Springer-Verlag, 1999.

[7] Y. K. Lee, L. Batina, and I. Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In *RFID, 2008 IEEE International Conference on*, 2008.