# Trivium hardware implementations for power reduction

J. M. Mora Gutiérrez[1,*], C.J. Jiménez Fernández[2], M. Valencia Barrero[2]

[1] *Instituto de Microelectrónica de Sevilla (IMSE-CNM-CSIC), Seville, 41092 Spain*
[2]*University of Seville and Instituto de Microelectrónica de Sevilla (IMSE-CNM-CSIC), Seville, 41092 Spain*

**SUMMARY**

This paper describes the use of parallelization techniques to reduce dynamic power consumption in the hardware implementations of the Trivium stream cipher. Trivium is a synchronous stream cipher based on a combination of three non-lineal feedback shift registers selected in 2008 as finalist for the hardware profile of the eSTREAM project. To compare and verify the power consumption study, the designs have been implemented and characterized in a 350 nm standard-cell technology with both transistors and gates level models, in order to permit both analog and digital simulations. The results show that the two low power Triviums designed decreasing average power consumption by between 15% and 25% with virtually no performance loss and only a slight overhead (about 5%) in area.

*KEY WORDS*: Trivium, stream cipher, low power, light cryptography, hardware implementation.

## 1. INTRODUCTION

In the coming years most of the communications of low complexity devices with applications in portable health-care devices or the Internet of things (IoT) will use cryptographic techniques to achieve inviolability and confidentially in data management. Hardware implementation in ASIC devices will require, not just cryptographic algorithms but also algorithms for Lightweight Cryptography [2]. In hardware implementations, chip size and power consumption are the important measures to evaluate the lightweight properties.

Among ciphers that fall into this type of cryptography are both block ciphers [3] and stream ciphers. The latter are of interest in this article. Stream ciphers are generally much faster than

[*] Correpondence to: José M. Mora Gutiérrez, Instituto de Microelectrónica de Sevilla-CNM (CSIC_Universidad de Sevilla), Sevilla, 41092 Spain.
*E-mail:* jmiguel@imse-cnm.csic.es

block cyphers and they use less hardware resources, making them an ideal alternative when high throughput, low gate counts or low power consumption are important requirements.

The initiative known as eSTREAM [1], [2] identified and published three new algorithms specially designed to give good performance in hardware (Grain, Mickey and Trivium). These stream ciphers are already being used in battery powered devices, passively powered devices and wireless communications [3], [4], where the power consumption is a critical factor, so the election of an algorithm that minimizes power consumption is a priority.

The objective of the work is to propose low power ASIC implementations of Trivium based on standard-cell libraries in CMOS process technology.

Analysis of the Trivium algorithm suggests that parallelization is the most appropriate technique to achieve a reduction in power consumption [5]. The parallelization technique was introduced by Schneider, Von Kaenen, and Piquet in 1995 [6].

In the literature, few contributions about analyzing and reducing Trivium power consumption have been published. In FPGA implementations some power summaries of results for eSTREAM candidates including Trivium have been reported [7-8] but there has not been applied any technique to reduce its power consumption. In ASIC implementation, power results for a Trivium in a 130 nm CMOS technology is shown in [9] where it is obtained 175 μW of average power at 10 MHz. In [10] power consumption in a Trivium radix-16 optimized for passively-powered devices is reduced applying clock gating and sleep mode logic as a method for reducing the effective clock frequency. The generation of 16 bit key stream requires 22 clock cycles. Source current values below 1 μA at 100 KHz and 1.5 V are obtained for a 350 nm technology.

This paper focuses on Trivium hardware implementations for low power applications. Two different parallelization alternatives have been applied to Trivium and presented in this paper. Firstly, the mixed parallel low power Trivium implementation (MPLP) alternative, where parallelization is applied to flip-flops unaffected by non-linear feedback paths. Secondly, the full parallel low power implementation (FPLP) version, where the parallelization technique is applied to all the flip-flops in the Trivium stream cipher even though this implies redesigning non-linear feedback paths.

The applied technique reduces the switching activity factor from internal flip-flops while maintaining the same external frequency so the power reduction will be related with the switching activities in the Trivium flip-flops.

This method was applied in a previous work [11] obtaining good results for a Trivium although only results from digital simulations were presented. In this work we have compared digital results with analog simulations in a standard-cell CMOS technology that include transistor models to evaluate and compare the accuracy of the power measurements. Moreover, this work presents another alternative low power implementation (MPLP) with less complexity and good results.

To compare the benefits of each of the proposed solutions, quantitative measurements of power consumption were made in the different designs. For this purpose, a detailed power consumption study was carried out at logic and electrical level in a 350 nm technology with both transistors and Verilog models, in order to permit both analog and digital simulations.

The results show that the application of this technique makes possible to reduce dynamic power and average current by between 30-58%, with no performance loss and only a slight penalty in area (less than 5%).

This paper is organized as follows. Section 2 briefly describes the Trivium algorithm and its hardware implementation. In section 3 architecture for a mixed parallel low power Trivium implementation (MPLP) with non-full parallel shift register is presented, along with power reduction results. Section 4 describes a second architecture for a full parallel low power Trivium implementation (FPLP), with better power reduction than the first design. Sections 5 show the main differences between MPLP and FPLP implementations. Finally, some conclusions are presented in Section 6.

## 2. TRIVIUM HARDWARE IMPLEMENTATION

Hardware implementation of Trivium [12] stream cipher is based on a 288-bit cyclic shift state register and combinational logic to provide its nonlinear feedback. It generates up to $2^{64}$ bits of pseudorandom key stream with an 80-bit secret key (KEY) and an 80-bit initialization vector (IV).

As it is shown in Figure 1, the implementation of the Trivium algorithm that generates one key stream bit in each clock cycle comprises three shift registers of different lengths and combinational logic to perform the exclusive-or sum and the AND operations.

The lengths of the shift registers are not the same; the first register has 93 bits, the second 83 bits and the third 111 bits.

The state register is loaded with a secret key (KEY) and an initialization vector (IV) of fixed length (80 bits) and some ones and zeros to initialize the state of the Trivium.

Once it is loaded, the state register must be shifted 1152 times (4x288) before a valid key stream can be obtained. The output *key stream* is an exclusive-or operation of signals from the three shift register.

With this architecture and operation mode most of the power is consumed by the flip-flops of the three shift registers. In order to reduce power consumption, we therefore focus on the shift register structure. Dynamic power depends on switching activity factor (which represents the average fraction of clock cycles in which a signal transition occurs), clock frequency, supply voltage and output capacitance. The more logic transitions occur in the cell output, the more switching power increases.

In our proposal, dynamic power in Trivium shift registers is reduced by decreasing the switching activity. This is done by applying the shift register parallelization technique, while maintaining the same frequency and supply voltage.

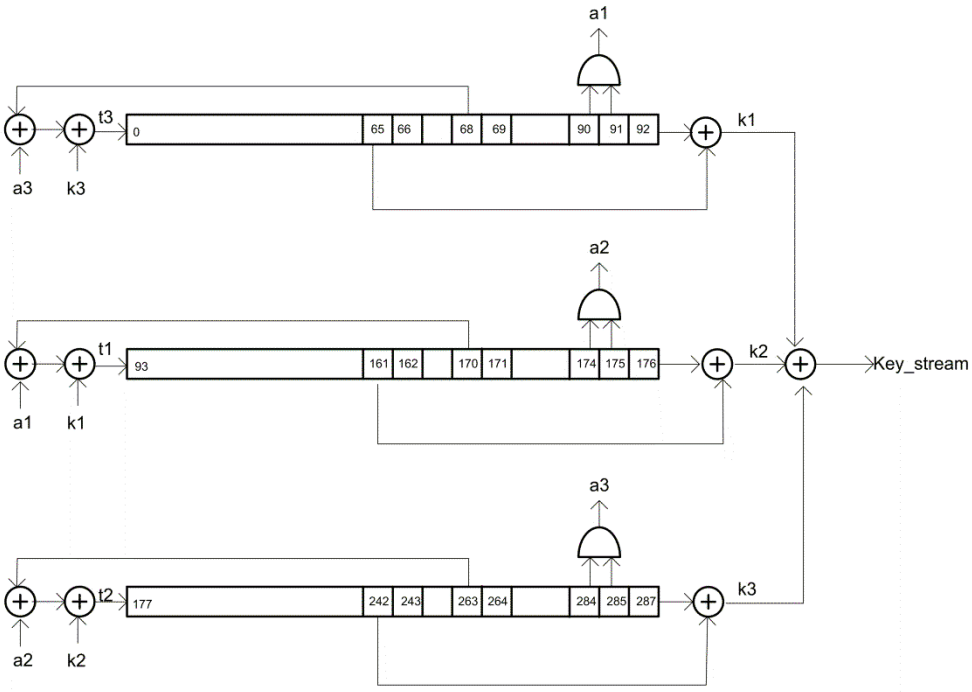


Figure 1. *Schematic representation of the Trivium cipher.*

To accurately estimate power consumption in Trivium stream cipher, analog and digital simulations were made in the different layout designs. Post-layout netlist contains the clock buffer in the clock trees and the core cell´s so the power consumption is the summation of the logic gates and the clock buffers. The I/O cells are not included.

An analog simulation based analysis is able to calculate power more accurately and in detail than digital simulation although has the huge disadvantage that it is extremely time-consuming.

A 350 nm CMOS process technology was chosen because it has models capable of performing digital and analog simulations using logic and transistor level models.

## 3. MIXED PARALLEL LOW POWER TRIVIUM (MPLP)

Parallelization technique in Trivium cannot be applied directly to all flip-flops of Trivium state register because the outputs of some of them are involved in logical operations. In this version, the technique has only been applied to the less significant bits of each shift registers that are not used in the feedback. From 0 to 63 bit in the first shift register, from 93 to 160 bit in the second shift register and from 177 to 240 bit in the third shift register (196 out 288 bits of the state register).

Its application requires a slight hardware modification in each shift register of the representation of Figure 1. As is shown in Figure 2, with the parallelization technique the bits of the shift registers not involved in feedback or combinational operations are divided into two shift registers denominated odd and even shift registers. The required modification

introduces a flip-flop to generate a clock divide by two and add a multiplexer to select the least significant bit of each shift register.

The MPLP implementation is shown in the Figure 3. The state register is loaded in parallel with a secret key and an initialization vector, taking into account that the even registers are loaded with the rising edge and the odd registers are loaded with the falling edge of an internal clock with half the frequency of the input clock.

The MPLP and the standard Trivium implementations were described in VHDL, synthesized with *Design Vision* (*Synopsys*), and verified using *ModelSim* simulation environment, with the same test vectors and using the same key and initialization vector as those presented in the Trivium reference files [2]. Simulation with different set of keys and initialization vectors have been done too. The layout implementation was done by *Encounter Digital Implementation System RTL-to-GDSII* (*Cadence*).

As previously mentioned, dynamic power depends on switching activity factor which represents the average fraction of clock cycles in which signal transition occurs. To estimate the effect of the introduction of the parallelization technique in the Trivium implementation, RTL simulations has been performed to compare the number of transitions occurred in the shift register flip-flops in each clock cycle. The results of the average (*avg*) and maximum (*max*) number of flip-flops that change by clock cycle (0 to 1 and 1 to 0 levels) are shown in Table 1.

The average of flip-flops changing its output in each clock cycle is 138 for the standard and 94 for the MPLP implementation. The parallelization technique therefore reduces the number of flip-flop transitions in each clock cycle approximately by 30%. This reduction is also seen on the average of transitions from 0 to 1 and 1 to 0 levels. With these results and due to the most of the power consumption occurs in the state register's flip-flops, a power reduction about 30% can be expected. This data has to be checked by digital and analog simulations.

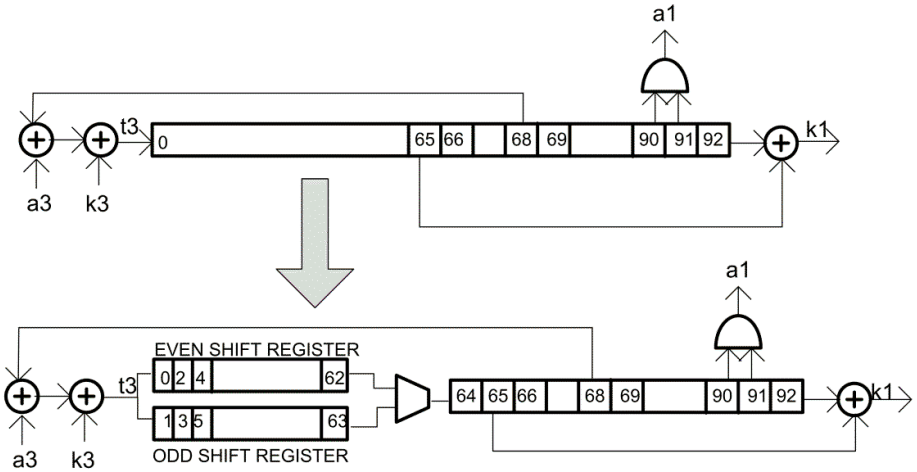


Figure 2. Shift registers parallelization schematic

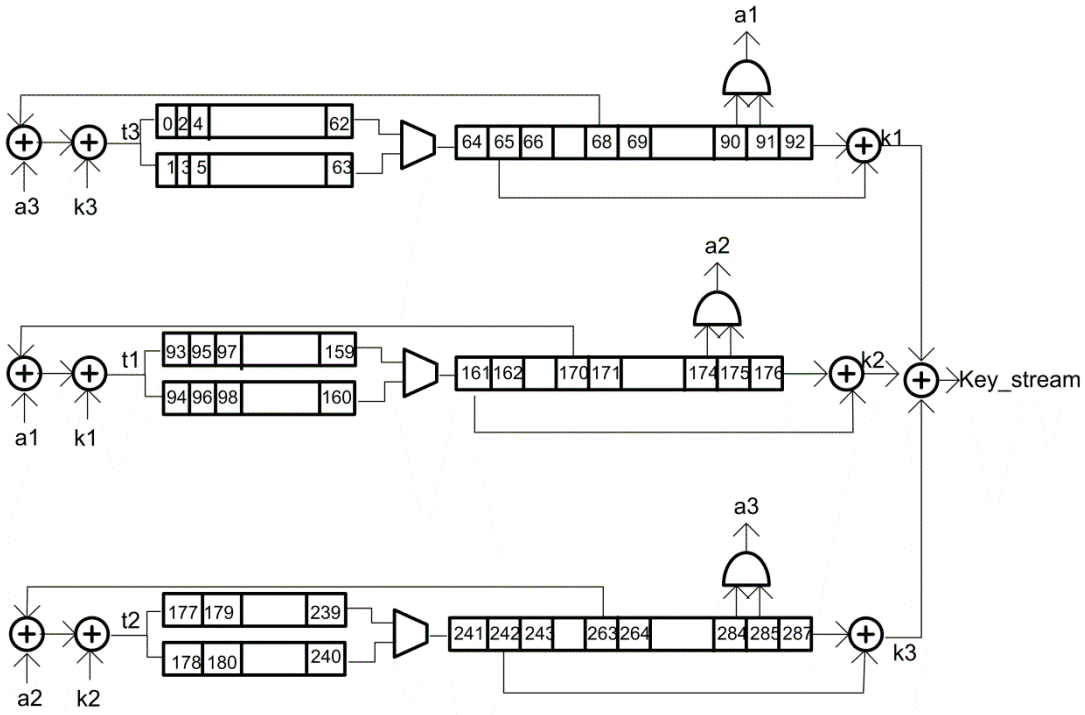


Figure 3. *Mixed-Parallel Low Power Trivium (MPLP).*

The combinational area of the MPLP version of the Trivium implemented in a 350 nm technology is quite similar to the area of the standard version, because the numbers of flip-flops do not change (only one flip-flop for the clock division is added) and the combinational area only add three multiplexers. None difference is expected between the two implementations. The area report provided by the Design Analyzer synthesis tool for the MPLP and standard Trivium is shown in Table 2.

In conclusion, the MPLP version has no area penalty in comparison with the standard version.

### *3.1. MPLP Trivium Power Consumption*

To know more accurately the power consumption and why reduction occurs, measurements of current drawn from the power supply in post-layout analog simulations have been realized.

Analog simulations are carried out with a clock frequency of 25 MHz, but due to the complexity of the circuit and the computing time, it was not possible to simulate a large number of clock cycles. Figure 4 shows a detail of the waveforms of the current supply for both implementations simulating for 1 μs. It can be noted that the power supply current peaks in the standard version of Trivium are very similar on both clock edges, while the MPLP Trivium presents a reduction in the current peaks on the rising and falling edges of the clock. It should be noted the current peaks in the falling edges has been strongly reduced.

Measurements from the analog simulations show that the peak current on the rising clock edge for the MPLP Trivium is reduced by about 20%, and strongly reduced on the falling edge about 69%. Furthermore, the average current consumption measured by analog simulation decreases about 25%, for MPLP Trivium compared to the standard version as it is shown in Table 3.

These results show a reduction in the power consumption a slightly less than expected by the reduction of the number of transitions in the flip-flops shown in Table 1. This is because clock tree power consumption is not considered in Table 1.

Dynamic power consumption have been measured from digital simulations and compared with analog simulations to validate data obtained. Digital simulations are carried out for more clock cycle because they are less time-consuming, although their results are less accurate than analog simulation.

The input patterns were the same in both simulations and it is used the initialization vector IV and the key presented in the Trivium reference files [2].

Power consumption is analyzed using Encounter RTL to GDSII tools with a switching activity file in VCD (value change dump) format. This file is generated with 1700 clock cycles (68 μs simulation) with a clock frequency of 25 MHz. As we mentioned before, Trivium needs 1152 clock cycles before a valid key stream is obtained. Capacitances and power models for wires and gates are taken from the technology library.

When the power consumption of the MPLP and standard Trivium implementations was compared, as shown in Table 4, it was noticed that the MPLP version has about 25% lower dynamic power consumption than the standard version. Again, the main reason for this reduction is the reduction in the number of flip-flops changing each clock cycle as it was shown previously in Table 1. This result is very similar to the measured by the analog simulation.

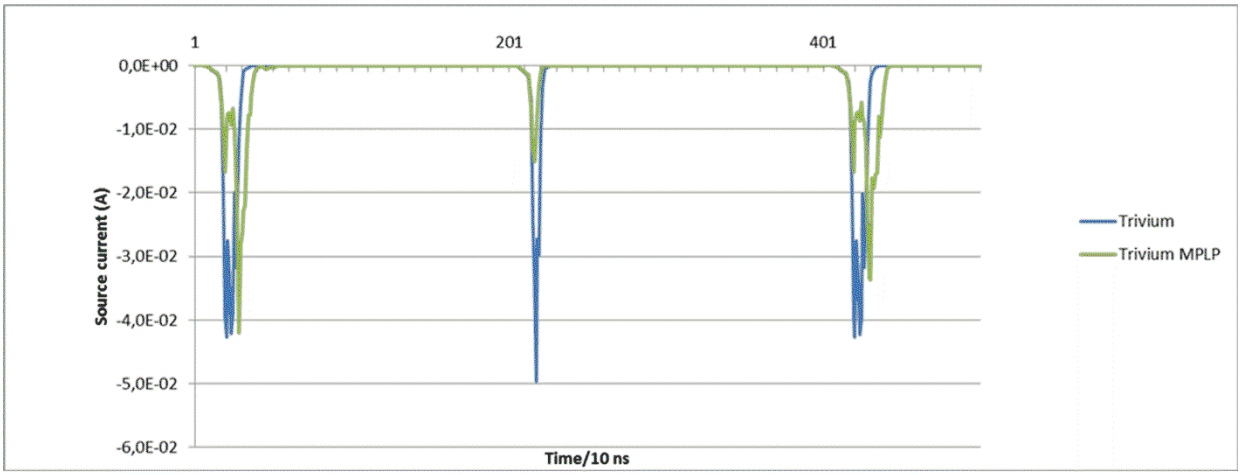


Figure 4. *Power supply current post-layout analog simulation.*

Parallelizing 196 of the 288 bits in the state register have achieved a power reduction in MPLP Trivium of about 25%. If the parallelization technique could be applied to all 288 bits in the state register, an even greater reduction in consumption could be obtained. Nevertheless, to do this it is necessary to introduce some hardware modifications. Therefore, a new low power version is presented in the following section.

## 4. FULL PARALLEL LOW POWER TRIVIUM (FPLP)

In FPLP implementation, the parallelization technique has been applied to all the flip- flops of the shift registers. However, to do this, it has required additional modifications in the structure of the Trivium.

Shift register parallelization of all the bits in the state register transforms each one of the Trivium's shift registers into two half of length shift registers (odd and even). Figure 5 shows a schematic representation of the FPLP Trivium. The length of each shift register is indicated in the figure inside the odd and even registers.

The generation of the input bits of each shift register and the generation of the key stream depend on the bits stored in different positions in the shift registers. But the problem posed by this new structure is that the location of these bits depends on whether the clock cycle is even or odd. In one case, the bit to be retrieved it is in the even register and in the other it is in the odd register. To select the bits correctly, some glue logic must be introduced. As shown in Figure 5, this added logic basically means multiplexers which, using the clock as the selection signal, will select the bit to be retrieved from odd of even shift register.

The FPLP Trivium version is described and designed using VHDL. The resulting implementation is verified using the *ModelSim* simulation environment with a post-layout netlist. The implementation of the FPLP Trivium increases the number of the cells and nets because more multiplexers and combinational cells have to be added to implement the algorithm. Table 5 shows the cell and nets count by Synopsys for a 350 nm technology. The FPLP version uses more cells (6.6%) and more nets (16%) than the standard Trivium and MLP implementation.

As in the MPLP version, analysis of the number of transitions occurred in the shift register flip-flops has been made. In each clock cycle, the results of the average (avg) and maximum (max) number of flip-flops that change (0 to 1 and 1 to 0 levels) were compared with those obtained for the standard version of the Trivium, and are shown in Table 6.

As it can be seen in this table, the average of flip-flops changing its output each clock cycle is 138 for the standard Trivium and 70 for the FPLP Trivium. This represents a 49% reduction in the number of transitions. This reduction also occurs in the averages of the transitions from 0 to 1 level and from 1 to 0 levels.

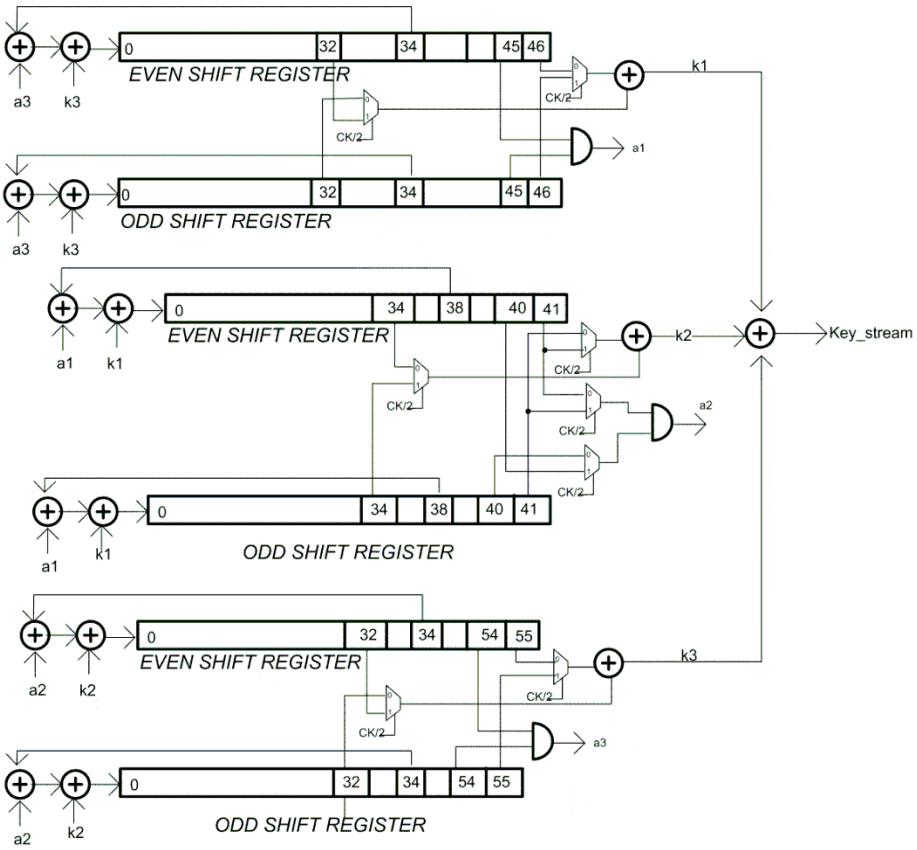


Figure 5. *Schematic of Full-Parallel Low Power Trivium (FPLP).*

Regarding area, the combinational area and the nets' area must be larger in the FPLP Trivium because more multiplexers and combinational cells have to be added to implement the algorithm. Table 7 shows the area estimation reports provided by the Design Analyzer synthesis tool for the FPLP and standard versions. The combinational area of the FPLP version increases by 19.1% over the standard version.

The non-combinational area is quite similar in both designs because the numbers of flip-flops do not change (only one flip-flop is introduced, for the clock division). Thus, the FPLP version has a cell area penalty of about 4% while the net area is increased by 8%.

### *4.1. FPLP Trivium Power Consumption*

As in the MPLP version, we have analyzed accurately how the power consumption is and where reduction occurs. Measures of power consumption have been taken from analog and digital simulations in Trivium layout circuits. Analog simulations were carried out with a clock frequency of 25 MHz simulating for 1 μs, doing the same steps as for MPLP Trivium simulations.

Figure 6 shows a detail of the waveforms of the current flown through the power supply for both implementations. It can be seen that the power supply current peaks in the standard version of Trivium are very similar on both clock edges, while the FPLP Trivium presents an increase in the current peaks on the rising edges of the clock and their total disappearance on the falling edge.

Measures from the analog simulations shown the peak current on the rising clock edge has been increased by about 35%, for FPLP Trivium implementation but it has been strongly reduced on the falling clock edge by about 93%. Furthermore, the average current consumption during the analog simulation has been decreased a 15% for FPLP Trivium as is shown in Table 8. The average power measurement from the analog simulation indicates a power reduction in the FPLP Trivium, about 15% as it is shown in Table 8.

Again, measures of consumption have been done from digital simulations as it was done in Section 3.1. When the power consumptions of the two implementations shown in Table 9 (standard Trivium and FPLP Trivium) are compared, it is noticed that the FPLP Trivium has cell dynamic power consumption 23% lower than the standard version. Switching power is very similar in both Trivium.

This result is slightly different to the measured by the analog simulation and the reduction is lower than obtained by the estimation of the number of flip-flops transitions by clock cycles, because clock tree power consumption.

## 5. COMPARISON BETWEEN MPLP AND FPLP TRIVIUM

The power reduction achieved by the MPLP version compared with the standard version is about 25% and the reduction achieved by the FPLP version is about 23-15%. Although the results with analog and digital simulations are slightly different in Trivium FPLP, in both cases it is conclude that MPLP and FPLP Trivium can reduce the dynamic power.

Table 10 summarizes the power consumption of other Trivium implementations reported in the literature along with our proposals.

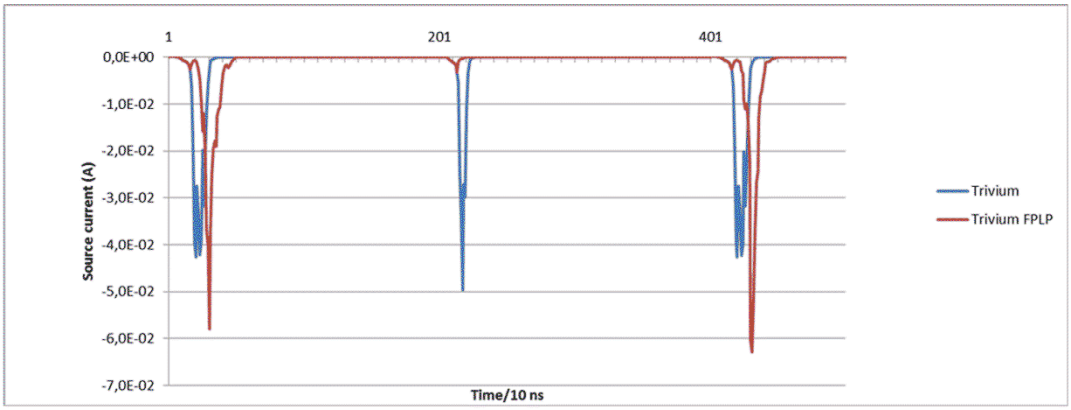


Figure 6. *Power supply current post-layout analog simulation.*

The comparison between the power consumption of the different Trivium implementations is difficult because the technologies used are different even though the transistor size is the same. For instance if frequency and voltage in 130 nm technology are scaled, FPLP Trivium implementation [11] has lower cell dynamic power consumption than the implementation [9]. For 350 nm technology, comparison is more difficult, not only because the technologies are different, but also because the low power Trivium implemented in [10] is radix-16 and uses a reducing effective clock frequency so scaling is more undetermined.

## 6. CONCLUSIONS

In this paper, two versions of low power Trivium implementations using logic parallelization techniques (MPLP and FPLP) have been presented. Power consumptions have been estimated with analog and digital simulations for both versions. Analog simulations have been possible because the 350 nm technology has transistor level models of their standard-cells. Some latest technologies are not able to provide standard-cells libraries with transistor level models.

The MPLP Trivium architecture offers greater power reduction than the FPLP Trivium, but also produces a slight increase in the complexity of the algorithm and the logic used, increasing the final area. The technique employed produced Trivium implementations with reductions in power consumption of between 25% and 15% and virtually no performance loss. With this technique, the current peaks are strongly reduced on the falling edge (more than 50%) and reduced about 25-15% on the rising edge.

The area penalty and cell number obtained with this technique is very low (less than 6%) while the reduction in dynamic power consumption is noticeable.

## ACKNOWLEDGEMENTS

This work has been partially funded by Spanish government projects: CITIES (TEC2010-16870) and CESAR (TEC2013-45523-R).

## REFERENCES

1. eSTREAM: ECRYPT Stream Cipher Project. *http://www.ecrypt.eu.org/stream/D.SYM.3-v1.1.pdf.*
2. Matthew Robshaw Olivier Billet (Eds.). *New Stream Cipher Designs. The eSTREAM Finalists*. Springer 2008.
3. Kocheta, M. ; Sujatha, N. ; Sivakanya, K. ; Srikanth, R. ; Shetty, Sridhar ; Ananda Mohan, P.V. A review of some recent stream ciphers. *International conference on Circuits, Controls and Communications (CCUBE),* 2013*;* 1- 6.
4. Jiezhong Gong ; Gongliang Chen ; Linsen Li ; Jianhua Li. A secure authentication protocol for RFID based on Trivium, *International Conference on Computer Science and Service System (CSSS),2011;* 107- 109.
5. C. Piquet. *Low-Power CMOS Circuits technology, Logic Design and CAD Tools*. CRC Press, 2006.
6. T. Schneider et al., Low-Voltage Low-Power Parallelized Logic Modules. *Proc. PATMOS95*. Paper S4.2, Oldenburg. October 4-6, (1995).

7. M. Rogawski. Hardware evaluation of eSTREAM Candidates: Grain, Lex, Mickey128, Salsa20 and Trivium. *State of the Art of Stream Ciphers Workshop*. SASC 2007, Bochum, Germany, Feb. 2007.
8. Marmolejo-Tejada, J.M; Trujillo-Olaya, V. ; Velasco-Medina, J. Hardware implementation of Grain-128, Mickey-128, Decim-128 and Trivium. ANDESCON, 2010 IEEE, pp 1- 6.
9. Good, T., Benaissa, M., Hardware results for selected stream cipher candidates. *State of the Art of Stream Ciphers Workshop* (SASC 2007), eSTREAM. ECRYPT Stream Cipher Project, Report 2007/023 (2007).
10. Feldhofer, M. Comparison of low-power implementations of Trivium and Grain. *State of the Art of Stream Ciphers Workshop* (SASC 2007), eSTREAM. ECRYPT Stream Cipher Project, Report 2007/027 (2007).
11. J. M. Mora-Gutiérrez, C. J. Jiménez-Fernández, M. Valencia-Barrero. Low Power Implementation of Trivium Stream Cipher. PATMOS (2012) 113-120.
12. C. De Canniere and B. Preneel. Trivium, A Stream Cipher Construction Inspired by Block Cipher Design Principles. *State of the Art of Stream Ciphers Workshop* (SASC 2006), eSTREAM, ECRYPT Stream Cipher Project, Report 2006/021. (2006).

Table 1. Flip-flops transitions by clock cycle in standard-MPLP Trivium.

| ***Flip-flops transitions*** | ***Transitions*** | | ***Transitions 0 to 1*** | | ***Transitions 1 to 0*** | |
|---|---|---|---|---|---|---|
| | ***avg*** | ***max*** | ***avg*** | ***max*** | ***avg*** | ***max*** |
| *Trivium* | 138 | 158 | 69 | 80 | 69 | 78 |
| *MPLP Trivium* | 94 | 117 | 47 | 58 | 47 | 59 |

Table 2. Trivium and MPLP Trivium Synopsys Report

| | ***350 nm*** | | |
|---|---|---|---|
| ***Synopsys Report*** | ***Trivium*** | ***MPLP Trivium*** | ***Reduction*** |
| *Cell Area($\mu m^2$)* | 126580 | 129165 | 2% |

Table 3. Average Power Consumption with analog Simulation

| ***Analog Simulation*** | ***Trivium*** | ***MPLP Trivium.*** | ***Reduction*** |
|---|---|---|---|
| *Average power(mW)* | 4.02 | 2.98 | 25% |
| *Average current(mA)* | 1.22 | 0.9 | 25% |

Table 4. Trivium and MPLP Trivium Encounter Power Report

| ***Power@25MHz@3.3V*** | ***350 nm*** | | |
|---|---|---|---|
| | ***Trivium*** | ***MPLP Trivium*** | ***Reduction*** |
| *Dynamic (mW)* | 5.84 | 4.36 | 25% |
| *Switching (mW)* | 1.12 | 1.11 | |
| *Cell internal(mW)* | 4.72 | 3.24 | 31% |

Table 5. Trivium and Trivium FPLP Synopsys area Report

| ***Synopsys Report*** | ***350 nm*** | | |
|---|---|---|---|
| ***Number of*** | ***TRIVIUM*** | ***FPLP Trivium*** | ***Overhead*** |
| *Cell* | 617 | 748 | 6.6% |
| *Nets* | 792 | 921 | 16% |

Table 6. Flip-flops transitions by clock cycle

| ***Flip-flops transitions*** | ***Transitions*** | | ***Transitions 0 to 1*** | | ***Transitions1 to 0*** | |
|---|---|---|---|---|---|---|
| | avg | max | avg | max | avg | max |
| *Trivium* | 138 | 158 | 69 | 80 | 69 | 78 |
| *FPLP Trivium* | 70 | 86 | 35 | 43 | 35 | 43 |

Table 7. Trivium and Trivium FPLP Synopsys area Report

| ***Synopsys Report Area($\mu m^2$)*** | ***350 nm*** | | |
|---|---|---|---|
| | ***TRIVIUM*** | ***FPLP Trivium.*** | ***Overhead*** |
| *Combinational* | 26990 | 32159 | 19.1% |
| *Non-comb.* | 99590 | 100573 | 1% |
| *Cell* | 126580 | 132732 | 4% |
| *Net* | 17559 | 19017 | 8% |

Table 8. Average Power Consumption Analog Simulation

| ***Analog Simulation*** | ***Trivium*** | ***FPLP Trivium.*** | ***Reduction*** |
|---|---|---|---|
| *Average power(mW)* | 4.09 | 3.39 | 15% |
| *Average current(mA)* | 1.22 | 1.03 | 15% |

Table 9. Trivium and Trivium FPLP Encounter Power Report

| ***Power@25MHz@3.3V*** | ***350 nm*** | | |
|---|---|---|---|
| | ***Trivium*** | ***FPLP Trivium*** | ***Reduction*** |
| *Dynamic (mW)* | 5.84 | 4.46 | 23% |
| *Switching (mW)* | 1.12 | 1.13 | |
| *Cell internal(mW)* | 4.72 | 3.33 | 29% |

Table 10. Comparative Results

| ***Trivium*** | ***Dynamic Power*** | ***Supply voltage*** | ***Clock rate*** | ***Technology.*** |
|---|---|---|---|---|
| *Trivium [9]* | 175.1 μW | 1.2v | 10 MHz | 130 nm |
| *Trivium radix-16 [10]* | 0.68 μA | 1.5V | 100 KHz | 350 nm |
| *FPLP [11]* | 178 μW | 3.3V | 25 MHz | 130 nm |
| *Trivium [This work]* | 5.8 mW | 3.3V | 25 MHz | 350 nm |
| *MPLP [This work]* | 4.3 mW | 3.3V | 25 MHz | 350 nm |
| *FPLP [This work]* | 4.4 mW | 3.3V | 25 MHz | 350 nm |