ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 29-34 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

A Concept Paper on Performance Trade-offs of Security Algorithms for Adhoc Networks

Pooja Srivastava[1], Dr. Seema Verma[2]
[1]Assistant Professor, Department of Electronics, Banasthali University, Rajasthan, India, pooja_enn@yahoo.co.in
[2]Associate Professor, Department of Electronics, Banasthali University, Rajasthan, India, seemaverma3@yahoo.com

Abstract Data security is an important issue in computer networks and cryptographic algorithms are essential parts in network security. Ad Hoc networks are much vulnerable to be attacked because of its characteristics. In this modest work, we have tried to study the problem of security in ad hoc networks.The comparative survey is carried out for the security schemes based upon the features like reliability, scalability, robustness and power consumption. The reason for choosing VHDL is its suitability for hardware implementation.

Keywords Clustering, IDEA, MANETs, VHDL

INTRODUCTION

Mobile adhoc networks (MANETs) are a collection of wireless hosts that communicate with each other through multi-hop wireless links, without the existence of any infrastructure or administrative authority. Therefore nodes must collaborate between them to accomplish some operations like routing and security. Regarding its costless, facility of use and deployment, MANET gets day after day new applications ranging from military applications for connecting soldier in battlefields and civil or commercial application such as Public and Personal Area Networks, virtual classrooms, emergency search and rescue operations in remote areas, other applications are recently under development will also benefit from MANETs advantages such as telemedicine, weather report and disaster environment.

MANETs nodes are more often part of a hostile environment that is not maintained professionally exposing the network to new risks ranging from physical attacks to eavesdropping due to the transmission range which often exceeds the area where the network is deployed. Because adhoc network is easily configurable chances of information leakage, eavesdropping, etc. increase. Hence a high security requirement is there for the adhoc network [5]-[7].

Adhoc network security is an important parameter to be considered while designing an adhoc network. Security goals that are to be kept in mind while designing a security algorithm for the adhoc network confidentiality of data, availability of network to every authenticated node, integrity of messages and non- repudiation of messages[8]-[11]. Two kinds of security algorithms are designed for Ad hoc networks namely symmetric algorithms (conventional encryption) and asymmetric algorithms (public key encryption). Symmetric encryption algorithm, shown in fig. 1, provides same encryption and decryption keys. The advantage of these algorithms is that they are fast and less complex. On the other hand, asymmetric algorithm shown in fig. 2, provides different keys for encryption and decryption so that receiver having particular key only also called private key of the receiver could access the data or information.

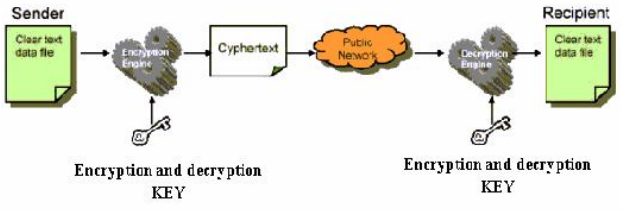

Fig 1: Symmetric Key Encryption and Decryption Process

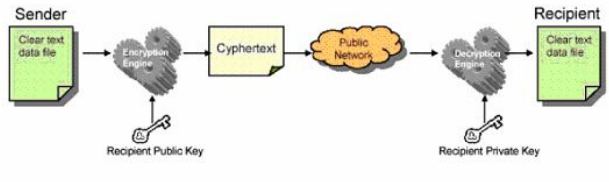

Fig 2: Public Key Encryption and Decryption Process

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 29-34 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

SYMMETRIC ALGORITHMS

A. Data Encryption Standard DES

DES has been a worldwide standard for data encryption for more than two decades now. On May 15, 1973, National Institute for Security Technologies (NIST) issued a public request for a data encryption algorithm. This request eventually resulted in the DES implementation. DES was officially endorsed by the U.S. government in 1977 as an encryption standard. Although it was originally developed by IBM (who holds the patent for DES), it has been extensively studied since its original publication. DES is, without doubt, the best-known and most widely used cryptosystem in the world [12].

B. The Advanced Encryption Standard AES

The Advanced Encryption Standard (AES) supersedes Data Encryption Standard (DES) as the new information protection standard defined by the United States to protect certain levels of federal information and communications. The selection process for an AES algorithm began in 1997, and the new standard was finalized in November 2001. The AES standard selected by the NIST specifies the Rijndael algorithm, which is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits [12].

C. Hash Algorithm

Hash algorithm concept was introduced in 1995, hash algorithm provided two functions simultaneously, firstly, encrypting the data to be send by a particular code and also dividing the data into fixed size packets so that problem of flooding does not occur. A hash function has many names, among others; message digest, fingerprint and compression function. A hash function H is a transformation that takes a variable-sized input m and returns a fixed-sized string, which is called the hash-value h (that is, $h = H(m)$). In general $H(m)$ will be much smaller in length than m; e.g., $H(m)$ might be 64 or 128 bits, whereas m might be a mega byte or more[13],[14].

ASYMMETRIC ALGORITHMS

A. RSA

RSA is perhaps the most well-known asymmetric or public key technique. Before we can use the RSA primitives, we must generate public and private RSA keys [13],[14].

B. Diffie-Hellman

Diffie-Hellman (DH) algorithm was one of the initial public key algorithms used to establish a secret between two parties by exchanging some messages through an insecure channel. In the DH algorithm, each of a given two entities A and B chooses a large prime p and a generator g of Z*. Both entity A and B choose a random secret a and b respectively. Then every entity computes respectively *ga* mod p and *gb* mod p and sends it over the insured channel. When this exchanging is achieved every party compute the secret k= *gab* mode p, which may be used to elaborate a secure channel between the two entities[14].

CONCEPT OF CRYPTOGRAPHY

Cryptography is a Greek word for "hidden writing" or the art and science of transforming (encrypting) information (plaintext) into an intermediate form (cipher text) which secures information in storage or transit. If an opponent acquires some cipher text, a vast number of different plaintext messages presumably could have produced that exact same cipher text, one for each of the possible keys. Cryptography includes at least: key generation, secrecy, message authentication.

PUBLIC KEY INFRASTRUCTURE

In order to protect critical applications and data and comply with new regulatory requirements, public key infrastructure (PKI) has recently increased in popularity for use in the banking, financial, and health care industries and in areas where the protection of proprietary data is imperative. A PKI is a set of technologies that enables an organization to ensure that similar levels and forms of trust that exist in the physical world are implemented in the digital world. It includes the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke certificates [14].

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 29-34 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

VLSI IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS

A. GODZUK Cryptographic Algorithm

The cryptographic GODZUK algorithm is a version of the GODZILLA algorithm, developed to be used in the third generation of cellular (according to the norms of the 3GPP). As GODZILLA, GODZUK is an algorithm of symmetrical key, whose operation structure is based on Feistel Network . The algorithm operates with blocks of 64 bits and with key of 128 bits, according to demands of the 3GPP. The algorithm is executed in eight rounds on Feistel Network. In the same way that in GODZILLA, the internal operations of the algorithm are operations of OR - exclusive, executed now in only two levels of functions SMER. GODZUK algorithm on the FPGA or ASIC demonstrated that it is possible to have a flexible, cheap and high performance implementation of a cryptographic algorithm on a standard host in adhoc network [15],[16].

B. Scalable Encryption Algorithm (SEA)

Scalable encryption algorithm (SEA) is a parametric block cipher for resource constrained systems. It was Initially designed as a low-cost encryption or authentication routine targeted for processors with a limited instruction set(i.e., AND, OR, XOR gates, word rotation, and modular addition). This algorithm takes the plaintext, key, *and* the bus sizes as parameters and, therefore, can be straight forwardly adapted to various implementation contexts and/or security requirements. This analysis explores the features of a low-cost field-programmable gate array (FPGA) encryption or decryption core for SEA [17],[18].

SEA **n** and **b** operates on various text, key, and word sizes. It is based on a Feistel structure with a variable number of rounds, and is defined with respect to the following parameters:

- n plaintext size, key size;
- b processor (or word) size;
- nb: number of words per Feistel branch;
- nr number of block cipher rounds.

Let x be a n=2-bit vector. We consider the following two representations.

- Bit representation: xb = x((n=2) □ 1) _ x(2) x(1) x(0).- - - - (1)
- Word representation: xW = xn □1 xn □2 _ x2 x1 x0.- - - - (2)

Implementation Results of SEA

Implementation results were shown by fig. 3, 4, 5 and 6 and extracted after place and route with the ISE 9.1 i tool from Xilinx on XC4VSX25 VIRTEX 4 platform with speed grade – 12 and package FF668. SEA exhibits a very small area utilization that comes at the cost of a reduced throughput. Consequently, it can be considered as an interesting alternative for constrained environments.

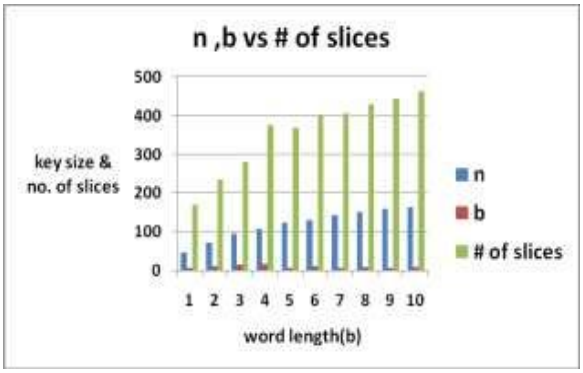

Fig 3: Reduction in Slices w.r.to n & b

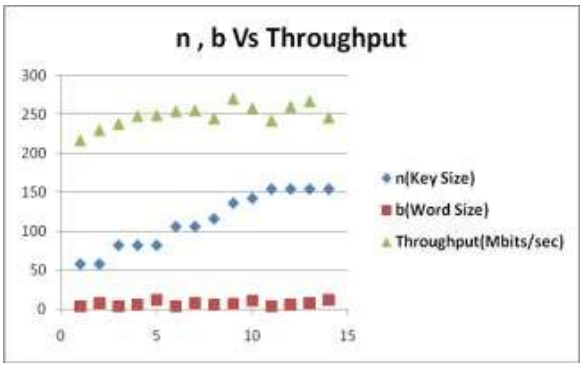

Fig 4: Increase in Throughput

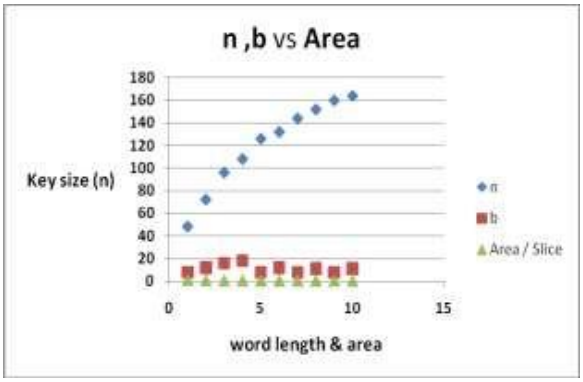

Fig 5: Reduced in Area / Slice

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 29-34 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

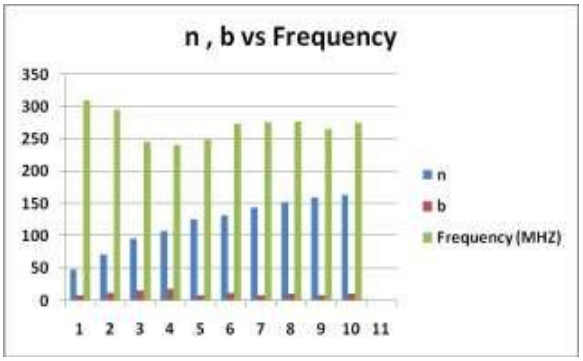

Fig 6: Change in the Frequency (MHZ) w.r.to key size & word length

C. Real-time FPGA-based Non-Cryptography System

Real-time FPGA-based Non-Cryptography System for Wireless Network Traditional privacy techniques for wireless communications are facing great challenges, due to the open radio propagation environment and limited options of transmission techniques. A new bilateral pilot aided protocol is presented, with single-tone based burst transmission over slow time varying flat fading wireless channels, and is investigated to enhance the security of quadrature amplitude modulation (QAM) system. In this concept, a real-time and link privacy method with FPGA-based design is proposed, which is based on the characteristics of radio channel including randomness and privacy [19].

The proposed approach is adequate for most real-time wireless communication and proposes the following bilateral piloting protocol for accessing the wireless channel:

1. A local oscillator (LO) at the transmitter is synchronized with a LO at the receiver.

2. The receiver sends a pilot signal, and starts sensing for a received signal.

3. The transmitter estimates the channel from the receiver and deduces the channel from itself to the receiver, based on channel reciprocity.

4. The transmitter sends a burst of QAM data symbols, compensated for channel phase and attenuation.

5. The transmitter stores the last 8 bits of each transmitted data, to be used as updated pilot signal by the receiver.

6. The receiver senses a received signal, and decodes the data symbols based on the a-priory known signal constellation.

7. The receiver tracks the time varying channel phase using some decision feedback method, and after a channel de-correlation period steps 2-6 are repeated, in step 2 receiver use updated pilot.

8. When the receiver needs to transmit a new pilot signal, it will use the last 8 bits of last received data to be used as a pilot and repeats the same steps from 2-7.

9. Repeats the steps from 2-8 according to a flow control mechanism in case of changing the transmission role between parities.

D. AES RIJNDAEL Algorithm

The AES Rijndael is a block cipher, which operates on different keys and block lengths: 128 bits, 192 bits, or 256 bits. The input to each round consists of a block of message called the state and the round key. It has to be noted that the round key changes in every round. The state can be represented as a rectangular array of bytes. This array has four rows; the number of columns is denoted by *Nb* and is equal to the block length divided by 32. The same could be applied to the cipher key. The number of columns of the cipher key is denoted by *Nk* and is equal to the key length divided by 32. The cipher consists of a number of rounds - that is denoted by *Nr* - which depends on both block and key lengths. Each round of Rijndael encryption function consists mainly of four different transformations: SubByte, ShiftRow, MixColumn and key addition. The proposed architecture is given by fig. 7.

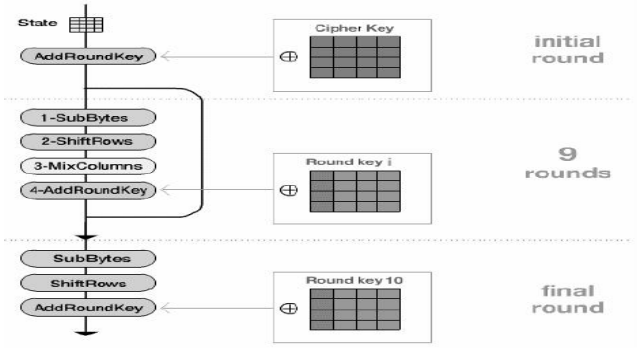

Fig 7: Overview of the AES Algorithm

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 29-34 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

On the other hand, each round of Rijndael decryption function consists mainly of four different transformations: Inv Sub Byte, Inv Shift Row, Inv Mix Column, and key addition. The 128-bit data block and key are considered as a byte array, respectively called "State" and "RoundKey", with four rows and four columns. The target hardware used in this paper is VirtexXC5VLX50 FPGA from Xilinx. Total area and Throughput results are presented and graphically compared [20]-[22].

E. RC4 Stream Cipher Based Algorithm

Wi-Fi Protected Access (WPA), WPA uses RC4 stream cipheras a security algorithm with new dynamic key managementmethod known as Temporal Key Integrity Protocol (TKIP). RC4 uses a variable length key from 1 byte to 256 bytesto initialize a 256-byte array. There are two 256-bytes arrays, S-Box and K-Box. The S-array is filled linearly such as S0=0, S1=1, S2=2 …….. S255=255. The K-array consists of thekey, repeating as necessary times, in order to fill the array. The RC4 algorithm works in two phases, key setup and pseudorandom key stream generation phase.

During N-bitkey setup (N being your key length), the encryption key isused to generate an encrypting variable using two arrays, s-array, k-array and N-number of mixing operations. These mixing operations consist of swapping bytes according toRC4 algorithm.RC4 uses two counters, counter i and counter j, which are initialized to zero value. RC4 uses two counters, counter i and counter j, which are initialized to zero value [22].

In the key setup phase the S-box is being modified according to pseudo-code:

Key setup phase:

For i= 0 to 255 j = (j + Si + Ki) mod 256 Swap Si and Sj Once the encrypting variables are produced from the key setup phase, it enters in the pseudorandom key stream generation phase.

The pseudorandom key stream generation phase is given by the following pseudo code:

Key stream generation phase:

i=(i+ 1)mod256 j = (j + Si) mod 256 Swap Si, and Sj t = (Si + Sj) mod 256 K=Si. The proposed architecture is given by fig. 8.

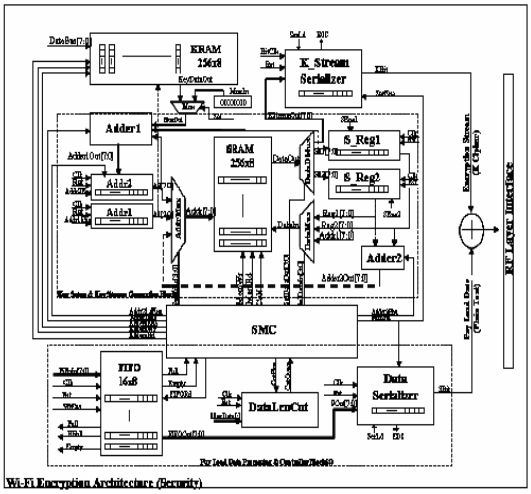

Fig 8: Hardware Module

The proposed architecture was captured by using VHDL. All the system components were described with structural architecture.

F. Secure Clustering Algorithm

A secure clustering algorithm based on reputation in defence of threats in clustering. In the algorithm, the nodes' reputation is used to improve security, which is evaluated by combining the experience of the node in the routing process. In addition, we consider degree and relative mobility in the clustering to guarantee the stability of clusters. The weight of each node is computed through considering the above three factors simultaneously. It is used to elect the secure backbone nodes in the networks.

Moreover, it is efficient in the cluster rebuilding and healing. In this algorithm, a reputation evaluation mechanism based on the behaviours of nodes is built to achieve accurate definition and precise quantization of reputation for nodes in the network. To improve the reliability of a cluster structure, this algorithm considers the reputation, correlation and mobility of nodes in the process of electing cluster heads and gateways. Moreover, the rebuilding and recovering mechanism in the algorithm is able to resist attacks on the cluster structure [1]-[3].

G. IDEA Algorithm

International Data Encryption Algorithm (IDEA) have found various applications in secure transmission of the data in networked instrumentation and distributed measurement systems. IDEA provides data integrity, authentication, and confidentiality. Previously there are many encryption standards for secure data transmission like RC5, RC6, DES and AES. But, IDEA is a superior encryption standard compared to any other encryption techniques. IDEA is a secret-key cipher whose encryption and decryption processes are symmetric. The cipher IDEA is an iterated cipher consisting of 8 rounds followed by an output transformation. It takes 64bit plaintext inputs and produces 64bit cipher text outputs by using a 128bit key. This can be used in very high speed & low power encryption/ decryption algorithms [4], [23]-[24].

CONCLUSION

In this paper, we have surveyed the security algorithms for Mobile adhoc networks. We gave a brief description about all the advance schemes discussed above and then a comparative survey has been provided. The Analysis gave a interesting result that the IDEA provides data integrity, authentication, and confidentiality and Secure Cluster Algorithm provides the rebuilding and recovering mechanism so it is able to resist attacks on the cluster structure. Scopes for further research include low power ASIC implementations purposed for RFIDs as well as further cryptanalysis efforts and security evaluations.

ACKNOWLEDGEMENTS

This work is supported by Department of Electronics, Banasthali University, Rajasthan, India.

REFERENCES

[1] D. Wei and H. A. Chan., Clustering Ad Hoc Networks: Schemes and Classifications. *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*. 2006, pp. 920 – 926.

[2] A. Akbari, A. Khosrozadeh and N. Lasemi., Clustering Algorithm in Mobile Ad Hoc Networks, *Computer Sciences and Convergence Information Technology*, 2009, pp. 1509-1513.

[3] M. Chatterjee, S. K. Das and D. Turgut., WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks, *Cluster Computing*. 2002, **5** (2): 193–204.

[4] Modugu.R, Yong-Bin Kim, Minsu Choi, "Design and performance measurement of efficient IDEA crypto hardware using novel modular arithmetic components", Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE, 3-6 May2010, pp1222-1227.

[5] Panagiotis Papadimitratos, Member, IEEE, and Zygmunt J. Haas, Senior Member, IEEE. *Secure Data Communication in. Mobile Ad Hoc Networks*. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO.2,2006 pp 343,356.

[6] Mohsen Guizani. "*Security and Trust in Mobile Ad Hoc Networks"*. Proceedings of the 4th Annual Communication Networks and Services Research Conference (CNSR'06). 2006.

[7] Konrad Wrona, *"Distributed security: ad hoc networks & beyond"*.Ad Hoc networks security, pompas workshop, 2002.

[8] NIST (National Institute of Security and Technologies). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*. Technical report

[9] Shariful Islam. *Efficient Key Management Scheme for Mobile Ad Hoc Network*. Master of Science. Royal Institute of Technology (KTH) SecLab Department of Computer and System Sciences (DSV). Stockholm, Sweden, 2005.

[10] Adam Burg, *Ad hoc networking: concepts, applications, and security*. Ad hoc network specific attacks Seminar, Technische Universität München, 2003.

[11] Tor Inge Skaar, Tor-Erik Thorjussen, *Security Specification, Access Control and Dynamic Routing for Ad-Hoc Wireless Networks applied to Medical Emergencies*. Project report Norwegian University of Science and Technology Faculty of Information Technology, Mathematics and Electrical Engineering, 2003.

[12] Tara M., Charles R.Elden,2002. *Wireless security and privacy Best Practices and Design Techniques*, Addison Wesley.

[13] Stinson Douglas, Vande May Serge. Cryptographie : théorie et pratique. Vuibert, 2001.

[14] John Rittinghouse, James Ransome, 2004. *Wireless operational security*, Digital Press.

[15] Barbosa, V., An Introduction to Distributed Algorithms. published in the MIT Press, 1996.

[16] Schneier, Bruce, "Applied Cryptography", Second Edition, John Wilwy & Sons inc., 1996.

[17] B. Praveen Kumar, P. Ezhumalai, S. Sankara Gomathi, Efficient Implementation of a Scalable Encryption Algorithm using FPGA, International Journal of Computer Applications (0975 – 8887), Volume 3 – No.10, July 2010.

[18] F. Mace, F. X. Standaert, and J.-J Quisquater "FPGA implementation(s) of a Scalable Encryption Algorithm," in IEEE Transaction on very large scale integration (VLSI) systems ,VOL.16, NO. 2, FEBRUARY 2008.

[19] Ali M. Allam, M. M. Abutaleb, "Real-time FPGA-based Non-Cryptography System for Wireless Network", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 2, May 2012.

[20] F. R-. Henriquez, N. A. Saqib and A. D. Perez, "4.2 Gbits/s single chip FPGA implementation of AES algorithm", *Electronics Letters*, Vol. 39, No. 15, pp. 1115-1116, 2003.

[21] I. A-. Badillo, C. F-. Uribe and R. C-. Para, "Design and implementation of an FPGA-based 1.452 Gbps non pipelined AES architecture", in Proc. of the International Conference on Computational Science and its applications, *Lecture Notes in Computer Science, Springer-Verilog*, Vol. 3982, pp. 446-455, 2006.

[22] D. S. Kundi, S. Zaka, Q. Ain and A. Aziz, "A compact AES encryption core on Xilinx FPGA", in Proc. of *2nd International Conference on Computer, Control and Communication*, pp.1-4, 2009.

[23] M.P.Leong, O.Y.H Cheung, K.H.Tsoi, and P.H.W.Leong"*A Bit-serial implementation of the International Data Encryption Algorithm IDEA"*. In B.Hutchings, editor, IEEE Symposium of Field Programmable Custom Computing Machines, pages 122 -13. IEEE Computer Society, 2000.

[24] Dr. Salah Elagooz, Dr. Hamdy,Dr. KhaledShehata and Eng.M. Helmy, "Design and implementation of High and Low Modulo (216+1) multiplier used in IDEA Algorithm on FPGA", 20th National Radio Science Conference CAIRO, Egypt , March 18-20 , 2003.