International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.267-274
http://dx.doi.org/10.14257/ijsia.2015.9.7.23

SSTL Based Power Efficient Implementation of DES Security Algorithm on 28nm FPGA

Bishwajeet Pandey, Vandana Thind, Simran Kaur Sandhu, Tamanna Walia and Sumit Sharma

Chitkara University Punjab
gyancity@gyancity.com, vandanathind@gmail.com,
simransandhu115@ymail.com, waliatamanna@gmail.com,
sumitkaushal07@gmail.com

Abstract

In this particular work, we have done power dissipation analysis of DES algorithm, implemented on 28nm FPGA. We have used Xilinx ISE software development kit for all the observation done in this particular research work. Here, we have taken SSTL (Stub-Series Terminated Logic) as input-output standard. We have considered six sub-categories of SSTL (i.e. SSTL135, SSTL135_R, SSTL15, SSTL15_R, SSTL18_I and SSTL18_II) for four different WLAN frequencies (i.e. 2.4GHz, 3.6GHz, 4.9GHz, and 5.9GHz). We have done analysis considering five basic powers i.e. clock power, logic power, signal power, IOs power, leakage power and total power. There is 50-60% reduction in power dissipation, which is possible with proper selection of the most energy efficient IO standards i.e. SSTL135_R among SSTL logic families.

Keywords: *DES, 28nm FPGA, SSTL, WLAN frequencies, power dissipation, IOs power, Supply power, LUT, Global Clock Buffer*

1. Introduction

In this particular research work, we have done power analysis of DES algorithm, which is implemented on 28nm FPGA using SSTL as input-output standard. The input-output standard is provided to the physical layout of the circuit, to produce flexible and reliable interface to high frequencies bus. There are many types of input-output standards, designed for different types of FPGA as shown in Figure 1 below.

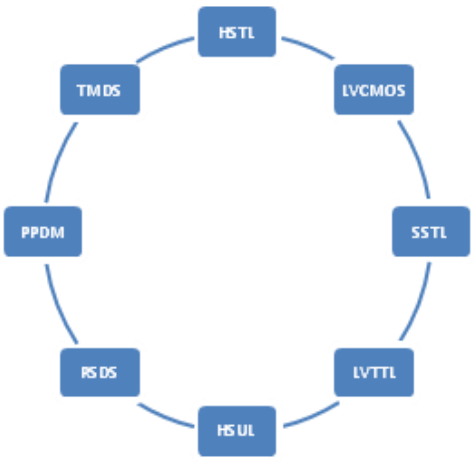

Figure 1. Different Types of Input-Output Standards

ISSN: 1738-9976 IJSIA

In this research work, we have taken SSTL (Stubs-Series Terminated Logics) as input-output standards. SSTL for 1.8V (SSTL18), 1.5V (SSTL15), and 1.35V (SSTL135) are I/O Standards used for general purpose memory buses. SSTL I/O Standard uses termination technique for the given interface, using signal-integrity analysis, which means purity is analyzed for actual PCB topologies including the memory devices used, the board layout, and transmission line impedances. Xilinx is high performance software which, provided us the reading of power dissipated using SSTL I/O Standard. The IO Standard we used i.e. SSTL supports both single ended signaling and differential signaling. Here we are using single ended signaling technique. First SSTL standard used is SSTL135 which is basically used for DDR3L SDRAM memory interfaces and it full strength driver is available for both the HP and HR I/O Banks. SSTL135_R is designed for a weaker, reduced-strength driver. Then we have use SSTL15 which is basically used for full strength driver and SSTL15_R is used for weaker, reduced-strength driver. SSTL18 class-I and class-II are available in both the HP and HR I/O banks.

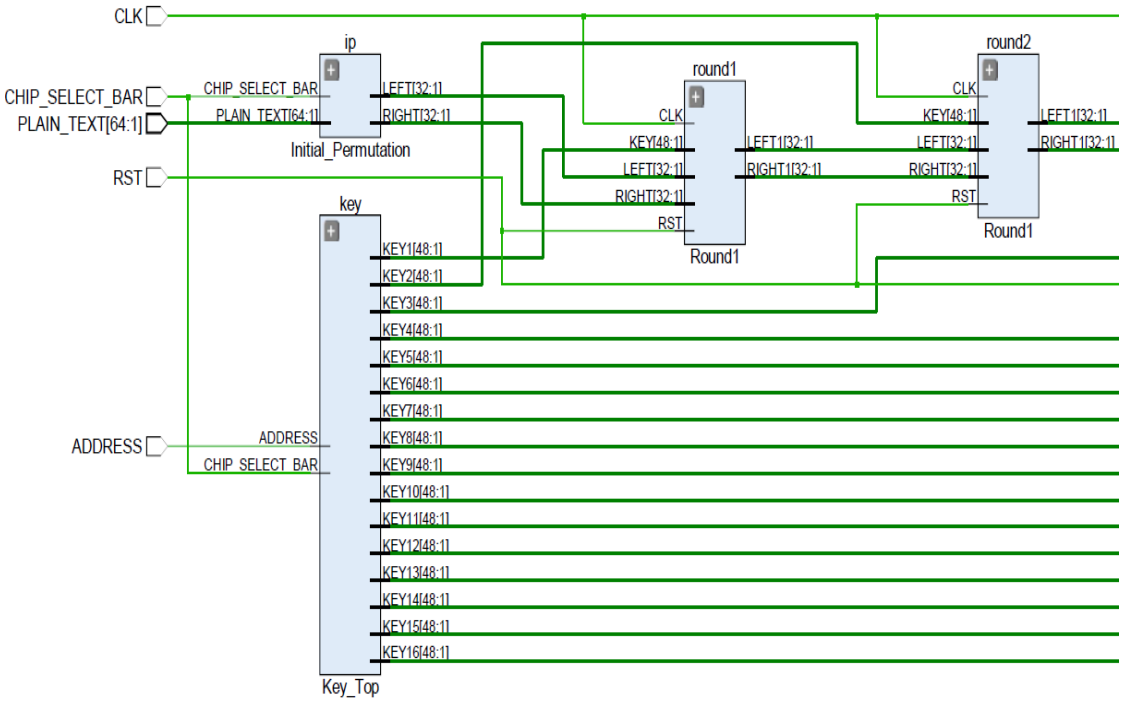

Figure 2. DES Algorithm

Figure 2, notify the RTL schematic of DES algorithm, which clearly shows the five inputs *i.e.* Clock pin, Chip-select-bar pin, Plain-text pin, Reset pin and Address pin. The structure of DES Algorithm basically consist of 16 identical stages of rounds and inverses named as initial and final permutation, these inverses were used for including data in order to facilitate loading blocks in and out with 8-bit based hardware. In between the algorithm XOR function is done to scramble the half a block together with some other keys.

In Table 1, We analyses the utilization report of DES algorithm from which we noticed that available registers are 126800 and 1024 (1%) is used by algorithm with 28nm FPGA. LUT is 3% used i.e. 1633, available is 63400. Global Clock Buffer is also used 3% of available (*i.e.* 1) and available is 32. IO available is 210, among which 63% of it used (*i.e.* 132).

Table 1. Number of Available Resources Used

Resources	Used	Available
Register	1024	126800
LUT	1633	63400
Global Clock Buffer	1	32
IO	132	210

We also studied primitive and black box usage of DES algorithm design, in which we noticed that there are 1633 BELS that consist of 975 LUT2, 146 LUT3 and 512 LUT6. This algorithm in total used 1024 Flip-Flops and latches, 1 Clock Buffers is used and total 131 IO buffers which basically consist of IBUF =67 and OBUF=64 as shown in Table 2 below.

Table 2. Number of Components Available and Used

Components	Total	Used
BELS	1633	--
LUT2	--	975
LUT3	--	146
LUT6	--	512
Clock Buffers	1	1
IO Buffers	131	131
IBUF	--	67
OBUF	--	64

2. Related Work

In some research work, researcher have used SSTL memory channel for some experiment of equalizer which minimize crosstalk and ISI [1], where as we have applied SSTL as input-output standard for DES algorithm which is basically algorithm for encryption. Other researcher have used SSTL for the analysis of sampling time window at particular data-rate for CMOS DFE (decision feedback equalization) receiver [2] where as we have used SSTL as input-output standard for DES algorithm and we have done power analysis. One scientist have used different IO standard of SSTL in 40 nm Virtex-6 and Spartan-6 FPGA [3], Where as we have used SSTL IO standard in 28nm Artix-7 FPGA for comparing different SSTL IO standard to get reduction in IO power. Another researcher have used LVCMOS as IO standard on 28nm technology based FPGA and they have analyzed the reduction in temperature [4] where we have done analysis on reduction of power as power is the most important factor of any design. Other researcher have done analysis, by using LVTTL as input-output Standards and they have done analysis on power reduction with respect to the capacitance [5], we have done analysis of power reduction by changing different frequencies. Some researcher have worked for the programmable input-output circuits, which have compatibility of its programming bits with TTL, GTL, GTLLP or LVDS type external circuits [6]. One researcher have studied that the multi-functional programmable I/O buffer available on field programmable gate array [7], we have studied about SSTL implemented on DES algorithm.

3. Power Analysis

In power analysis, we have calculated the percentage change in power dissipation, with change in input-output standards at different WLAN frequencies. We have paritcularly calculated the percentage change in power dissipiation of IOs power. we have taken into

consideration on-chip clock power, logic power, signals power, leakage power and total power consumed for analysis.

3.1. For Input-Output Standard :SSTL135

In Table 1, we see that the power dissipation in every component is increasing with increase in frequency, but leakage power is same for all the frequencies. Percentage change in IOs power, when frequency is changed from 2.4GHz to 3.6GHz is 25.25%, from 3.6GHz to 4.9GHz is 13.58% and 17.97% is change in power for change in frequency from 4.9GHz to 5.9GHz.

Table 3. Power Dissipation at Different Frequency with SSTL135 IOs Standard

On-chip	2.4GHz	3.6GHz	4.9GHz	5.9GHz
Clocks	0.076	0.127	0.178	0.211
Logic	0.063	0.068	0.074	0.077
Signals	0.140	0.199	0.248	0.288
IOs	2.087	1.560	2.037	2.403
Leakage	0.030	0.029	0.030	0.030
total	2.395	1.983	2.566	3.010

3.2. For Input- Output Standard :SSTL135_R

Table 2, infers that percentage change in IOs power, when frequency is changed from 2.4GHz to 3.6GHz is 25.7%, from 3.6GHz to 4.9GHz is 21.8% and 14.3 is for 4.9GHz to 5.9GHz frequency.

Table 4. Power Dissipation, when SSTL135_R is IOs Standard

On-chip	2.4GHz	3.6GHz	4.9GHz	5.9GHz
Clocks	0.076	0.127	0.178	0.211
Logic	0.063	0.068	0.074	0.077
Signals	0.140	0.199	0.248	0.288
IOs	0.611	0.823	1.053	1.230
Leakage	0.028	0.029	0.029	0.029
total	0.918	1.245	1.582	1.836

3.3. For Input- Output Standard :SSTL15

Table 3, notifies that percentage change in IOs power, when frequency is changed from 2.4GHz to 3.6GHz is 27.96%, from 3.6GHz to 4.9GHz is 23.27% and 17.88% is for 4.9GHz to 5.9GHz frequency.

Table 3. Power Dissipation, when SSTL15 is IOs Standard

On-chip	2.4GHz	3.6GHz	4.9GHz	5.9GHz
Clocks	0.076	0.127	0.178	0.211
Logic	0.063	0.068	0.074	0.077
Signals	0.140	0.199	0.248	0.288
IOs	1.159	1.609	2.097	2.472
Leakage	0.029	0.029	0.030	0.030

total	1.466	2.031	2.626	3.079

3.4. For Input- Output Standard :SSTL15_R

In Table 4, we see that the percentage change in IOs power, when frequency is changed from 2.4GHz to 3.6GHz is 25.7%, from 3.6GHz to 4.9GHz is 21.7% and 14.3% is for 4.9GHz to 5.9GHz frequency.

Table 4. Power Dissipation, when SSTL15_R is IOs Standard

On-chip	**2.4GHz**	**3.6GHz**	**4.9GHz**	**5.9GHz**
Clocks	0.082	0.128	0.173	0.208
Logic	0.063	0.069	0.073	0.077
Signals	0.148	0.195	0.245	0.283
IOs	0.627	0.844	1.079	1.260
Leakage	0.029	0.029	0.029	0.029
total	0.949	1.264	1.600	1.857

3.5. For Input-Output Standard :SSTL18_I

In Table 4, we see that the percentage change in IOs power, when frequency is changed from 2.4GHz to 3.6GHz is 29.4%, from 3.6GHz to 4.9GHz is 24.16% and 15.6% is for 4.9GHz to 5.9GHz frequency.

Table 5. Power Dissipation, when SSTL18_I is IOs Standard

On-chip	**2.4GHz**	**3.6GHz**	**4.9GHz**	**5.9GHz**
Clocks	0.076	0.127	0.178	0.211
Logic	0.063	0.068	0.074	0.077
Signals	0.140	0.199	0.248	0.288
IOs	1.885	2.671	3.522	4.177
Leakage	0.030	0.031	0.032	0.032
total	2.194	3.095	4.053	4.786

3.6. For Input- Output Standard :SSTL18_II

Table 2 infers that percentage change in IOs power, when frequency is changed from 2.4GHz to 3.6GHz is 29.33%, from 3.6GHz to 4.9GHz is 24.10% and 15.64% is for 4.9GHz to 5.9GHz frequency.

Table 6. Power Dissipation, when SSTL18_II is IOs Standard

On-chip	2.4GHz	**3.6GHz**	**4.9GHz**	**5.9GHz**
Clocks	0.082	0.128	0.173	0.208
Logic	0.063	0.069	0.073	0.077
Signals	0.148	0.195	0.245	0.283
IOs	2.269	3.211	4.231	5.016
Leakage	0.030	0.031	0.032	0.034
total	2.592	3.633	4.756	5.618

4. Comparison of Supply Power

Along with the comparison of IOs power, we have done the analysis on the supply power of different SSTL input-output standards at four different frequency (*i.e.* 2.4GHz, 3.6GHz, 4.9GHz and 5.9GHz). we have calculated the percentage change in supply power, when frequency is changed.

Table 7. Comparison of Supply Power at Different Frequency

IOs Standards	2.4GHz	3.6GHz	4.9GHz	5.9GHz
SSTL135	2.721	2.440	3.149	3.685
SSTL135_R	1.243	1.702	2.164	2.511
SSTL15	1.792	2.489	3.209	3.754
SSTL15_R	1.289	1.720	2.175	2.523
SSTL18_I	2.519	3.553	4.637	5.462
SSTL18_II	2.933	4.090	5.332	6.285

Figure 3, shows the comparison between the supply power dissiption of six different IOs Standards at different WLAN frequencies. This anlysis notify us that SSTL135_R have least and SSTL18_II have highest supply power dissipation at four different WLAN frequencies. We also observed the maximum percentage change at 2.4GHz is 57.6%, at 3.6 GHz is 58.3%, at 4.9GHz 59.4% and at 5.9GHz is 60.4%.

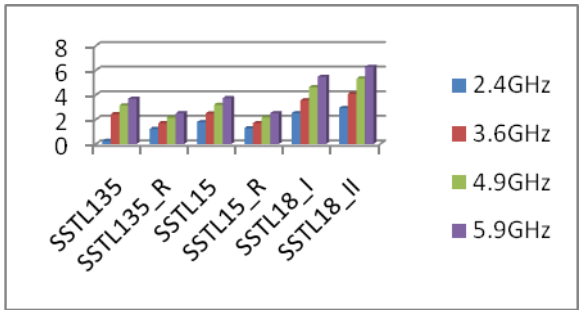

Figure 3. Comparison of Supply Power at Different Frequencies

4. Conclusion

We have concluded that with increase in frequency, power dissipation also increases. DES algorithm is compatible with different WLAN frequencies, as we have analyzed DES algorithm using four different WLAN frequencies (i.e. 2.4GHz, 3.6 GHz, 4.9 GHz and 5.9 GHz). As we have used 6 different IO Standards of category SSTL, from which we have concluded that SSTL135 and SSTL135_R are most efficient IO Standards for DES algorithm. We also observed that the leakage power dissipation is least for different on-chip components and IOs power is maximum. Therefore, energy efficient implementation of DES algorithm is possible with SSTL IOs Standards and different WLAN frequencies.

5. Future Scope

In this implementation of DES algorithm, we have used SSTL IOs Standards. In future, we can use different IO standards like LVCMOS, HSTL, SSTL, LVTTL, Mobile DDR, GTL, LVDS and so on. There is also open scope to implement other security algorithm like AES algorithm, MD5 and SH-2 on FPGA. In this work, target FPGA is 28nm

technology based Artix-7 FPGA. We can also use 16nm ultra scale FPGA and 3-D IC in our future work.

References

[1] J. H. Bae, "A crosstalk-and-ISI equalizing receiver in 2-drop single-ended SSTL memory channel", *Custom Integrated Circuits Conference (CICC), 2010 IEEE*. IEEE, (**2010**).
[2] Y.-S. Sohn, "A 1.2 Gbps CMOS DFE receiver with the extended sampling time window for application to the SSTL channel", *VLSI Circuits Digest of Technical Papers, 2002. Symposium on*. IEEE, (**2002**).
[3] T. Das, "SSTL based green image ALU design on different FPGA", Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on. IEEE, (**2013**).
[4] P. K. Maheshwari, and M. F. Irshad, "Thermal aware energy efficient comparator design using LVMOS IO standards on 28nm FPGA", *Open Source Systems and Technologies (ICOSST), 2014 International Conference on*. IEEE, (**2014**).
[5] K. Tanesh, "LVTTL IO STANDARDS AND CAPACITANCE SCALING BASED ENERGY EFFICIENT ALU DESIGN ON FPGA", *NED University Journal of Research* (**2014**), p. 39.
[6] M. S. Manohar, "Programmable input/output circuit for FPGA for use in TTL, GTL, GTLP, LVPECL and LVDS circuits", U.S. Patent No. 6,218,858, 17 April (**2001**).
[7] W. B. Andrews and H. N. Scholz, "Multi-functional I/O buffers in a field programmable gate array (FPGA)", U.S. Patent No. 6,480,026, (**2002**) 12 November.