A NOVEL ASYNCHRONOUS E-FPGA ARCHITECTURE FOR SECURITY APPLICATIONS

Taha Beyrouthy, Alin Razafindraibe, Laurent Fesquet, Marc Renaudin
TIMA Laboratory
Institut National Polytechnique de Grenoble
46 Avenue Félix Viallet 38031 Grenoble France
email: taha.beyrouthy@imag.fr

Sumanta Chaudhuri, Sylvain Guilley Philippe Hoogvorst, Jean-Luc Danger
Ecole Nationale Supérieure des Télécoms
46 rue Barrault
75634 Paris cedex 13 France
email: Sumanta.Chaudhuri @enst.fr

ABSTRACT

With the growing security needs of applications such as homeland security or banking, the frequent updates in cryptographic standards and the high ASIC costs, the ciphering algorithms on an asynchronous embedded FPGA co-processor are becoming a viable alternative. Within the SAFE project, a novel architecture of asynchronous e-FPGA has been proposed. This architecture is natively robust against side channel attacks such as simple and differential power analysis or clock based fault attacks. Simulation-based security proofs are also presented.

1. INTRODUCTION

The past two decades have seen the increasing attractiveness of programmable circuits that proved their validation role in the logic design flow and their high level of flexibility. At the same time, asynchronous circuits are more and more used in order to remove the clock distribution problems and the power consumption overhead which drastically increases with frequency. Moreover, because of their weak sensitivity to the so-called Side-Channel Attacks (SCAs) which aim at illegally retrieving secret information contained in cryptographic systems, the asynchronous circuits appear to be an interesting alternative to their synchronous counterparts for implementing cryptosystems [9].

In the literature, several architectures of programmable asynchronous circuits have been proposed (PGA-STC [3], PAPA[5], Achronix [12] FPGAs GALSA [4]. From the security point of view, all these FPGAs are vulnerable to Differential Power Analysis (DPA) attacks and more generally to SCAs attacks. In spite of this situation, very few research works address the FPGA security.
In this context, the "SAFE" project aims at specifying, designing and validating an asynchronous programmable circuit suitable for secure implementations. Whitin this project, we propose a novel architecture which is natively robust to DPA attacks and which appears to be more flexible than the actual asynchronous programmable circuits. To achieve such a level of robustness, all security problems are addressed at all abstraction layers: architectural, logical, electrical and physical (routing).

2. SECURITY FEATURES OF THE SAFE FPGA

The FPGA reconfigurability offers major advantages for cryptographic applications [11]. However, the physical implementation of FPGAs might provide a side-channel that leaks unwanted information. Examples for side-channels include in particular: power consumption, timing behavior, electromagnetic radiation, surface temperature, etc. All of these side-channels are information sources which can potentially be used by attackers to reveal the secret key. Simple Power Analysis (SPA) and Differential Power Analysis (DPA) are introduced in [6]. While performing a cyphering operation, the power consumption of cryptographic devices, are analyzed in order to extract the secret cipher keys. These attacks exploit the data-dependent power consumption of the cryptographic device in order to reveal the secret information.

Many countermeasures have recently been implemented in ASICs to prevent SPA, DPA, EMA and FAs. One approach — using balanced quasi delay insensitive (QDI) asynchronous circuits [7] — appears to be one of the most promising. The SAFE project aims at transposing this method in an e-FPGA context. The challenge is first to make the asynchronous FPGA natively robust against SPA and DPA while being very flexible. Afterwards, countermeasures against other SCAs and FAs can be easily explored and experimented. The SAFE e-FPGA is expected to have a number of advantages for security:
Balanced power consumption — QDI circuits which generally use 1-of-n encoding (for example: dual-rail, triple-rail, etc.) can be balanced to reduce the power consumption dependency with the processed data. Indeed, the bit encoding ensures that the data are transmitted and computations are performed with a constant Hamming weight. This is important since the leakage of the Hamming weight or distance can be exploited by SPA, DPA, and EMA.

Absence of a global clock signal — No clock means that FAs based on clock are removed. Moreover, DPA and SPA attacks without global clock signal are expected to be much more difficult. Indeed, the clock absence will make very complicated the synchronization of the DPA and SPA signatures.

Environment variation tolerance — QDI circuits adapt to their environment such as voltage and temperature variations, which means that they tolerate many forms of fault injection (power glitches, thermal gradients, etc). These QDI circuits can be easily combined with other countermeasure to efficiently counteract FAs [8].

Redundant data encoding — QDI circuits typically use a redundant encoding scheme (1-of-n). For example, the dual-rail encoding (a bit is encoded onto two wires) provides a mean to encode an alarm signal to counteract FAs [7].

3. E-FPGA ARCHITECTURE

This section gives an overview of the proposed architecture of the asynchronous FPGA. Our proposed programmable Logic bloc architecture consists of 4 major blocks: 2 Logic elements each including 2 LUT6-1 (6 inputs - 1 output), 1 LUT 2-1 and 1 LUT4-1.

3.1. General description of the FPGA architecture

The global architecture of the e-FPGA is an Island-style architecture composed by Programmable Logic Blocks (PLBs).

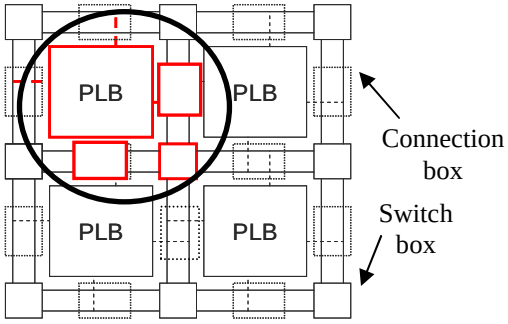

Figure 1: e-FPGA architecture.

As a classical FPGA, it also contains a programmable routing whose the building blocks are Connection Boxes (CBs) and Switch Boxes (SBs) [1], [2]. Finally, the e-FPGA architecture is the repetition in 2-dimension of the pattern made by a PLB, 2 connection boxes, and a switch box as described in **Figure 1**.

3.1.1. The Programable Logic Block

The PLB architecture has been designed to be a good compromise between the high flexibility required to be style independent and the optimal use of PLB resources. Figure 2 shows the details of the PLB architecture, which has 12 inputs and 7 outputs. Its outputs are directly connected to the connection boxes. It consists in two Logic Element (LE), one Look-Up-Table 2-1 (LUT2-1), and one Look-Up-Table 4-1 (LUT4-1).

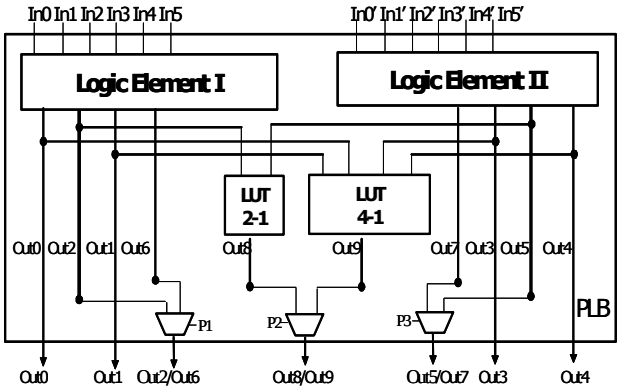

Figure 2: PLB architecture.

3.2. Technology mapping

The e-FPGA is a reconfigurable integrated circuit that is formed essentially by a sea of PLBs surrounded by a programmable routing structure. The PLBs are based on the 6-input lookup table (LUT6-1) where a LUT6-1 contains 2^6 truth table configuration bits so it can implement any 6-input function.
On the one hand, the number of PLBs needed to implement a given circuit determines the size and cost of the FPGA. On the other hand, its security depends on the symmetry of the whole PLB network. Therefore one of the most important phases of the FPGA design flow is the technology mapping step which maps the optimized circuit description into a PLB network.

The goal of the technology mapping step is first to balance the architecture of the whole circuit and second to reduce area and delay. Within the SAFE project, the algorithm of technology mapping allows keeping the symmetry when implementing "balanced function". Therefore, it allows a secure implementation of asynchronous circuits regardless both the encoding style (1-of-n encoding) and the communication protocol (2-phase or 4-phase). More precisely, this algorithm is able to implement balanced functions with the following features:

Area-efficient: the implementation will use the minimum of PLB's resources.

Secure: the whole circuit will be balanced at the architectural level. In the case of a complex function (K-input, K>7), the algorithm is able to split the latter into many smaller functions (K-input, K<7). Afterwards, the algorithm is able to map each small function on a PLB and implement a fully balanced circuit (Balanced tree topology). More precisely, in a logical cone, each input is propagated from input to output through the same number of blocks.

3.3. Physical implementation of LUTs

This section addresses the implementation of the LUTs which compose the PLBs. The basic idea is to design these LUTs to ensure that the benefits of the balanced architecture – in terms of security – are not lost. With this intention, we focus on the logical and electrical features of the LUTs to keep FPGA safe against power and electromagnetic based attacks. Thus, the challenge is to implement each LUT to ensure that the power consumption is data independent.
A LUT is a direct implementation of a truth table. It is composed by a memory part to store the configuration bits and a decoder part. A classical LUT implementation is presented in figure 5.

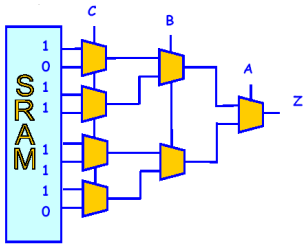

Figure 3: Classical LUT implementation.

From the security point of view, the above classical LUT implementation exhibits drawbacks:

Single rail encoding: Simple binary encoding of data, where one wire is used to propagate one bit, results in power consumption proportional to the number of state changes. As a result, power consumption is expected to be data dependent or Hamming weight dependent.

Unbalanced input capacitances: If we refer to the above figure, the capacitance of pin C is the highest and the one of A is the smaller. At electrical level, it means that power consumption differs according to the switching input(s).

Timing variation: Referring the above figure, the number of logical depth crossed by data differs according to the inputs activity. As the timing directly depends on this number, the current waveforms and thus the power consumption depend on the input activity, which is not desirable for security.

At logical level, we remove the security problems induced by the binary encoding by using dual-rail encoding which is supported by the LEs. In this case, the Hamming weight is constant.

At electrical level, to keep the benefits of using dual-rail encoding and the well-balanced architecture, all input capacitances has been balanced to ensure constant power consumption. Finally to avoid timing variation, in addition to the balanced input capacitances, a unique logical depth is imposed between the configuration bits and the LUT output and all data paths in the Decoder are well balanced. These is implemented first by using an array of switches between the configuration bits and the LUT output and second by correctly adjusting the sizes of the Decoder's inverters (see Figure 4).

Hazard freeness issues

To avoid malfunction, the asynchronous circuit must be hazard-free. To guarantee this constraint, a better coordination between the configuration bits and the possible combinations of the Decoder's inputs is needed. In fact, this problem is solved by the synthesis tool which takes into account the encoding style, the details of the implementation and the communication protocol (2-phase or 4-phase) [10].

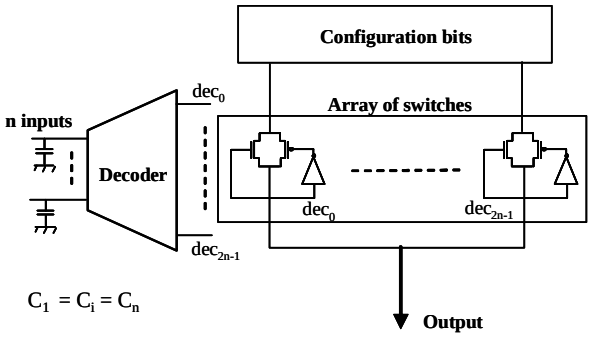

Figure 4: Balanced LUT implementation.

4. EXPERIMENTAL RESULTS

In this section, a sensitive sub-module of the DES (Data Encryption Standard) algorithm is studied (see Figure 5). A brief presentation describes the design and the architecture used to secure this module and make its consumption data-independent. Experimental results show that power consumption is data-independent.

4.1. Mapping a sensitive DES sub-module.

Figure 5 shows that the combination of the plaintext with the secret key is done by a 6-input XOR. It is important to ensure a high level of security on this bloc and on the S-BOX [12]. Otherwise a hacker could easily retrieve, through a power consumption analysis the secret key used during the encryption.
In terms of resource, 8 PLBs are required to have an implementation of this sub-module that respects the security constraints. The XOR is implemented on three PLBs and five are used to implement the 6-input dual-rail S-BOX2 (6 dual-rail inputs, 4 dual-rail outputs).

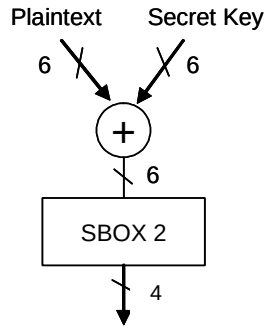

Figure 5 : Experimental setup.

In order to evaluate the area efficiency of the bloc implementation, a filling ratio described below has been calculated. The filling ratio of the LEs is defined as the number of used primary inputs over the total number of primary inputs. The Logic Element (LE) of the PLB has in total 6 primary inputs (In_0, In_1, In_2, In_3, In_4, and In_5). Thus the filling ratio of this sub-module is 92%.

To meet the security constraints presented in section 2:

- The sub-blocs of this function are implemented using a 1 out of N encoding. This strategy guarantees a constant Hamming weight which is required to make power consumption data-independent.
- The circuit architecture is fully symmetric. This means that all the data paths have the same logical depth.

To validate the e-FPGA native robustness against SPA and DPA attacks, an electrical simulation campaign have been carried out. The analyzed bloc (cf. Figure 5) has been designed in a CMOS 65nm technology. Remind that, to be robust against SPA and DPA, the bloc (cf. Figure 5) should have the same current profiles and a constant running time whatever the manipulated data.
During the electrical simulation campaign and for a given secret key, random plaintext vectors have been processed. The corresponding current profiles are given in Figure 6 and the outputs are given in Figure 7.

A

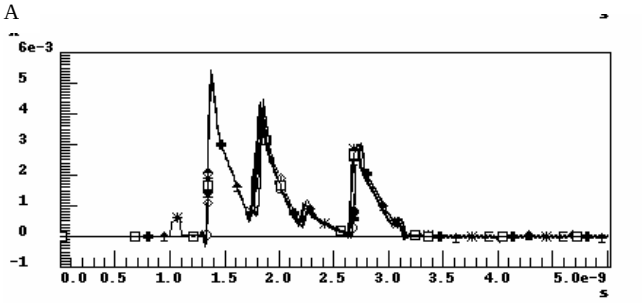

Figure 6: Current profiles of the bloc.

S

V

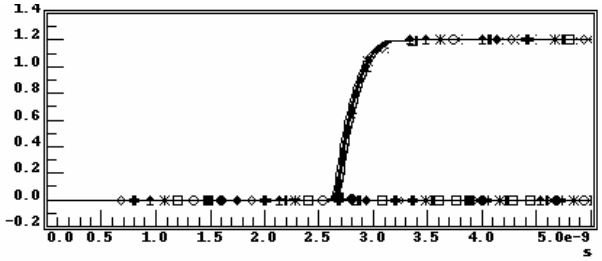

Figure 7 Outputs of the Figure 5 bloc.

S

Figure 6 shows that, whatever the manipulated data are, the current profiles are very similar. In other words, the power consumption is data independent. In addition, as shown in Figure 7, the outputs are completely superposed. This means that the e-FPGA running time is data independent. This drastically increases the circuit robustness against SCAs exploiting the running time variations. In conclusion, with data independent power consumption and a constant running time, the proposed asynchronous e-FPGA architecture is natively robust against SPA, DPA and timing attacks.

5. CONCLUSION

In this paper, we proposed a novel asynchronous embedded FPGA architecture which is mainly dedicated to security applications. This novel architecture has been designed to be natively robust against power-based attacks and enough flexible to allow exploring and experimenting countermeasures against SCAs and FAs. To achieve data independent power consumption, this novel architecture adopts the 1-of-n encoding and four phase protocol communication. In addition, the building blocs have been designed to be logically and electrically balanced. In summary, within the SAFE project, all the security problems have been addressed at the architectural, logical, electrical and routing levels.
Up to now, these first encouraging results indicate that a high security level is possible for secure applications implemented on a dedicated asynchronous e-FPGA. Such an embedded FPGA is a promising approach to

counteract attacks against cryptosystems such as SPA, DPA, timing and faults attacks.

6. REFERENCES

[1] L. Fesquet, M. Renaudin. “Programmable logic architecture for prototyping clockless circuits” IN FPL 2005, Tampere, Finland, August 24-26, 2005, pp 293-298.

[2] N. Huot, H. Dubreuil, L. Fesquet, M. Renaudin , “FPGA architecture for multi-style asynchronous logic”, In DATE 2005, Munich Germany, March 7-11, 2005, pp. 32-33.

[3] Kapilan Makeswaran and Venkatesh Akella: ”PGA-STC : Programmable Gate Array for Implementating Self-Timed Circuits”, International Journal of Electronics, Volume 84, Number 3/March 1, 1998.

[4] B. Gao: ”A globally asynchronous locally synchronous configurable array architecture for algorithlm embeddings”, PhD thesis, University of Edinburg, December 1996.

[5] John Teifel and Rajit Manohar: ”Highly Pipelined Asynchronous FPGas”, In 2th ACM International Symposium on Field-Programmable Gate Arrays, Monterey, CA, February 2004.

[6] Paul C. Kocher, Joshua Ja_e, and Benjamin Jun: “Diferential power analysis, Advances in Cryptology ”, CRYPTO '99 (M. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999, pp. 388-397.

[7] S. Moore, R. Anderson, P. Cunningham, R. Mullins and G. Taylor: “Improving Smart Card Security using Self-timed Circuits”, in Proc. 8th IEEE International Symposium on Asynchronous Circuits and Systems – ASYNC ’02, pp. 23–58, IEEE 2002.

[8] Yannick Monnet, Marc Renaudin, Régis Leveugle, "Designing Resistant Circuits against Malicious Faults Injection Using Asynchronous Logic," IEEE Transactions on Computers, vol. 55, no. 9, Sept., 2006, pp. 1104-1115.

[9] F. Bouesse, G. Sicard, M. Renaudin, “Path Swapping Method to Improve DPA Resistance of QDI Asynchronous Circuits” 8th International Workshop on Cryptographic Hardware and Embedded Systems–CHES2006, , Yokohama, Japan, October 2006, LNCS 4249 Springer 2006,pp. 384-398.

[10] Quoc Thai Ho, Jean-Baptiste Rigaud, Laurent Fesquet, Marc Renaudin, Robin Rolland: 'Implementing Asynchronous Circuits on LUT Based FPGAs', FPL 2002, pp 36-46.

[11] Thomas Wollinger and Christof Paar, "How Secure Are FPGAs in Cryptographic Applications?", In 13th International Conference on Field Programmable Logic and Applications - FPL 2003, Lisbon, Portugal, September 1-3, 2003

[12] http://www.achronix.com/