Power Analysis of Energy Efficient DES Algorithm and Implementation on 28nm FPGA

Thind, Vandana ; Pandey, Bishwajeet; Hussain, Dil muhammed Akbar

Published in:
Proceedings of the 15th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES 2016)

DOI (link to publication from Publisher):
10.1109/CSE-EUC-DCABES.2016.247

Publication date:
2016

Document Version
Early version, also known as pre-print

Power Analysis of Energy Efficient DES Algorithm and Implementation on 28nm FPGA

Vandana Thind, Bishwajeet Pandey
Department of Electronic And Communication Engineering
Chitkara University
Punjab, India
vandanathind@gmail.com, gyancity@gyancity.com

D M Akbar Hussain
Department of Energy Technology,
Aalborg University
Denmark
akh@et.aau.dk

***Abstract*—in this work, we have done power analysis of Data Encryption Standard (DES) algorithm using Xilinx ISE software development kit. We have analyzed the amount of power utilized by selective components on board i.e., FPGA Artix-7, where DES algorithm is implemented. The components taken into consideration are clock power, logic power, signals power, IOs power, leakage power and supply power (dynamic and quiescent). We have used four different WLAN frequencies (2.4 GHz, 3.6 GHz, 4.9GHz, and 5.9 GHz) and four different IO standards like HSTL-I, HSTL-II, HSTL-II-18, HSTL-I-18 for power analysis. We have achieved13-47% saving in power at different frequencies and with different energy efficient HSTL IO standard. We calculated the percentage change in the IO power with respect to the mean values of IO power at four different frequencies. We notified that there is minimum of -37.5% and maximum of +35.8% variations. This work helps to design and implement DES algorithm with maximum power efficiency.**

Keywords—XILINX, Clocks Power, Signals Power, IOs Standard, Leakage Power, Supply Power, Maximum Power Efficiency, DES Algorithm, mean power, standard deviation.

I. INTRODUCTION

In this particular paper we have performed power analysis for DES algorithm,which is implemented on 28nm FPGA using SSTL as input-output standard. DES Algorithmis symmetric-key algorithm for theencryption of electronic data as shown in figure 1. It is identified need for the government-wide standard for encrypting unclassified, sensitive information. DES works by using the same key to encrypt and decrypt a message, so both sender and the receiver must know and use the same private key.

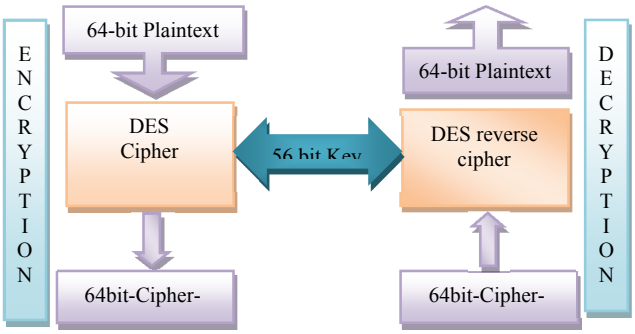

Figure 1: Block Diagram of DES Encryption

The input-output standard is provided to the physical layout of the circuit, to produce flexible and reliable interface to high frequencies bus. Power analysis basically helps us in detecting the effect of given sample. IO standards are used to communicate with ICs. We have considered five different WLAN channel i.e.,802.11b/g/n, 802.11y, 802.11y Public Safety WLAN, 802.11p and 802.11adhaving frequencies 2.4GHz, 3.6GHz, 4.9GHz, 5.9GHz and 60GHz respectively as shown in Table 1.

Table 1: List of WLAN Frequencies with Channels

Channels	**Frequencies**
802.11b/g/n	2.4 GHz
802.11y	3.6 GHz
802.11y Public Safety WLAN	4.9 GHz
802.11p	5.9 GHz
802.11ad	60 GHz

In this work, we have also done power analysis by changing different IO standards for the above mentioned frequencies. In xilinx, there are 29families of IO standards among which we have considered four members of HSTL IO standard family (i.e. HSTL- I, HSTL-II, HSTL-II-18, HSTL-I-18) as shown in figure 2. HSTL is High Speed Transceiver Logic. Futher we have calculated the percentage changes in power, at different frequencies, with different IO standard.

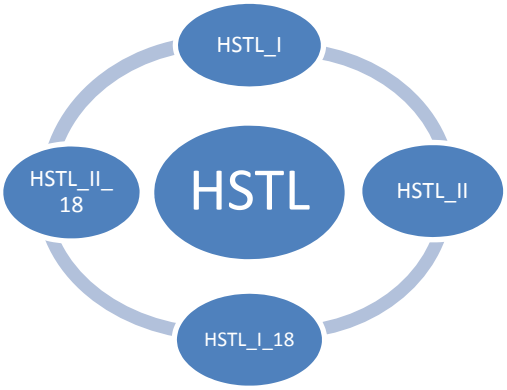

Figure 2: Types of HSTL IO-standard

II. RELATED WORK

Some researcher have implemented IO standard on LVDCI for the analysis of energy efficiency on different temperature i.e., for different regions [1]where we have done totally different analysis on power for different IO standards on DES algorithm[1]. A researcher had done research on energy efficiency of Gurumukhi Unicode reader on FPGA by implementing IO standard [2]. Therefore, we have done analysis on DES algorithm of encryption at different IO standards [2]. one scientist have done research, on digitally controlled impedance IO standard in memory interface design [3]where as we have used IO standard for power analysis which is totally different than this paper[3]. Some researcher have used LVCMOS as IO standard and done the analysis on operation of extreme and normal temperatures[4]. Whereas we have particularly done analysis on the energy efficiency of DES algorithm at different IO standards available on Xilinx by implementing them on different frequencies[4]. Another researcher have done the analysis on maximum ambient temperature by comparing the IO standards of two different FPGA technology [5]where we have considered single FPGA i.e.,Artix-7 and for the same FPGA we have analyzed percentage change in power utilized by changing WLAN frequencies[5]. In one research work, researcher has done analysis on the basis of performance comparison of security of DES algorithm[6]. Some researcher has done analysis on differential power of DES algorithm [7].Where we have used DES algorithm as well as IO standards together. Here, we did analysis of power on DES algorithm by varying IO standard.

III. DIAGRAM

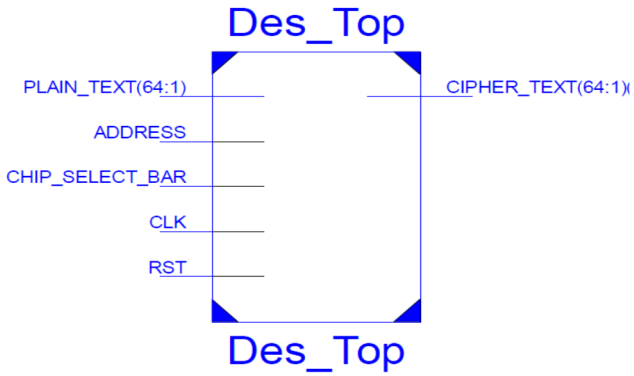

Figure 3: Top-level Schematic of DES Algorithm

The ISE software provide the xilinx synthesis technology, which helps insynthesis of HDL report. Here we synthesized macro statistics from HDL report that there are 128byte RAMs, 32 Registers, 120 tristate buffer which is individually of 1-bit and 16 XOR2. Whereas advanced HDL synthesis notify us that all the 120 tristate is being replaced by 1024 flip-flops.

IV. POWER ANALYSIS

In power analysis, initally we have taken four IO standards i.e.,HSTL- I, HSTL-II, HSTL-II-18, HSTL-I-18and we have analysised the change in power utilized by selective components on chip like clocks, logics, signals, IOs, leakage and total power calculated. At each IO standard we have taken into consideration five different frequencies i.e., 2.4GHz, 3.6GHz, 4.9GHz, 5.9GHz and 60GHz. One common thing we analyzed from this research is that power of clocks, logic, signals at different frequencies remains same in there domains of frequencies. The percentage changes along with detailed data is given below in tables.

A. Power analysis with HSTL_Ias IO Standard

Table 2:Comparison of On-chip Component using HSTL_I IO Standard

On-chip	2.4GHz	3.6GHz	4.9GHz	5.9GHz	60 GHz
Clocks	0.218	0.353	0.496	0.592	5.942
Logic	0.251	0.272	0.294	0.310	1.092
Signals	0.561	0.794	0.991	1.153	9.458
IOs	1.704	2.397	3.149	3.727	34.993
Leakage	0.050	0.054	0.059	0.064	0.773
Total	2.784	3.871	4.988	5.845	52.259

Table: 2 notify us the power dissipation, when we have taken input-output standard as HSTL_I. Here, we analyzed that with the increase in frequencies power utilization is also increasing, but there was problem when we increase the frequency to 60GHz. The percentages changes in IOs when frequency is increased from 2.4GHz to 3.6GHz is 28.9%, 3.6GHz to 4.9GHz is 23.8%, 4.9GHz to 5.9GHz is 15.5%.

Table 3: Power Statistics using HSTL_I IO Standard

	Mean	Std. Deviation	N
Clocks	.41475	.163852	4
logic	.28175	.025747	4
signals	.87475	.255537	4
IOs	2.74425	.881726	4
Leakage	.05675	.006076	4

We have also done analysis on the power statistics as shown in observation Table 3. We notified that mean of IOs power is 2.74425W.Where as the percentage change in IO power at different frequencies with respect to mean power is -37.9% for 2.4GHz, -12.65% for 3.6GHz, +12.8% for 4.9GHz and +26.3% for 5.9GHz as shown in figure 4. Above observation also show that standard deviation of IO power is maximum and leakage power have minimum standard deviation.

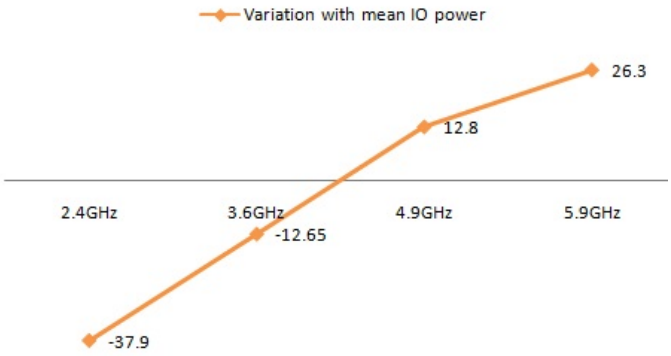

Figure 4: variation with Mean IO Power HSTL_I as IO Standard

B. Power analysis with HSTL_II as IO Standard.

Table 4: Comparison Of On-Chip Component Using HSTL_II IO Standard

On-chip	2.4GHz	3.6GHz	4.9GHz	5.9GHz	60GHz
Clocks	0.218	0.353	0.496	0.592	5.942
Logic	0.251	0.272	0.294	0.310	1.092
Signals	0.561	0.794	0.991	1.153	9.458
IOs	1.294	1.693	2.126	2.458	20.452
Leakage	0.049	0.051	0.055	0.057	0.773
Total	2.373	3.164	3.961	4.570	37.717

Table: 4 shows us the power dissipation, when we have taken input-output standard as HSTL_II. Here we analyzed the percentages changes in IOs power. When frequency is increased from 2.4GHz to 3.6GHz, percentages changes in IOs

power is 23.56%. Similarly, 20.36% and 13.5% reduction with frequency change from 3.6GHz to 4.9GHz and 4.9GHz to 5.9GHz respectively.

Table 5: Power Statistics using HSTL_II IO Standard

	Mean	Std. Deviation	N
Clocks	.41475	.163852	4
logic	.28175	.025747	4
signals	.87475	.255537	4
IOs	1.89275	.507384	4
Leakage	0.05300	.003651	4

Observation Table 5 shows power statistics using HSTL_II IO Standard. Above Observation notifies that mean of IOs power is 1.89275W which is of maximum value. The Percentage change observed in IO power at different frequencies with respect to mean power is -31.6% for 2.4GHz, -10.5% for 3.6GHz, +12.3% for 4.9GHz and +29.8% for 5.9GHz as shown in figure 5. Above statistical data also show that standard deviation of IO power is maximum and leakage power have minimum standard deviation.

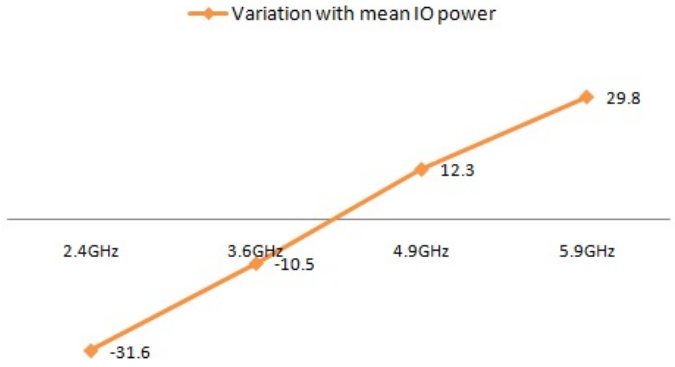

Figure 5: variation with Mean IO Power using HSTL_II as IO Standard.

C. Power analysis with HSTL_I I_18 as IO Standard

Table 6:Comparison of on-chip component using HSTL_II_18 IO Standard

On-chip	**2.4GHz**	**3.6GHz**	**4.9GHz**	**5.9GHz**	**60 GHz**
Clocks	0.218	0.353	0.496	0.592	5.942
Logic	0.251	0.272	0.294	0.310	1.092
Signals	0.561	0.794	0.991	1.153	9.458
IOs	1.556	2.008	2.499	2.877	23.297
Leakage	0.050	0.053	0.056	0.059	0.773
Total	2.636	3.481	4.336	4.991	40.563

Table 6 shows us the power dissipation when we have considered input-output standard as HSTL_II_18. The percentages changes in IOs power, when frequency is increased from 2.4GHz to 3.6GHz is 22.5%, 3.6GHz to 4.9GHz is 19.65%, 4.9GHz to 5.9GHz is 13.3%.

Table 7:Power Statistics using HSTL_II_18 IO Standard

	Mean	Std. Deviation	N
Clocks	.41475	.163852	4
logic	.28175	.025747	4
signals	.87475	.255537	4
IOs	2.23500	.575740	4
Leakage	0.05450	.003873	4

Table 7 infer the power statistics of observation Table which is power analysis using HSTL_II_18 IO standard here, we notified that mean of IOs power is 2.23500W.Where as the percentage change in IO power at different frequencies with respect to mean power is -30.3% for 2.4GHz, -10.2% for 3.6GHz, +11.81% for 4.9GHz and +28.7% for 5.9GHz as shown in figure 6. Above observation also show that standard deviation of IO power is maximum and leakage power have minimum standard deviation.

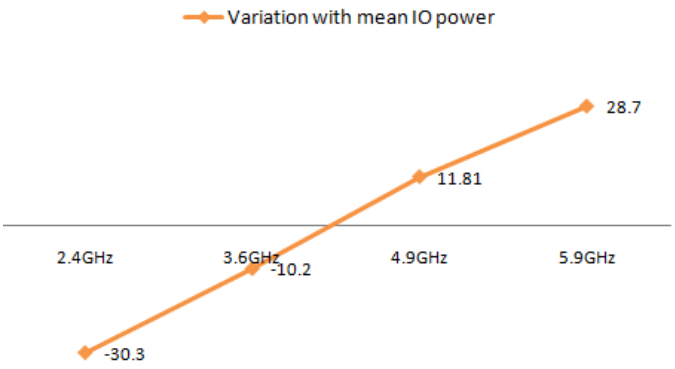

Figure 6: variation with Mean IO Power using HSTL_II_18 IO Standard.

D. Power analysis with HSTL_I_18 as IO Standard.

Table 8:Comparison of On-chip Component using HSTL_I_18 IO Standard

On-chip	**2.4GHz**	**3.6GHz**	**4.9GHz**	**5.9GHz**	**60 GHz**
Clocks	0.218	0.353	0.496	0.592	5.942
Logic	0.251	0.272	0.294	0.310	1.092
Signals	0.561	0.794	0.991	1.153	9.458
IOs	2.130	2.999	3.939	4.663	43.812
Leakage	0.052	0.057	0.064	0.069	0.773
Total	3.213	4.475	5.783	6.787	61.078

Table 8infers that the power analysis of HSTL_II_18 as input-output standard. There percentage changes in IOs power dissipation, when frequency is increased from 2.4GHz to 3.6GHz is 28.9%, 3.6GHz to 4.9GHz is 23.8%, 4.9GHz to 5.9GHz is 15.5%.

Table 9:Power Statistics usingHSTL_I_18 IO Standard

	Mean	**Std. Deviation**	**N**
Clocks	.41475	.163852	4
logic	.28175	.025747	4
signals	.87475	.255537	4
IOs	3.43275	1.103797	4
Leakage	0.06000	.008287	4

We have also done analysis on the power statistics as shown in observation Table 9. We notified that mean of IOs power is 3.43275W.Where as the percentage change in IO power at different frequencies with respect to mean power is -37.9% for 2.4GHz, -12.6% for 3.6GHz, +14.7% for 4.9GHz and +35.8% for 5.9GHz as shown in figure 7. Above observation also show that standard deviation of IO power is maximum and leakage power have minimum standard deviation.

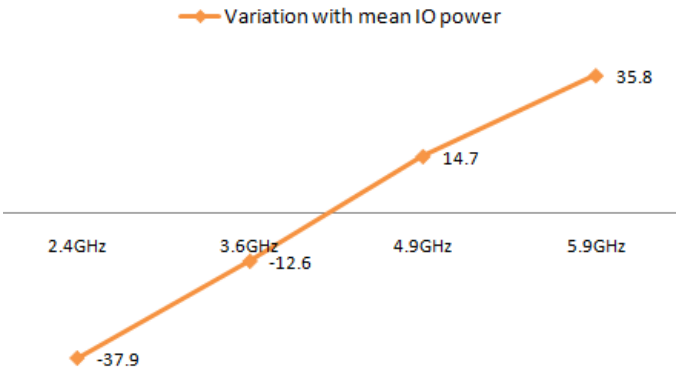

Figure 7: variation with Mean IO Power using HSTL_I_18 IO Standard.

V. COMPARISON OF POWER AT DIFFERENT IO STANDARDs

Table 10 shows the values of total on-chip power at four different input-output standards i.e HSTL- I, HSTL-II, HSTL-II-18, HSTL-I-18. Here, we have analyzed the percentage change in power, when frequency is changed from 2.4GHz to 3.6GHz, 3.6GHz to 4.9GHz, 4.9GHz to 5.9GHz as shown in figure 8.

Table 10: Comparison of total power at different IO standards

On-chip	2.4GHz	3.6GHz	4.9GHz	5.9GHz
HSTL_I	2.784	3.871	4.988	5.845
HSTL_II	2.373	3.164	3.961	4.570
HSTL_II_18	2.636	3.481	4.336	4.991
HSTL_I_18	3.213	4.475	5.783	6.787

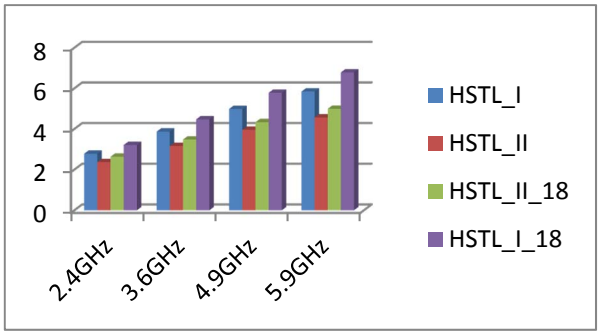

Figure 8: Power at Different Input-Output Standards

Table 11shows the percentage change in power when frequencies are changed.there is maximum percentage change in power when frequency changes from 2.4GHz to 3.6GHz at HSTL_II_18 as an IO standards, 3.6GHz to 4.9GHz and 4.9GHz to 5.9GHz at HSTL_I_18 as IO standardas shown in figure 9.

Table 11: Percentage Change in Power at Different Frequencies.

On-chip	2.4GHz to 3.6GHz	3.6GHz to 4.9GHz	4.9GHz to 5.9GHz
HSTL_I	39.04%	28.86%	17.18%
HSTL_II	33.3%	25.19%	15.37%
HSTL_II_18	47.31%	24.56%	15.11%
HSTL_I_18	40.8%	31.34%	18.38%

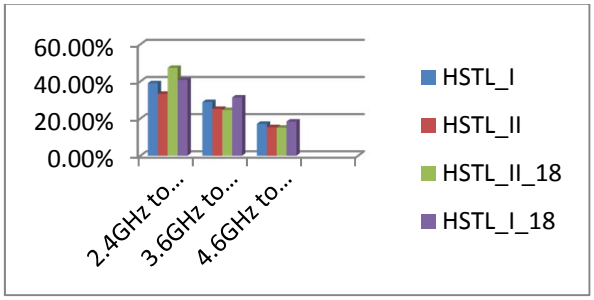

Figure 9: Variation in Power when Frequency is changed

VI. CONCLUSION

From this work, we have concluded that the power utilization by different component increase, if we change WLAN frequencies in ascending order. By changing the input-output standards we analyzed that there is variations in total power consumption by various components on chip. This analysis infers that when we change different frequencies, minimum saving in power take place with HSTL_II_18 and maximum saving take place with HSTL_I_18 input-output standard. We also noticed there is significant variation in power for lower frequency range. We calculated the percentage change in IO power with respect to, mean value of all power values of few on-chip component powers and also there standard deviation. From this we concluded that mean value of IO power is maximum, whereas for leakage power mean is minimum. Standard deviation of IO power is maximum and minimum for standard deviation.

VII. FUTURE SCOPE

This particular work of analysis has a bright future scope as whole analysis, done here is useful for the work which is particularly related to the power. This approach will help us to solve the problem of energy crisis, if we shall integrate these energy efficient IO standards in other algorithm and electronic devices. In future, we can also use LVCMOS, SSTL, LVDCI, MOBILE DDR, PIC, HSUL IO standards other than HSTL in DES algorithm. This design is implemented on 28nm FPGA. Therefore, there is open scope to re-implement DES algorithm on 20nm, 16nm FPGA and 3-D ICs and System on Chips(SoCs).

REFERENCES

[1] K. Goswami, et al. "Low Voltage Digitally Controlled Impedance Based Energy Efficient Vedic Multiplier Design on 28nm FPGA." *Computational Intelligence and Communication Networks (CICN), 2014 International Conference on*. IEEE, 2014.

[2] B. Pandey, and G. Singh. "Simulation of CMOS IO Standard Based Energy Efficient Gurmukhi Unicode Reader on FPGA." *IEEE 6th International Conference on Computational Intelligence and Communication Networks (CICN), Bhopal*. 2014.

[3] B. Pandey, and R. Kumar. "Low voltage DCI based low power VLSI circuit implementation on FPGA." *Information & Communication Technologies (ICT), 2013 IEEE 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. Kalia, et al. "I2C and HSTL IO Standard Based Low Power Thermal Aware Adder Design on 45nm FPGA." *Advanced Materials Research*. Vol. 1098. 2015.

[6] A. Nadeem, and M. Y. Javed. "A performance comparison of data encryption algorithms." *Information and communication technologies, 2005. ICICT 2005. First international conference on*. IEEE, 2005.

[7] P. Kocher, J. Jaffe, and B. Jun. "Differential power analysis."*Advances in Cryptology—CRYPTO'99*. Springer Berlin Heidelberg, 1999.