PREDOMINANCE OF BLOWFISH OVER TRIPLE DATA ENCRYPTION STANDARD SYMMETRIC KEY ALGORITHM FOR SECURE INTEGRATED CIRCUITS USING VERILOG HDL

V. Kumara Swamy[1] Prabhu Benakop[2]

[1]Dept of ECE, Sreenidhi Institute of Science and Technology,Yamnampet, Ghatkesar, Hyderabad, Telangana, India

[2]Dept of ECE, Indur Institute of Engineering and Technology, Siddipet Dist, Telangana, India

ABSTRACT

Computer data communication is the order of the day with Information Communication Technology (ICT) playing major role in everyone's life, communicating with smart phones, tabs, laptops and desktops using internet. Security of the data transferred over the computer networks is most important as for as an organization is concerned. Hackers attempt hard to crack the software key and indulge in cyber crimes. In this paper, the main concern is not only to provide security to the data transferred at the software level but it provides the security at hardware level by the modified Blowfish Encryption and Decryption Algorithms. It results minimum delay, high speed, high throughput] and effective memory utilization compared to Blowfish (BF) and Triple Data Encryption Standard (TDES) algorithms. The implementation of Blowfish with modulo adder and Wave Dynamic Differential Logic (WDDL) is to provide security against Differential power analysis (DPA). In the proposed four implementations, BF with constant delay n-bit adder (BFCDNBA) yielded minimum delay, maximum frequency, high memory utilization and high throughput compared to BF with modulo adder and WDDL logic (BFMAWDDL), BF with modulo adder (BFMA) and TDES algorithms. The VLSI implementation of Blowfish and TDES algorithms is done using Verilog HDL.

KEYWORDS:

BF, TDES, WDDL, DPA, BFMA, BFCDNBA, BFMAWDDL, HDL.

1. INTRODUCTION

Many encryption algorithms have come into an existence for information confidentiality, authenticity, integrity, non repudiation and access control such as DES, TDES, Advanced Encryption Standard (AES) and Blowfish [4, 10] etc. This research work analyzes the merits and demerits of Blowfish compared to TDES algorithm in terms of their operation, propagation delay, memory utilization and throughput of the algorithms considered. The brief information about following algorithms is explained below:

1.1. DATA ENCRYPTION STANDARD (DES)

Data Encryption Standard encrypts 64-bit block plain text with 56- bits key length. It is a fiestel network. After initial permutations, it undergoes 16- rounds of processing steps. It can operate in Cipher Block Chaining (CBC), Electronic Code Book (ECB), Cipher Feedback (CFB) and Output Feedback (OFB) modes [10] [12]. It is prone to Brute Force attack in which hacker attempts to break the key by applying all possible combinations of inputs. It's a popular and most widely used algorithm before TDES, AES, and BF algorithms. It's an insecure algorithm [23] [10]

DOI: 10.5121/ijnsa.2017.9603

1.2. TRIPLE DATA ENCRYPTION STANDARD (TDES)

It is also known as Triple Data Encryption Algorithm (TDEA) which is triplication of Data Encryption Standard (3DES) applied to every 64-bits data block, came into an existence to overcome the brute force attacks commonly suffered by DES algorithm. It has 48 rounds of operations. In this method, three keying options are there:

- Three keys k1,k2 and k3 are independent
- Keys k1 and k2 are independent and k3 = k1.
- All three keys are equal, i.e., k1= k2 =k3.

Thus option-1 is the strongest among all three. It has 168 bits of independent key bits where as option-2 has 112 key bits which are moderately secured compared to the option-1. The last option is having 56 key bits as same as DES but used thrice in the algorithm because of all three keys are equal and prediction can be done easily. It is a symmetric key block cipher [16]. It is less secured than AES.

1.3. ADVANCED ENCRYPTION STANDARD (AES)

AES is a block cipher with variable key length. The block length is 128 bits and key length may be 128/192/256 bits with 9/11/13 rounds respectively. Each processing round consists of four steps, i.e., substitute bytes, shift rows, mix columns and add round key. AES encryption is flexible, more secured and fast [14] [20] [16]. It is a popular and secured encryption algorithm in the industry compared to DES [9] [12], but it is prone to side channel attacks.

1.4. BLOW-FISH (BF)

Blowfish is a symmetric block cipher with variable key length. The plain text is in 64-bit blocks but the key length varies from 32 to 448 bits. The data encryption occurs through 16-round fiestel network. Each round consists of plain text and key dependent operations such as XOR, ADD AND SUBSTITUTE etc. It's faster than TDES and AES [15] [17]. It's a replacement for DES algorithm [16] [4] [10]. Blowfish algorithm is used more than AES due to its large key length and high security. It provides high throughput compared to other algorithms considered in this research work [18, 21]

1.5. RELATED RESEARCH REVIEW

Literature review reveals that Blowfish Algorithm implemented using Verilog HDL gave better results in terms of reduced delay and increased throughput. To mention a few, the jest of few papers referred is given below:

Performance of blowfish algorithm based on field programmable gate array (FPGA) is analyzed in terms of speed, rate of encrypting the given data and power. Results indicate that the proposed Blowfish algorithm reduced delay and increases throughput with low power consumption compared to AES. This paper focused on small high-speed security architectures and systems with low power consumption for mobile devices [1].

The amalgamation algorithm consists of both Blowfish and Rivest Cipher 6 (RC6) to solve the security problems and maintains the efficiency. It provides faster data transfer and high security, both are very important for Wi-Fi applications. The collision attack problem is eliminated using S-Box overlapping process and Brute Force attack is eliminated using Sub key generation process. It decreases delay time and frequency [2].

Cloud computing needs secure, fast and area efficient cryptographic techniques. Blowfish cryptosystem is one of the strong and fast algorithms used for cryptography. It uses hybrid algorithm consists of RSA and blowfish algorithms and implemented using VHDL. It has

symmetric and asymmetric properties. Thus, it is more useful for cloud computing applications [3]

Various range application of blowfish algorithm can be implemented for data encryption sent from an Internet of Things physical network which has IP-based data. Performance metrics are analyzed such as Security, Complexity, propagation delay, and throughput of Blowfish Algorithm. Hardware implementation of blowfish algorithm on FPGA using VHDL which yielded reduced propagation delay and enhanced throughput [6, 18]

Conjugate- structure algebraic CELP coding method is used in speech encryption using Blowfish algorithm. A new method for generating S-boxes and P-arrays which are the main building blocks of the Blowfish algorithm is proposed which reduces time, complexity and provides more security [8].

Performance of symmetric encryption algorithms on power consumption for wireless devices is studied and analyzed to have less battery power consumption. The algorithms considered are DES, 3DES, AES, Blowfish, Rivest Cipher2 (RC2), and RC6. Energy efficiency is the main focus of this design [15, 19].

Blowfish has better performance than other commonly used encryption algorithms. Blowfish can be considered as an excellent standard encryption algorithm than AES. AES requires more processing power and more processing time than Blowfish algorithm [20].

Performance analysis of DES and Blowfish is done for wireless networks to provide security to the information. It presented about security, speed and power consumption. Results confirm that Blowfish algorithm runs faster than DES but power consumption is almost same even though blowfish has 448-bit key length and more number of iterations/operations [23].

2. THEORETICAL ANALYSIS OF BLOW-FISH ALGORITHM

Blowfish is a block cipher; encryption and decryption is performed in the block sizes of 64-bits. It is a 16-round fiestel network and symmetric algorithm. The plain text of 64-bits separated as two halves, 32 bit each (LE and RE). We perform 16-rounds of operations during encryption and decryption processes as shown in equation 1 and 2 respectively which involve XOR, Fiestel function (F), XOR and SWAP LE and RE operations in each round as shown in flowchart fig no.1. Fiestel function (F) involves XOR and modulo addition operation [7] [11].

The Encryption operation equation is given below in equation (1).

$$\begin{aligned} &\text{For } i=1 \text{ to } 16 \text{ do} \\ &RE_i = LE_{i-1} \oplus P_i; \\ &LE_i = F[RE_i] \oplus RE_{i-1}; \\ &\qquad LE_{17} = RE_{16} \oplus P_{18}; \\ &\qquad RE_{17} = LE_{16} \oplus P_{17} \quad \ldots\ldots\ldots (1) \end{aligned}$$

The Decryption operation equation is given below in equation (2).

$$\begin{aligned} &\text{For } i=1 \text{ to } 16 \text{ do} \\ &RD_i = LD_{i-1} \oplus P_{19-1}; \\ &LD_i = F[RD_i] \oplus RD_{i-1}; \\ &\qquad LD_{17} = RD_{16} \oplus P_1; \\ &\qquad RD_{17} = LD_{16} \oplus P_2 \quad \ldots\ldots\ldots (2) \end{aligned}$$

The flowchart depicts Encryption process of converting plaintext in to Cypher text as shown below

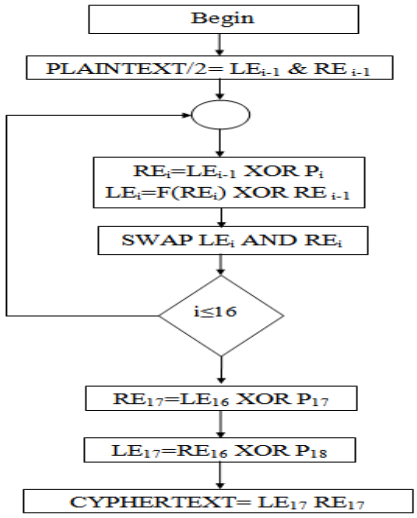

Fig.1.0: Encryption Process Flowchart

Fig. 1.0 indicates the complete process of LE and RE generations in every round of operation which includes XOR, Fiestel Function (F) and Swapping operation. Every round is supported by P-array elements.. After completion of 16-rounds of operations, LE_{16} and RE_{16} are XORed with P_{17} and P_{18} to generate RE_{17} and LE_{17}. LE_{17} and RE_{17} are concatenated to get the 64-bit Cyphertext as an output. Reverse operation is performed in the decryption process.

3. ARCHITECTURAL DESIGN OF PROPOSED BLOWFISH ALGORITHM

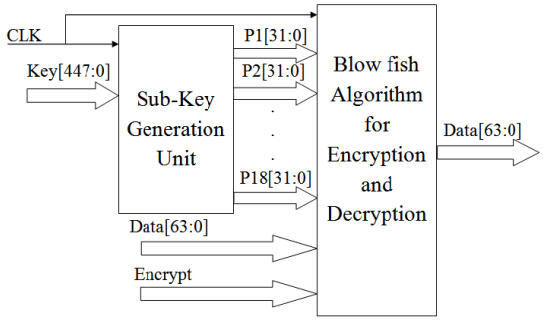

Fig.2.0: Top level Design module of Blowfish Algorithm

As shown in fig.2.0 above, Blowfish algorithm [5, 13] is divided in to two parts: Encryption & Decryption unit for data processing and Sub-key generation Unit for generation of sub-keys to be used in each round of operation. In the data encryption and Decryption block, input 64-bit data block is divided in to two halves as 32-bit Left Encryption (LE) and 32-bit Right Encryption (RE). In each round of operation, the algorithm will perform RE and LE operations as shown in equation (1) for encryption and equation (2) for Decryption which is also shown in fig.1.0 for Encryption process. The Fiestel function (F) in each round consists of combination of substitution, addition/modulo addition, XOR and addition/modulo addition operations. Thus, the algorithm follows the procedure for 16-rounds. RE_{16} and LE_{16} are XORed with P_{17} and P_{18} respectively to generate RE_{17} and LE_{17}. Reverse operation is performed for the decryption operation [7] [11] [22].

The sub-key generation unit is to generate 18- sub-keys (P-Array) from 448-bit input key, i.e., K-array has 14 input sub-keys of 32-bit each, can be used in generating P-Array of P1 to P18 initial sub-keys as shown in fig.2.0, each one is 32-bit in width which is updated as per the following equations (3):

P1=P1^K1, P2=P2 ^K2…P14=P14^K14,
P15=P15^K1, P16=P16 ^K2,
P17=P17^K3, P18=P18 ^K4; (3)

Where K1 to K14 (32-bits each) are generated from 448-bit input key.

3.1. MODULO- M-BIT ADDER:

In the encryption or decryption operation, modulo-addition operation [24] with and without WDDL logic is shown in fig.3.0. For increasing the speed of series adders in this figure can be operated in parallel. one adder adds Two h-bit residues, X and Y to form their sum $S_1+2^hC_{out1}$.Another one is 3-operand adder that computes "X+Y+m". Note that if $m=2^n+1$, we have h=n+1.It has been reported that if either Cout1 or Cout2 of this addition is '1' then the output is X+Y+m instead of X+Y. However, in the following we illustrate that only if the carry of "X+Y+m" is '1', it is sufficient to select it as the final output.

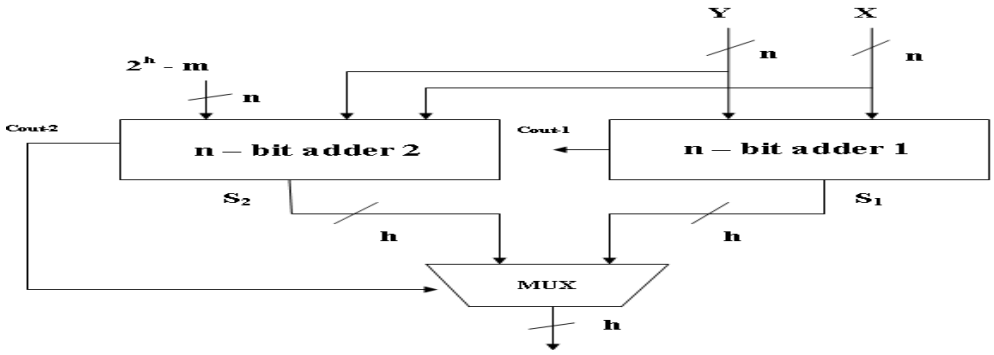

Fig.3.0: Modulo M –bit adder

3.2. CONSTANT DELAY N-BIT ADDER:

Constant Delay n-bit adder is adder is used to perform two array addition operations as shown in fig.4.0. The main advantage of this adder is irrespective of input the delay is constant so it's called Constant Delay n-bit adder.

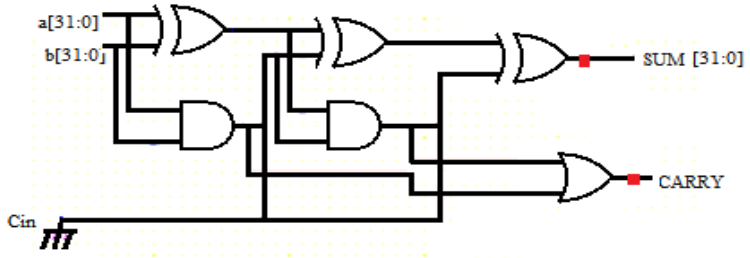

Fig.4.0: Constant Delay n-Bit Adder

The constant delay n-bit adder consists of three n-bit XOR gates, two n-bit AND gates, one n-bit OR gate. In this the input arrays are Xored in XOR n-bit gate and AND operation is performed in AND n-bit gate. The Output of AND n-bit gate is performed left shift operation and the resulted value XORed with output of XOR n-bit gate and AND operation with AND n-bit gate. Again the Output of AND gate is performed left shift operation and the resulted value XORed with output of present XOR n-bit gate. The output of XOR n-bit adder is declared as sum of constant delay n-bit adder. The MSB bit of each AND n-bit gate output before shift, is performed OR operation with OR gate and output is declared as carry bit output.

4. RESULTS AND DISCUSSION

The implementation of Blowfish Algorithm is done in three methods which are compared with Triple DES Algorithm. The implementation of the design followed bottom up approach. The test bench is written in Verilog HDL for every module of the design to provide 100% code coverage of the design. Top level Test Bench (TB) of the design is instantiated with top module of the design which consists of all the sub modules instantiated in it. Test cases are generated, applied to the Design Under Test (DUT) and results are generated for further verification of functionality, Delay estimation, frequency of the design and Throughput calculation. Mentor Graphics ModelSim is used for simulation. Xilinx ISE Design Suite14.2 is used to implement the design on Altera 6.3g_p1 (Quartus II 8.1). The synthesis tool Xilinx ISE 14.2 generated the RTL circuit, Memory Utilization, Propagation delay and even the percentage of area utilized by the design. The Comparison of the four implementations is given in the table.1. This paper compares delay, frequency, memory utilization and throughput of the four implementations listed in the table. 1.

Table.1 Comparison Of BFMAWDDL, BFMA, BFCDNBA And Triple DES Implementations

S NO	Crypto processor algo/parameter	Delay (ns)	Freq(10KHz)	Memory Utilization (Mb)	Throughput (Mbps)
1	Triple DES	197.241	506	294.74	320
2	BF with modulo adder and WDDL logic (BFMAWDDL)	112.566	888.4	469.384	570
3	BF with modulo adder (BFMA)	99.395	1006	460.808	640
4	BF with constant delay n-bit adder and WDDL Logic (BFCDNBA)	76.337	1309	520.584	840

In the delay comparison shown in fig.5.0, Blowfish with constant delay n-bit adder and WDDL logic implementation produces constant delay irrespective of number of stages of adders in the parallel adder design. Constant delay adder makes lot of difference in hardware implementation compared to modulo adder with and without WDDL gates. Hence, it resulted in lowest delay (76.337ns) compared to other implantations.

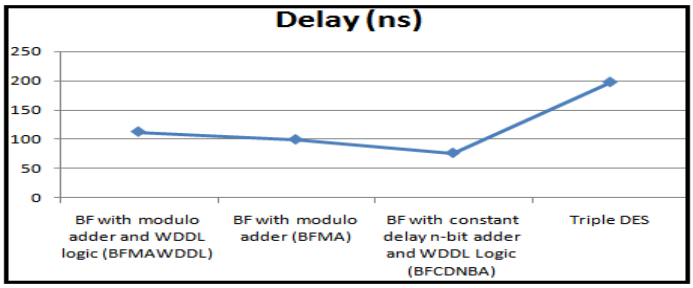

Fig.5.0: Delay comparison of BFMAWDDL, BFMA, BFCDNBA and Triple DES implementations

As the delay is less for Blowfish with constant delay n-bit adder and WDDL logic because of parallelism in implementing the hardware design,the frequency is more (13.09MHz) for

BFCDNBA implementation compared to TDES, Blowfish with modulo adder implementations as shown below in fig.6.0. As the frequency of design is high which can convert plaintext to ciphertext at faster rate. Triple DES , Blowfish with modulo adder with and without WDDL logic implementations are more of sequential implementations. Hence, they are slow. Critical path delay is reduced with effective implementation and thus the frequency is improved for constant delay n-bit adder approach.

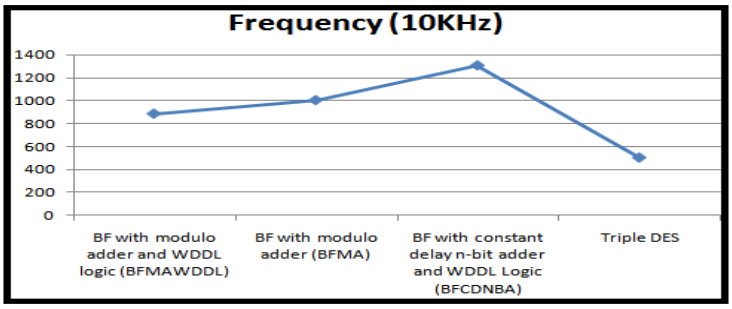

Fig.6.0: Frequency comparison of BFMAWDDL, BFMA, BFCDNBA and Triple DES implementations

As per fig.7.0 shown below, the memory utilization of BFCDNBA is more (520.584Mb) because more of parallelism in implementing the hardware design, data related to more number of operations and more iterations are to be stored than other implementations for high speed of Encryption and Decryption processes. S-Boxes are also called as Look Up Tables (LUTs) contains large number of data items to be stored in for future substitutions. Intermediate P-array keys are also requires more memory utility to generate sub-keys for every round of encryption and decryption operations.

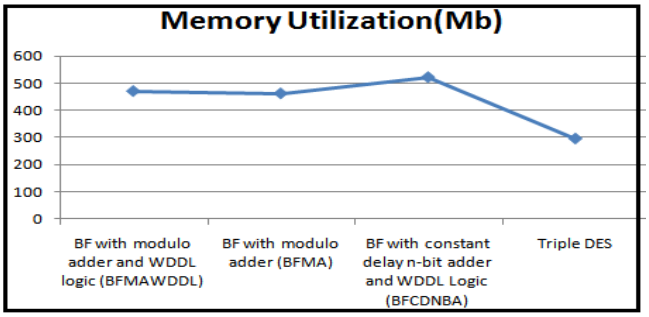

Fig.7.0: Memory Utilization comparison of BFMAWDDL, BFMA, BFCDNBA and Triple DES implementations

Throughput is defined as the ratio of number of bits Encrypted/Decrypted to the time taken by the algorithm. As per the results obtained shown in fig.8.0, BFCDNBA implementation yielded best throughput (840Mbps) compared to other implementations considered. As explained with respect to fig.5.0, the delay is very less in BFCDNBA implementation compared to other implementations considered in this research work. Hence throughput is very good in the BFCDNBA implementation.

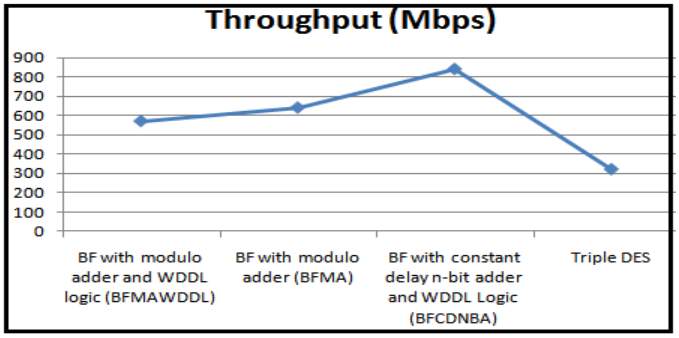

Fig.8.0: Throughput comparison of BFMAWDDL, BFMA, BFCDNBA and Triple DES implementations

As shown in fig. 9.0, delay of the Blowfish with constant delay n-bit adder and WDDL logic implementation is less and thus throughput of the same is more than the other implementations considered in this research paper. Even though the number of bits of the adder is increasing, the delay is constant and thus the throughput is increased with this approach.

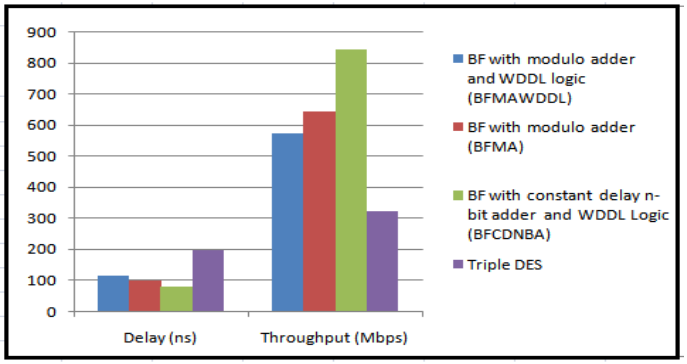

Fig.9.0: Delay and Throughput comparison of BFMAWDDL, BFMA, BFCDNBA and Triple DES implementations

5. CONCLUSIONS

As discussed in the results and discussion that BFCDNBA implementation gave better results compared to other implementations. Constant delay n-bit adder circuit used in the Blowfish Algorithm which reduced the delay to 76.337ns, increased frequency to 13.09MHz and thus increased throughput to 840Mbps compared to BFMAWDDL, BFMA and Triple DES implementations. It is providing more security because of 448 bit key length and incorporating WDDL logic in the Encryption and Decryption process of Crypto-processor digital design flow. However, the memory utilization is more (520.584Mb) for BFCDNBA implementation compared to other implementations considered in this research paper because of its complexity, more number of iterations/operations and more key length to provide at most security to the plaintext. Blowfish algorithm is developed in Verilog HDL and implemented it on ModelSim-Altera 6.3g_p1 (Quartus II 8.1) Web Edition and Xilinx ISE Design Suite14.2. This was run on a Windows 7 Home Basic (64-bit) Operating System, Intel® Core(TM) i3-2350M Processor @ 2.30 GHz clock rate with an internal Memory of 4 GB and 500 GB Hard Disk.

Future scope of this research work is to decrease the delay, improve the frequency and yielding better throughput compared to BFCDNBA implementation. This research work is also expected extend it analysis to compare the area utilization of the crypto algorithms considered in this design.

ACKNOWLEDGEMENT

The author would like to thank Dr. Prabhu Benakop for his continuous guidance and support to carry out this research work and present it in a systematic way.

REFERENCES:

[1] Rafidah Ahmad, AsrulnizamAbd. Manaf, "Development of an Improved Power-Throughput Blowfish Algorithm on FPGA", 2016 IEEE 12th International Colloquium on Signal Processing & Its Applications (CSPA),Vol 12, 06 March 2016.

[2] Nusrat Jahan Oishi, Arafin Mahamud, Asaduzzaman, "Enhancing Wi-Fi Security Using a Hybrid Algorithm of Blowfish and RC6",2016 International Conference on Networking Systems and Security (NSysS), 7-9 Jan, 2016..

[3] Viney Pal Bansal,Sandeep Singh, "A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), 21-22 Dec. 2015

[4] Ashraf Odeh, Shadi R.Masadeh, Ahmad Azzazi, "A Performance Evaluation of Common Encryption Techniques with Secure Watermark System (SWS)", International Journal of Network Security & Its Applications (IJNSA), Vol.7, No.3, May 2015, DOI : 10.5121/ijnsa.2015.7303

[5] Vaibhav Poonia, Dr.Narendra Singh Yadav, "Analysis of modified Blowfish Algorithm in different cases with various parameters", International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015 ISSN 2091-2730.

[6] Kurniawan Nur Prasetyo, YudhaPurwanto, Denny Darlis, "An implementation of data encryption for internet of things using Blowfish algorithm based on FPGA", Vol 2, 2014.

[7] V .Kumara Swamy, Dr Prabhu G Benakop, "High Throughput and High Speed Blowfish Algorithm for Secure Integrated Circuits", Ana le. Seria Informatică. Vol. XII fasc. 1 – 2014, Annals. Computer Science Series. 12th Tome 1st Fasc. – 2014

[8] Amaal A. Abd El-Sadek, Talaat A. El-Garf, Mohammed M.Fouad, "Speech Encryption Applying a Modified Blowfish Algorithm", October 2014.

[9] Meenakshi Shankar, Akshaya.P, "Hybrid Cryptographic Technique using RSA Algorithm and Scheduling Concepts", International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014, DOI : 10.5121/ijnsa.2014.6604.

[10] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona," Analysis and Comparison of Symmetric Key Cryptographic Algorithms based on various file features", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014, DOI : 10.5121/ijnsa.2014.6404.

[11] V .Kumara Swamy, Dr Prabhu G Benakop, "Performance Analysis of Secure Integrated Circuits using Blowfish Algorithm", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, Issue 17, Version 1.0,Page no.10-15, December 2013, Global Journals Inc (USA), Online ISSN. 0975-4172, Print ISSN.0975-4350.

[12] Kuo-Tsang Huang , Jung-Hui Chiu1 and Sung-Shiou Shen, "A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013, DOI : 10.5121/ijnsa.2013.5102

[13] Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012.

[14] M.Chandra Mohan, V.Kumara Swamy, Dr. T.Srinivasulu, "Design of High Speed AES Algorithm", International Conference on Electronics and Communication Engineering (ICECE-2012),GNIT, Hyderabad, Andhra Pradesh, India, 19-20,July 2012

[15] Monika Agrawal, Pradeep Mishra, 'A Comparative Survey on Symmetric Key Encryption Techniques', International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Vol. 4, No. 05, pp.877, May 2012

[16] Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks", International Journal of Computer Applications, ISSN: 09758887, Volume 44– No11, April 2012

[17] Walied W. Souror, Ali E. Taki el-deen, Rasheed Mokhtar-awady Ahmed, Adel Zaghlul Mahmoud - An Implementation of High Security and High Throughput Triple Blowfish Cryptography Algorithm, International Journal of Research and Reviews in Signal Acquisition and Processing (IJRRSAP) Vol. 2, No. 1, March 2012, ISSN: 2046-617X.

[18] Gurjeevan Singh, Ashwani Kumar Singla, K. S. Sandha - Through Put Analysis of Various Encryption Algorithms, IJCST Vol.2, Issue3, September 2011.

[19] Diaa Salama, Hatem Abdual Kader and Mohiy Hadhoud (2011), "Studying the Effects of Most Common Encryption Algorithms", International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011, pp 1-10.

[20] SimarPreet Singh, and Raman Maini (2011), "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127.

[21] A.Rathika, Parvathy Nair and Parvathy Nair (2011), "A High Throughput Algorithm for Data Encryption" International Journal of Computer Applications (0975 – 8887) Volume 13, No.5, January 2011 pp 13-16.

[22] V.Kumara Swamy, Dr Prabhu G Benakop and P.Sandeep, "Implementation of a digital design flow for DPA secure WDDL Cryptoprocessor using Blowfish Algorithm", Libyan Arab International Conference on Electrical and Electronic Engineering(LAICEEE-2010), Tripoli, Libya, October 23-26, 2010, pp.565-73

[23] Tingyuan Nie, Chuanwang Songa and Xulong Zhi (2010), "Performance Evaluation of DES and Blowfish Algorithms", Proceedings of 2010 IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), 23-25 Apr 2010. pp 1-4.

[24] Somayeh Timarchi, Keivan Navi - Improved Modulo 2n +1 Adder Design, International Journal of Computer and Information Engineering 2:7 2008.

AUTHORS BIBLIOGRAPHY:

V. Kumara Swamy completed his B.E (ECE) in1998 from Osmania University, Hyderabad and his M.Tech (DSCE) in 2005 from JNTUH, Hyderabad and pursuing PhD in the area of VLSI Design from JNTUH, Hyderabad. His areas of research include VLSI Design, advanced Digital Design, Cryptography and Computer Networks and Applications. He has published 8 research papers in international journals and conference proceedings. He has expertise in industry standard EDA tools such as Cadence, Mentor Graphics and Xilinx Tools etc. He has 20 years of teaching and research experience in India and abroad. He is currently working as an Associate Head, Department of ECE in Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India

Dr. Prabhu G Benakopis a renowned educationalist and he is currently working as Principal in INDUR Institute of Engineering & Technology, Telangana State, India. Formerly he held the positions of PRINCIPAL in Aurora's Engineering College, Director in Aurora's Technological and Research Institute, Hyderabad. He has 28years of teaching and research experience. Senior Member, IEEE, Member, International Biomedical Engineering, Life Member of Indian Society for Technical Education, Life Member of CSI, Life Member of Instrument Society of India. Guided/Guiding 11 research scholars under JNTUH, Hyderabad and VTU Bangalore for PhD programme. His areas of research include VLSI System Design, Embedded Systems, Computer Networks, and Biomedical Signal Processing. He has published more than 90 research papers in national, international journals and conference proceedings.