Differential Power Analysis Countermeasure for Improved DES with Dynamic Key Management

Toseef Abid, Muhammad Ali

Abstract — **Leakage of information in the form of side channel, from cryptographic hardware has opened up new ideas for intruders to break their security. This leakage is present in all type of hardware whether smart cards, FPGAs or ASICs. One of the most popular and effective information leakage is power. Differential Power Attacks (DPA) due to their effectiveness has become a great threat in the field of cryptography. In this paper, a countermeasure based on random power masking to avoid DPA is proposed for FPGA based hardware implementation of a dynamic key management for Improved Data Encryption Standard (IDES). Dynamic key management include three different key reconfiguration systems which can independently be used to generate sub-keys. Hardware implementation include, a 16 staged fully pipelined IDES with conventional Data Encryption Standard (DES) based, Linear Feedback Shift Register (LFSR) based, and Chaos Logistic Register (CLR) based key scheduling system. IDES having a 96 bit architecture which is more complex making it more immune to cryptographic analysis can give more throughput in as compared to simple DES. Three different key scheduling systems having 128 bit architecture includes more security in comparison to the 64 bit key systems. Implementation results of Virtex 7 series FPGA are operation frequency of 570 MHz and a throughput of 54.72 Gb/s.**

Index Terms — **IDES, DPA, LFSR, CLR, Key management system.**

I. INTRODUCTION

DES is amongst the few most widely used data encryption standards, and was developed by IBM in 1974. Despite its tremendous popularity and enormous use in the communication industry, the algorithm has some weaknesses which have been pointed out by IBM [1]. Because of the high processing capabilities being used now, it has become very easy to hack DES even with brute force. In 1999 RSA security organized Hank DES Challenge III in which it took 22 hours and 15 min to hack it by brute force [2]. Basically, DES is a symmetric key block ciphering suitable for long data streams. DES algorithm has a 64 bit key size and smaller S-boxes which should be improved in order to strengthen the cryptographic security DES [3]. Although the algorithm has its weaknesses but, DES and 3DES are still FIPS-approved encryption algorithms until 2030 to allow transition to AES [4].

Apart from the simple attacks over the passage of time, techniques have been created to hack cryptographic hardware which involve, putting as much information as one can about the cryptographic hardware and its capabilities and try to decrease the time in which one can hack that system. Most legendary amongst them all is the power analysis and attacks based on it [5-6]. Simple power analysis (SPA) which is one of the above mentioned attacks reveals information which is directly related to the data being processed and the mathematical functions applied on that data. A lot of information regarding encryption algorithm under attack is required in the technique. Second is differential power based hacking technique in which several thousand encryption processes are observed and their power consumption is recorded and saved along with their encrypted data. Once the real time data from the hardware is collected, one of the many possible keys is assumed and a simulated power consumption for different data, with a power model is generated. Then by using statistical analysis secret key is obtained [5].

Two main types of power models are available in literature; the hamming weight and the hamming distance power models. In the hamming weight power model number of "1s" in state variable is used in power calculation [7]. In hamming distance model number of bit changes in the state variables is used to calculate power [7]. Both of these power models have widespread use depending on the attacking technique and nature of the attack.

Due to an imminent threat of DPA attacks many methods to circumvent the problem have been formulized which can be categorized in to masking and hiding.

Masking techniques elaborated in [8-9] use masking of random numbers with data to decrease the correlation between measured power and predicted power by some power model. Masking techniques are vulnerable to higher order DPA [7].

Hiding of actual power due to encryption by simultaneously executing other different tasks is another way to prevent DPA succession, like [8] introduces dummy operation to create a path with constant execution [10] but this type of countermeasure effect the timing of cryptographic operation and thus the throughput.

Another technique of the same nature is presented in [11] where the use of true random numbers, generated form 12 number of 3 stage ring oscillators to add random power and break the dependency between predictable and measurable power.

A method placed in hiding technique is opted by [12] in which duplicate cores of the same algorithms are generated; one processes the original encryption and the duplicate core processes the complementary encryption. Significant succession in DPA resistance is obtained in this method but it consumes 50% more resources.

Toseef Abid, Muhammad Ali, Department of Electrical Engineering, University of Engineering and Technology, Lahore, Pakistan. E-mail: toseefabid@hotmail.com. Manuscript received June 25, 2015; revised on August 29 and December 05, 2015; accepted on December 28, 2015.

 ISSN – 1999-4974

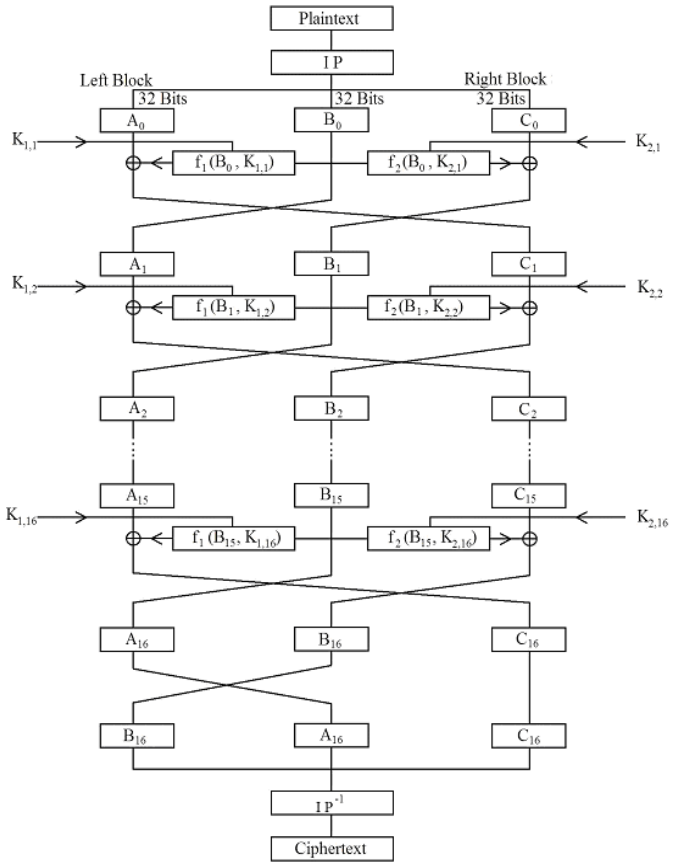


Fig. 1. Improved DES Architecture.

Randomised multi-modulo based on residue number system is presented in [13] for ECC. Random selection of modulo is presented in this work. Operation of double and add is used.

In [14] inverted operation of ring oscillators is added to the synchronous core to change the clock frequency, which adds variable time delays in the power traces. As the power consumption of any hardware spikes at the cloak event thus this method can easily be circumvented by using peak power only and more number of traces in DPA. The same is the case with [15] which inserts random delays in the data path in cryptographic core.

Numerous balancing techniques on logic circuitry level have been proposed using complementary operations to balance bit-flips. In [16] logic based on sense amplifier is discussed involving circuitry which consumes same amount of dynamic power despite the number of bit-flips and circuit level implementation with dual rail [17] do the same. Both techniques have proved to be the most usefulness against power attacks but cause a major wastage in hardware resources.

Wave dynamic differential logic (WDDL) [18-19] makes use of two complementary gate connected in parallel with each other which removes the dependency of power with data, as one gate is the complement of the other and if one goes for 0 to 1 the other goes from 1 to 0. This consumes balanced power but this type of countermeasure doubles the hardware resources.

TABLE I. DES EQUATIONS.

Encryption	Decryption
$L_i = R_i$ $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$	$R_{i-1} = L_i$ $Li\text{-}1 = R_i \oplus f(R_{i-1}, K_i)$ $= R_i \oplus f(L_i, K_i)$

TABLE II. IDES EQUATIONS.

Encryption	Decryption
$A_i = B_{i-1}$ $B_i = C_{i-1} \oplus f(B_{i-1}, K_i)$ $C_i = A_{i-1} \oplus f(B_{i-1}, K_i)$	$A_{i-1} = C_i \oplus f(A_i, Ki)$ $B_{i-1} = A_i$ $C_{i-1} = B_i \oplus f(A_i, K_i)$

In this paper, an improved version of DES having a fully multiplexed triple key configuration system with the capability to effectively use power masking to secure it from DPA based attacks. The rest of the paper is organized as follows: Section-II describes IDES. Section-III is about the dynamic key management in IDES. Section-IV discusses the resistance against differential power analysis and the hardware implementation of IDES. Section-V concludes the paper.

II. IMPROVED DES

The Improved DES (IDES) inherits the original block ciphering structure just like DES but instead of two blocks of 32 bits three blocks of 32 bits will be used making the total data block of 96 bits rather the 64 bits. The three blocks A, B, and C which are applied to encryption process as shown in Figure 1. The encryption and decryption equations of original DES are shown in Table I.

By applying the same mathematics we can get encryption and decryption equations for IDES. They are shown in Table II [1].

Initial and final permutations are inverse of one another and done on 96 bits. Function "f" is substitution and permutation involving data and round key. A_{16} and B_{16} in the last round should be interchanged.

Instead of using 64 bit key IDES uses 128 bit which is further divided into two parts K_1 and K_2 each of 64 bits. They are subjected to different mathematical techniques to generate 48 round keys. Round keys $K_{1,1}$ to $K_{1,16}$ are generated from K_1 and, Round key $K_{2,1}$ to $K_{2,16}$ are generated from K_2 which are applied to the function block.

III. DYNAMIC KEY MANAGEMENT

This part involves the implementation of a Linear Feedback Shift Register (LFSR) based, a Chaos Logistic Register (CLR) based and conventional DES key based key configuration system. LFSR and CLR are used to generate pseudo random codes. The original DES key, LFSR and CLR work together to improve the cryptographic strength of the design [20-21].

ISSN – 1999-4974

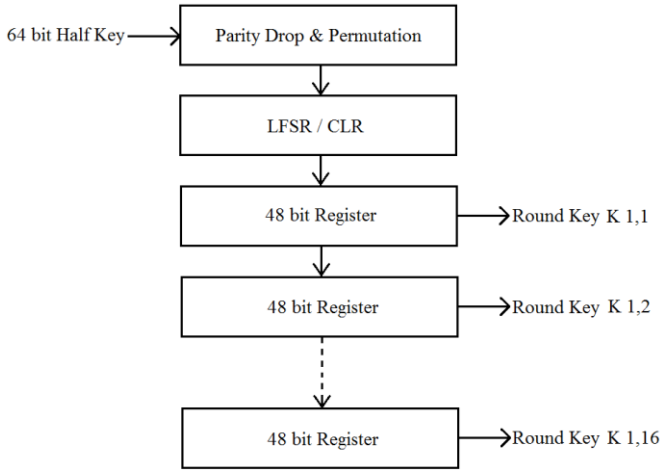


Fig. 2. LFSR / CLR based key configuration system.

A. *LFSR Based Key*

A linear feedback shift register of "n bit" width has a maximum state number 2^n that in our case is 2^{128} which is an extremely large number. LFSR in most cases is used to generate pseudo random codes. The randomness of LFSR output depends on two values, the "initial value" and the "tap coefficient" [23]. If we change the initial value or the tap coefficient, the state variation of LFSR and the randomness can be changed. Initial value is the first output and upcoming output variation depends on tap coefficient. LFSR only repeats a value once it completes a full cycle of its states. As the complete cycle of a LFSR is extremely large it is impossible that any number is repeated in a single session of communication. Implementation of LFSR based key is done by applying original key as initial value to obtain sub keys. The mathematical function of LFSR is given below.

$$a[n-1] = a[0] \quad \text{Eq. 1}$$

$$a[k] = tap\_coef[k] \,.\, (a[k-1] \oplus a[0]) \quad \text{for } n-2 \le k \le 0 \quad \text{Eq. 2}$$

B. *CLR Based Key*

Use of chaos logistic in cryptography and data encryption is eminent due to its lager spectrum, undeniable randomness and unpredictability. Use of two chaos logistics map to generate pseudo random numbers is discussed in [27] and three chaos logistics map is used in [28]. Extreme sensitivity of structural parameters and initial state make a strong argument for its use. The equation is given below.

$$X_{n+1} = r * X_n * (1 - X_n), \; (n = 1,2,3,4 \ldots.) \quad \text{Eq. 3}$$

X_n is a state variable and r is system parameter that controls the behaviour of the output and its randomness, its value can very between 1 to 4 but studies have shown that if the value of r is between 3 to 4 the system response reaches chaos [24]. Original key is applied as X_n in the above equation to obtain the sub keys.

Improved DES requires 32 different round keys each of 48 bits, to be generated from 128 bits of original key. They are obtained by first splitting the original key in two parts.

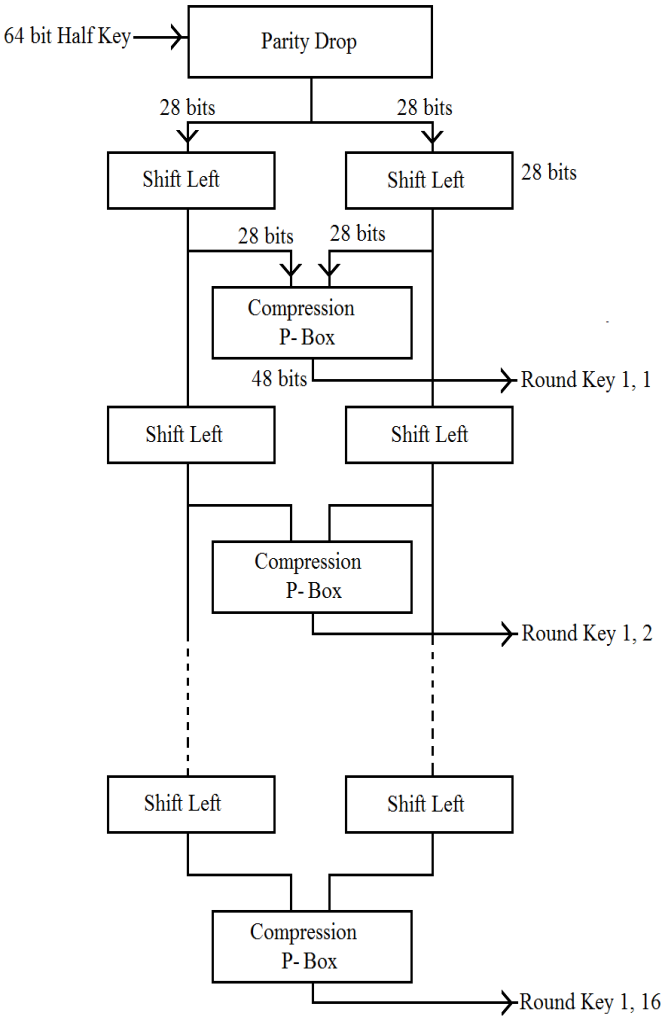


Fig. 3. DES Based key configuration system.

Each part is processed separately but with the same process. Initially parity bits form the 64 bit half key are dropped and remaining 56 bits are permuted and compressed to 48 bits by dropping every 7th bit. After this, it is fed to LFSR or CLR which then generates 16 round keys in 16 clock cycles which are transferred to a 16 stage pipeline of 48 bit registers. After 16 clock cycles, register loading is stopped and round key generation process is complete. Main clock supplied to key configuration systems is stopped during encryption process to reduce power. This is applied to both parts of the original key to generate 32 different round keys. LFSR/CLR based key configuration system is shown in Figure 2.

C. *DES Based Key*

Conventional DES based key configuration has the original DES key pipe line architecture. 128 bit key is divided in to two 64 bit halves. After removing parity and permutation, it is further divided into two parts. These halves are shifted to one or two positions depending on which round key is being generated and passed through key compression for all rounds keys [25]. 64 bit half key gives 16 round keys. This is done to both halves to get 32 sub keys for IDES. This is illustrated in Figure 3.

ISSN – 1999-4974

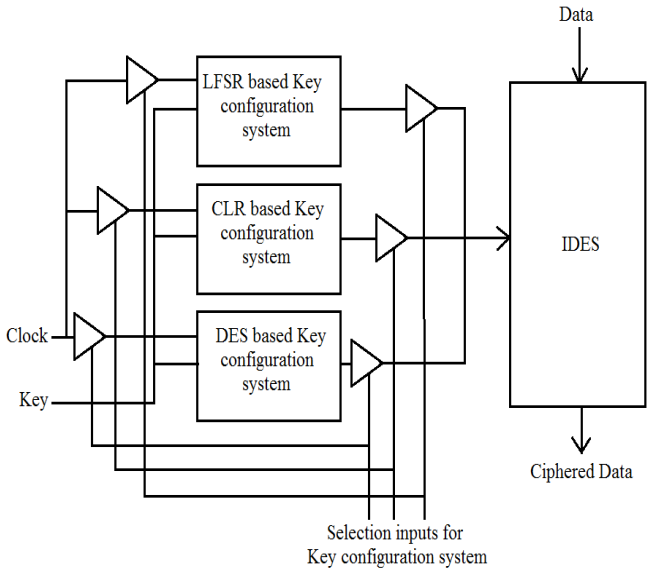


Fig. 4. Selection of key configuration system.

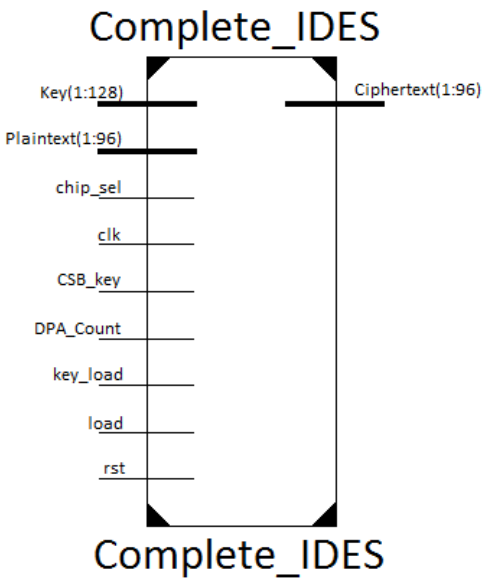


Fig. 5. RTL Schematic of Complete IDES.

D. Selection of Key Configuration System

Three key configuration systems are implemented in such a way that, original key is applied to all three systems, but the one which is enabled will generate 32 different round keys in 16 clock cycles, which will then be applied to improved DES and after an initial delay of 16 clock cycles encrypted data can be received after every clock cycle. If any one of the key configuration systems is enabled rest will not works as their clock can be disabled to reduce power consumption [26]. Three key configuration systems have tri-state gated output so the output of one cannot interfere with output of other key configuration system. This is shown in Figure 4.

IV. PROTECTION AGAINST DIFFERENTIAL POWER ANALYSIS

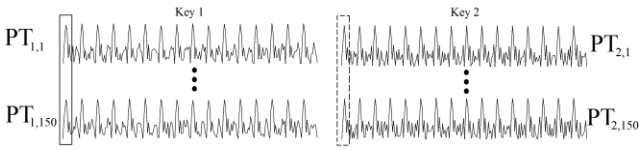
Power based attacking of cryptographic hardware makes use of the correlation between the real time power traces measured from the hardware and simulated power traces generated from computer, with an assumed key. Then by using statistical analysis, these two sets of power traces reveal the secret key. If there is no significant success, only the simulated power traces are to be generated with a different key and the same process is repeated again and again till success is achieved. To avoid this, the correlation between measured and simulated power traces is to be broken.

To achieve this, a power masking technique has been proposed using 128 bits LFSR and CLR working simultaneously to generate random power which will be added to the overall power consumption during the encryption process thus protecting the system from differential power analysis.

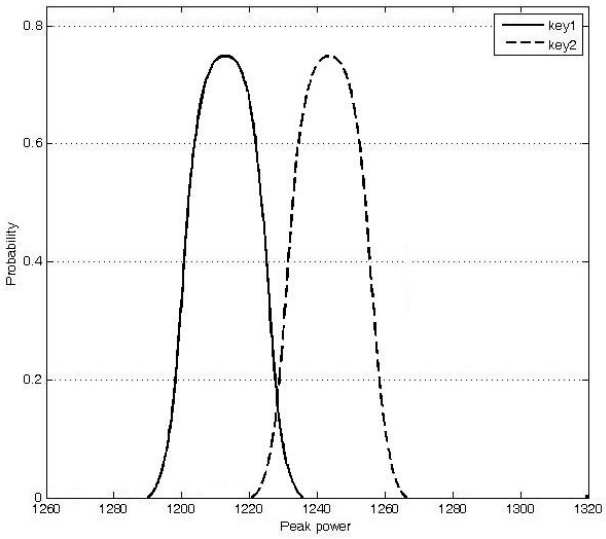
A. LESR and CLR based DPA Countermeasure

As discussed in previous section that during encryption process, clock of LFSR and CLR can be disabled to reduce power consumption. Proposed hardware has a provision of working in power saving mode and DPA protection mode as shown in Figure 5. If pin "DPA_Count" is asserted the power saving mode is disabled and in this case all processes will work exactly the same with a difference that when the encryption process starts, clock of LFSR and CLR will not stop. Two pseudo random number generators will continue to generate pseudo random number, though these number will not be utilized anywhere in encryption, but they will consume power in random amounts to provide protection against DPA.

Normally any type of DPA rely on a simple fact that when a data D_1 is encrypted by a key K_1 it will consume a



(a)



(b)

Fig. 6. (a) Power traces of unprotected IDES with two different keys. (b) Peak Power Distribution Function for unprotected IDES.

ISSN – 1999-4974

specific power. If we call this $PT_{1,1}$ it is evident that whenever D_1 is encrypted with K_1 using the same hardware they will result in the same power trace $PT_{1,1}$. If data is changed from D_1 to D_{150} using 150 different random data values with same key, different power traces can be obtained. All of them will be different from each other in a small amount. Lets call this power set $P_1=\{PT_{1,1}.....PT_{1,150}\}$. But if a different key K_2 is used for same data values from D_1 to D_{150}, the power set $P_2=\{PT_{2,1}.....PT_{2,150}\}$ will show significant change. This change can be observed in different mathematical and statistical characteristics of those power traces like, mean power distribution or peak power distribution. Xilinx Xpower simulation based power traces [29] for an unprotected IDES with 150 different data values and two different key is shown in Figure 6, along with peak power distribution of first round. It is clear from two far-apart peaks in the distribution that statistical analysis can be applied to detect a key with power analysis. Ideally, if these two peaks are at the same point it will be impossible to detect in between the two keys that which one is used and by extending the same idea, if all peaks are at the same point DPA will fail to detect any key.

Practically, it is not possible to bring all peaks at the same point. The best possible way is to bring them close and increase the standard deviation, so overlapping of curves will cause confusion in statistical analysis and stray the hacker form correct path.

In our DPA countermeasure, a key K_1 when applied to IDES module and all round key are generated by any one of the three key configuration systems, after which encryption process starts and data is fed to pipeline of IDES. Same data from D_1 to D_{150} is applied at 150 different time values, and power traces are saved for analysis. The same process is done for a second key K_2 with same data. Peak power distribution function for first round for all 150 readings shows a tremendous change from unprotected IDES readings. A shown in Figure 7, the standard deviation is largely increased, probability of peak value is also considerably reduced and overlapping area of two curves is 80 % of the total area under the curve which all lead to misleading results in DPA. These results are similar to those presented in [11]. They show a significant improvement in protection against DPA. Protected IDES utilizes 26.21% more power than unprotected IDES but increases the standard deviation to about 3 times. Probability of successful DPA is dropped from 72% to 18% by DPA countermeasure.

Attack applied on simple DES for differential power analysis tries to obtain 6 bits of secret key at first and repeat this process 8 times to obtain 48 bit round key. After successfully obtaining any round key, original key is obtained as the key configuration system of simple DES is fixed. This weakness of the architecture is also removed in our proposed work by using three key configuration systems. If an attacker tries to mount the same attack on IDES following problems in the attack will lead to more processing and false results.

- LFSR and CLR countermeasure adds more power to the overall power consumption which will prevent any DPA attack.

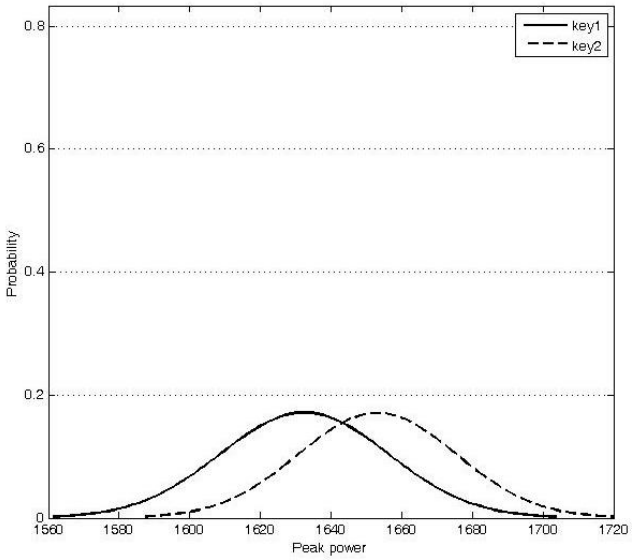


Fig. 7. Peak Power Distribution Function for IDES with DPA Protection.

- DES rounds has 8 S-Boxes but IDES round has 16 so, to obtain a round key double processing is required.
- Even if first two are somehow circumvented, and round key is obtained there is no way to find out which of the three key configuration systems is used to generate rest of the round keys.

B. Hardware Implementation

Hardware designing of all parts is done on Xilinx software with Verilog HDL as hardware description language. Hardware Synthesis of complete module is done on Virtex 7 series FPGA. Maximum clock speed of 570 MHz and a total of 54.72 G-Bits/Sec data throughput is achieved. Different Hardware resources of FPGA for complete IDES are given in Table III.

Test bench waveforms generated on Xilinx for different modules are shown in Figures 8 to 10. Figure 8 shows the output of a LFSR based key configuration while it is disabled. Figure 9 shows 16 sub keys generated in 16 clock cycles when LFSR based key configuration system is enabled. Figure 10 shows complete data encryption using IDES using the following inputs.

Key = 0123456789ABCDEFFEDCBA9876543210
Data =00000000000000000000000001
Ciphered Data=EAE16BEBA05C8867B0AE2C9F

TABLE III. SYNTHESIS RESULTS.

FPGA Resources	Complete IDES	LFSR Key Configuration System	CLR Key Configuration System
Slice Registers	4896	997	1632
Slice LUTs	6794	1638	1674
LUT-FF Pairs	4355	1536	1767
IOBs	294	-	-
BUFG/ BUFGCTRL/ BUFHCEs	4	-	-
DSP48	12	-	12

ISSN – 1999-4974

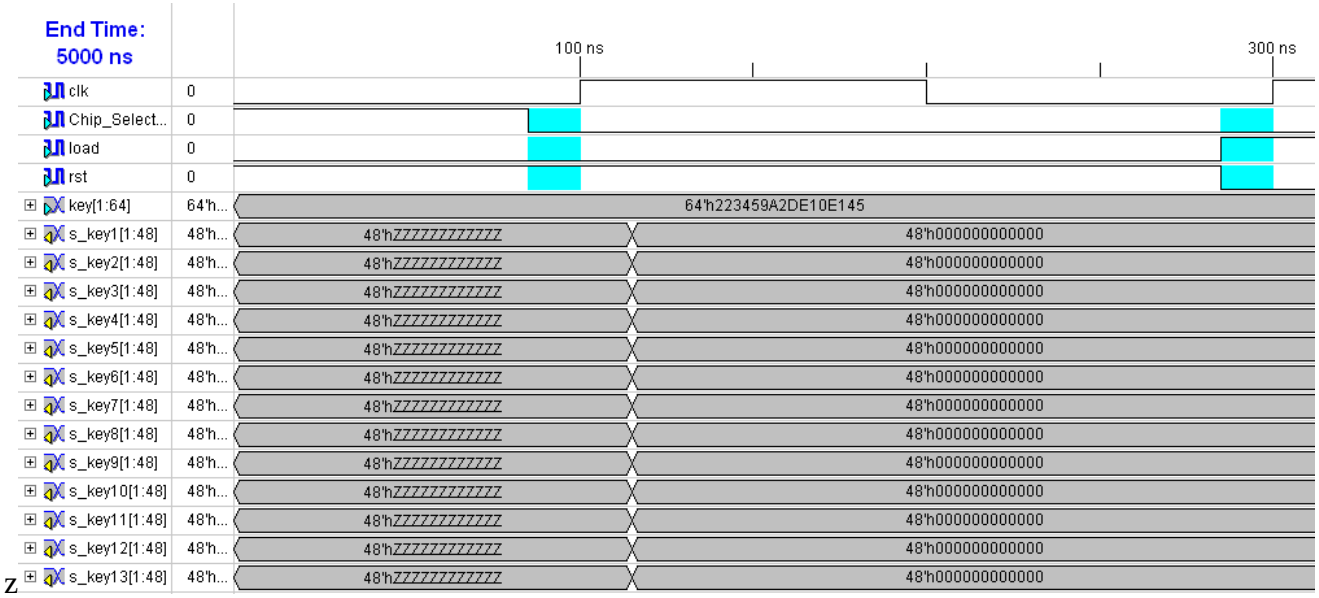


Fig. 8. Simulation (LFSR Key Configuration System Disabled).

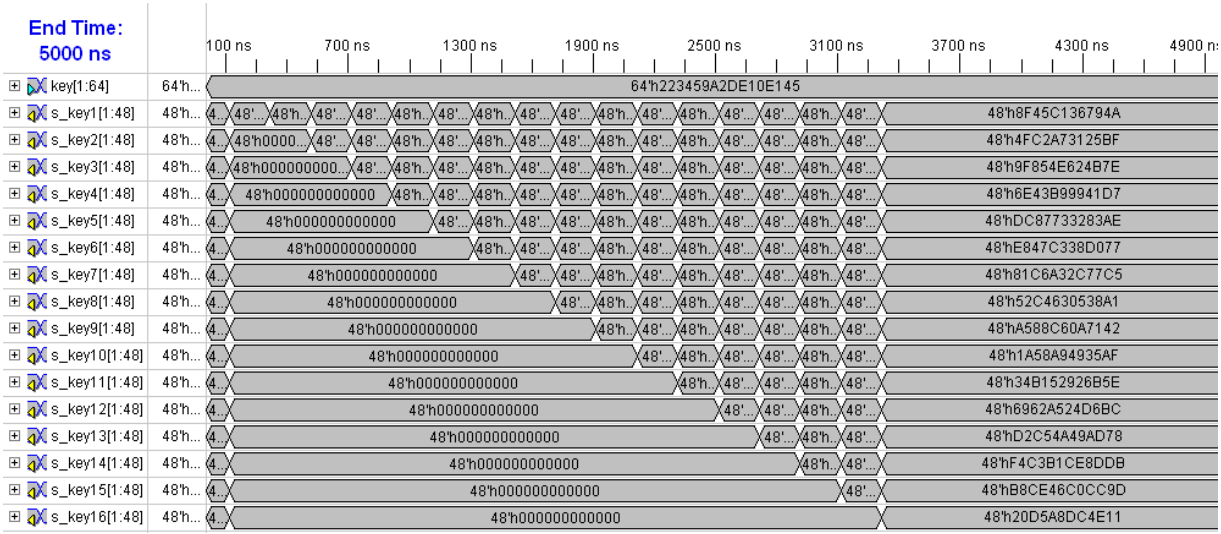


Fig. 9. Simulation (LESR Based Key Configuration System).

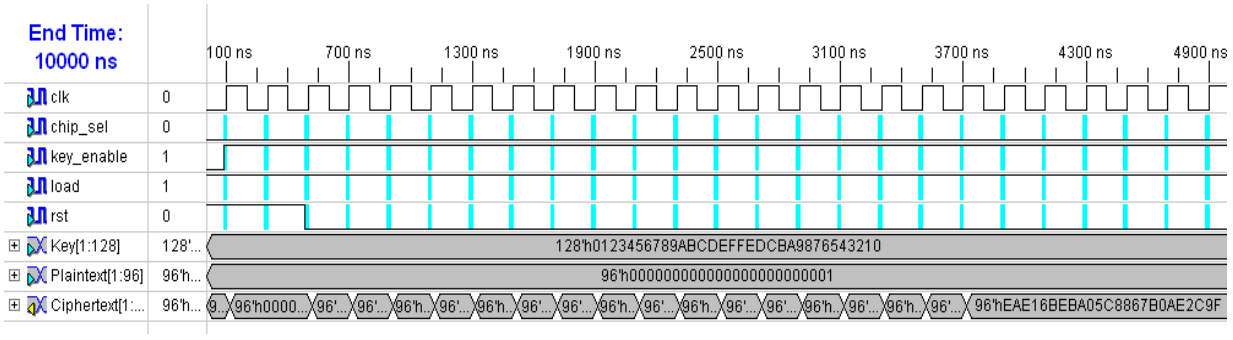


Fig. 10. IDES Simulation.

ISSN – 1999-4974

V. CONCLUSION

In this paper, hardware implementation of IDES and its three different key configuration systems in FPGA is presented. IDES inherits the basic block ciphering philosophy. Encryption function "f" is the same as of DES but in a complete pipe line of the encryption process it is used 32 times instead of 16 as in DES. Input data is divided into 3 parts which are subjected to the pipe line, and a 128 bit key instead of 64 bit key is used. The three different key configuration systems namely DES based key, LFSR based key and CLR based key are also presented. The complete pipe line architecture provides a maximum throughput of 54.72 Gb/s. Security of the algorithms is also improved as compared to DES because IDES uses more encryptions functions and lager key in the algorithm, which decrease the probability if successful hack over a fixed period of time. In addition to that LFSR and CLR based key configuration system add more security. Use of power masking through random number generators substantiates the security against power analysis attacks and use of gated clock for gated clock is implemented to eliminate the unnecessary wastage of power.

REFERENCES

[1] D. Coppersmith, "The Data encryption standard (DES) and its strength against attacks," *IBM jaurnsal Research Devwlop*, vol. 38, no. 3, pp. 243 – 250, 1994.

[2] RSA Security. RSA's DES Chalange III is solved in record time, Available at http://www.rsa.com/rsalabs/node.asp?id=2108, 18 January 1999.

[3] Seung-Jo Han, Heang-Soo Oh, Jangan Park "The Improved Data Encryption Standard (DES) Algorithm", *Spread Spectrum Techniques and Applications*, vol. 3, pp. 1310-1314, 1996.

[4] National Institute of Standard and Technology, Information technology library, "Recommendations for the TDES Block Cipher" *Special Publications*, http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf, January 2012

[5] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Introduction to differential power analysis", *Journal of Cryptographic Engineering*, vol 1(1) pp. 5-27, 2011.

[6] Stefan Mangrad, "A simple Power-Analysis (SPA) Attack on Implementation of the AES Key Expansion", Fifth International. Conference of International Security and Cryptology (ICISC), Seoul, Korea, 28-29 November 2002 Revised papers (LNCS, 2587), pp. 343-358

[7] S. Mangard, E. Oswald, T. Popp "Power Analysis Attacks: Revealing the Secrets of Smart Cards", *Springer* 2007

[8] M. Tehranipoor, C.Wang, "Introduction to Hardware Security and Trust", *Springer*, 2011.

[9] C. Gebotys "A table masking countermeasure for low-energy secure embedded systems", *IEEE Trans. Very Large Scale Integrated (VLSI) System*, vol 14, (7), pp. 740–753, 2006.

[10] M. Barbosa, D. Page, "On the automatic construction of indistinguishable operations", in *IMA International. Conference*, 2005, pp. 233–247.

[11] P. C. Liu, H. C. Chang, C. Y. Lee, "A True Random-Based Differential Power Analysis Countermeasure Circuit for an AES Engine", *IEEE Transactions on Circuits and Systems II*, Express Briefs 59 pp. 103–107, 2012.

[12] J.A. Ambrose, R.G. Ragel, "Multiprocessor information concealment architecture to prevent power analysis-based side channel attacks", *IET Computers & Digital Techniques*, vol 5, pp. 1-15, 2011.

[13] J. A. Ambrose, H. Pettenghi "Randomised multi-modulo residue number system architecture for double-and-add to prevent power analysis side channel attacks" *IET Circuits, Devices & Systems*, vol. 7, no. 5, pp. 283-293, September 2013.

[14] Y. Zafar, D. Har, "A Novel Countermeasure to Resist Side Channel Attacks on FPGA Implementations", *International Journal on Advances in Security*, vol. 2, no. 1, 2009.

[15] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, Y. Xie, "Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach", in *DATE 05: Proceedings of the conference on Design, Automation and Test in Europe, Washington DC, USA: IEEE Computer Society*, pp. 64-69, 2005.

[16] D. Hwang, P. Schaumont, K. Tiri, I. Verbauwhede, "Securing embedded systems", *IEEE Security and. Privacy*, vol 4, no 2, pp. 40–49, 2006

[17] D. Sokolov, J. Murphy, A. Bystrov and A. Yakovlev, "Design and analysis of dual-rail circuits for security applications", *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 449 - 460, 2005.

[18] K. Tiri, I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation", in *DATE 04: proceeding of the conference on Design, automation and test in Europe, Paris, France*, pp. 246-251, 2004.

[19] K. Tiri I. Verbauwhede, "A digital design flow for secure integrated circuits", *IEEE Transactions. CAD of Integrated Circuit Systems*, vol. 25, no 7, pp. 1197–1208, 2006.

[20] Ji Yaoa, Hongbo Kang, "FPGA Implementation of Dynamic Key Management for DES Encryption Algorithm", *Electronic and Mechanical Engineering and Information Technology*, Vol. 9, pp. 4795 – 4798, 2011.

[21] Khemraj Deshmukh "Key Reconfiguration in DES Algorithm", *International Journal of Digital Application & Contemporary Research*, Vol. 1, No. 6, Jan 2013.

[22] McLoone, M., McCanny, J.V. "High-performance FPGA implementation of DESusing a novel method for implementing the key schedule", *Circuits, Devices and Systems*, Vol. 150 No. 5 pp. 373–378, 2003.

[23] Michael D. Ciletti, "Logic Design with Behavioral Models of Combinational and Sequential Logic" in *Advance Digital Design with Verilog HDL*, Prentice Hall of India, 2005, ch 5, sec 5.10, pp 174-177

[24] V. Patidar, K. K. Sud, N. K. Pareek, "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing", *Informatica*, vol 33 no. 4, pp 441-452, 2009.

[25] Block ciphers and the Data Encryption Standard, [Online] https://engineering.purdue.edu/kak/compsec/Lectures.html

[26] A. M. Deshpande, M. S. Deshpande and D. N. Kayatanavar, "FPGA Implementation of AES Encryption and Decryption", IEEE International Conference on Control, Automation, Communication, and Energy Conservation, vol. 01, no. 04, pp.1-6,Jun.2009

[27] M. Francois, T. Grosger, "A New Psudo Random Number Generator Based on Two Chaos Maps" *Informatica* vol. 24, no. 2, 181-197, 2013

[28] M. Francois, D. Defour, "A Psudo-Random Bit Generator using Three Chaos Logistics Maps", 2013

[29] Xilinx Development System Reference Guide ch 12, Xpower available at http://www.xilinx.com/itp/xilinx10/books/docs/dev/dev.pdf

 ISSN – 1999-4974