An Enhanced Encryption Algorithm for 4G Networks

Prerana Choudhari[1]
Information Technology
Thakur College of Engg & Tech
Mumbai, India

Vikas Kaul[2]
Information Technology
Thakur College of Engg & Tech
Mumbai, India

S K Narayankhedkar[3]
M.G.M College of Engg & Tech
Navi Mumbai, India

Abstract*— This paper, presents the design and evaluation of enhanced encryption algorithm for 4G networks. An enhancement is done by modifying the S-box of AES algorithm and complexity is increased by using AES in Round structure. The static S-box is made dynamic using cipher key. The inverse S-box is also modified accordingly. 4G simulation model is developed by using AWGN channel and BPSK modulator/demodulator. Comparison is made between AES and the enhanced system on the basis of performance evaluation based on Runtime and Throughput.

***Keywords*—3G; 4G; AES; S-box; Round structure**

I. Introduction

4G, the next-generation mobile telecommunication system, is being model for increased security and reliable communication. 4G wireless networks will operate entirely on the TCP/IP, so it becomes completely IP based. This makes 4G wireless technologies different from 3G and other preceding versions [1]. The 4G systems will support both the next generation of mobile service as well as the fixed wireless networks [24].

AES is one of the encryption techniques which are used most frequently because of its high efficiency and simplicity. It is the highly secure algorithm. Currently there are three cipher suites in 3GPP UMTS systems; including a block cipher Kasumi and two stream ciphers SNOW 3G and ZUC. These cipher suites are also used into the 4G-LTE standard. But Kasumi is replaced by AES in 4G-LTE [2]. AES represents the current recommended standard by NIST for encryptions.

Wireless 4G LTE network uses 128-bit Advanced Encryption Standard (AES) and SNOW3G algorithms for integrity protection. The 128-bit AES algorithm is the most preferred option in the Wireless 4G LTE network because it has undergone closed observation than other encryption algorithms [4]. EEA2 or EIA2 is used in LTE-SAE security. They are based on the Advanced Encryption Standard [7]. The 168-bit Digital Encryption Standard or the newer Advanced Encryption Standard is used in WiMAX standards because it specifies that, over-the-air transmissions should be encrypted [9]. Many researchers have taken interest in the field of combining other encryption algorithms with AES. So, it can be considered as a motivational factor for further enhancement of AES.

To enhance secure data transmission in 3G/4G, Transport Layer Security (TLS) is used here. Within TLS Advanced Encryption Standard (AES) is used for encryption. The goal of this work is to develop advanced encryption method using enhanced AES algorithm. The whole cryptographic system has been developed. This includes encryption of data, key exchange and message authentication. RSA is used for key exchange and SHA-256 for message authentication.

Then AES is used in Round structure for proposed system. The proposed algorithm generates dynamic S-box to enhance AES algorithm. In Round structured AES, S-box changes in every round. So, S-box is generated ten times for each block of data. The cipher key is used to convert static S-box into dynamic. The inverse S-box is also changes according to the S-box.

Analysis of algorithm is done on the basis of various parameters. The parameters are encryption time, throughput, avalanche effect, CPU usage, and memory consumed.

A. *Transport Layer Security*

TLS is a protocol created to provide authentication, confidentiality and data integrity between two communicating applications. TLS is an IETF (Internet Engineering Task Force) standard for communicating e-mail securely. Many web browsers and server applications rely on secure SSL and TLS communications. SSL and TLS are frameworks that include cryptographic protocols which are intended to provide secure communications on the Internet.

B. *Advance Encryption Standard*

The Advanced Encryption Standard, an algorithm acts on 128-bit blocks and can use a key of 128, 192 or 256 bits in length. For encryption, each round consists of the four steps: Substitute bytes, Shift rows, Mix columns, and Add round key. For decryption, each round consists of the steps: Inverse sub bytes, inverse shift rows, inverse mix columns and Add round key.

C. *AES S-box*

The Rijndael S-box is a matrix used in the Advanced Encryption Standard (AES) cryptographic algorithm. which is a substitution box and acts as a lookup table. The S-box is generated by determining the multiplicative inverse for a given number in GF (2^8).

D. *Binary Phase Shift Keying*

Phase-shift keying is a digital modulation scheme that modulates the phase of a reference signal and BPSK is the simplest form of phase shift keying (PSK). It uses two phases which are separated by 180°.

E. *Adaptive White Gaussian Noise*

AWGN is an Additive White Gaussian Noise and it implements AWGN channel. AWGN adds Gaussian noise to its input signal.

II. RELATED WORK

In September 2008,in the paper[15] S-box is made key dependent without changing its value and without changing the inverse S-box. The algorithm ensures that no trapdoor was present in the cipher and expands the keyspace to slow down attacks. In 2008, the paper[18] reviewed possible attacks on AES algorithm. The hybrid structure of AES-DES was proposed to overcome the weaknesses of AES algorithm. This paper presented the design and implementation of a symmetrical hybrid based 128 bit key AES-DES algorithm as a security enhancement for live motion image transmission. Feistel structure of AES and DES is used for the same. Razi Hosseinkhani and H. Haj Seyyed Javadi generate Dynamic S-Box using cipher key in AES Cipher System in 2012. They change static S-box into dynamic to increase the cryptographic strength of AES cipher system. In their paper [14] they described the process of generating S-Box dynamically from cipher key and finally analyze the results and experiments. In the paper [21], Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman made AES S-box key dependent to make AES stronger. Here, only the S-box is made key-dependent without changing the value. The cryptanalysis with algebraic attack is the future work of their paper.

In proposed system, we are increasing complexity of AES algorithm by using Round structure as well as enhancing AES algorithm by making S-box and inverse S-box dynamic.

III. PROPOSED SYSTEM

To overcome drawbacks of other 3G/4G cipher algorithms, AES cipher algorithm is used in the proposed system because AES is the most secure algorithm. The S-box and inverse S-box of AES algorithm is improved by making it dynamic. The traditional AES algorithm uses 128 bit input data. There are certain attacks on the AES algorithm like linear, algebraic attacks and the solution is to increase the complexity. Hence to increase the complexity, AES is used in Round structure which uses 256 bits input data.

This work is focused on enhancement of encryption algorithm. The whole cryptographic system has been developed in this work. This includes encryption of data, key exchange and message authentication. RSA is used for key exchange and SHA-256 for message authentication. To create a 4G scenario, channel is used. The data is modulated using BPSK modulator then noise is added by AWGN. After adding noise BPSK demodulator is used for demodulation.

The performance evaluation is done based on parameters: Throughput, Encryption and Decryption Time.

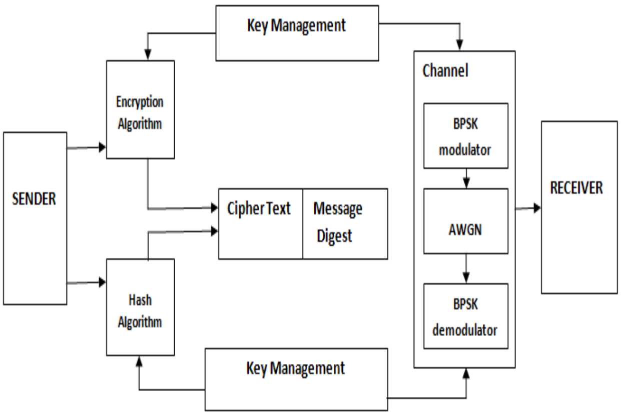

Fig.1. Proposed system

A. *Model development*

256 bits key length and 256 bits input data is given to the enhanced AES system. The proposed system's encryption and decryption is the same as traditional AES algorithm. The round function of encryption process is also similar as the traditional AES algorithm. The 256 bits key is divided into two parts 128 bits each. First part of 128 bits is given to the round structure and second part of 128 bits is given to the AES algorithm. The various models for developing enhanced system are as follows:

1) *Dynamic S-box Generation*

Algorithm	**Bits in one block**	**Total no of bits**	**encryption time**	**decryption time**
AES	128	656	0.008353	0.002977
AES with dynamic S-box	128	656	0.008489	0.003302
Round structured AES with dynamic S-box	256	656	0.009198	0.016122

- There is additional phase of making S-box dynamic as shown in Fig. 2.
- The hexadecimal digits of AES key are XORed with each other and obtained number is used as the shift value to the S-box.
- The S-box is rotated by that shift value.
- Before sub byte stage, the static S-box is converted into dynamic using cipher key.
- The inverse S-box is also modified after S-box to obtain correct inverse values.

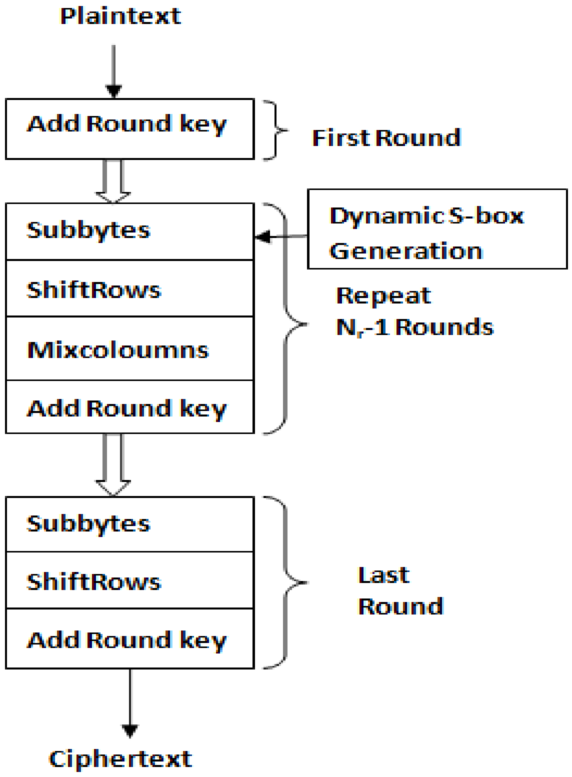

Fig2.. AES dynamic S-box

2) *Round AES with Dynamic S-box Generation*

- The Round structure of AES is used as shown in Fig. 3. Here the Input Data is split into two blocks of 128 bits each.
- One Block is given as Input to the AES section of the System. The other Block is given as Input to the AES section of the System in the next round as per the Round structure.
- This is done for all ten rounds respectively. These outputs are then combined together to form 256 bit block of encrypted data.
- Dynamic S-box is applied to the Round structure of AES as shown in Fig. 3.
- In the round structure, ten times AES is applied to the block of data hence total ten times different S-box is created hence it is called dynamic S-box.

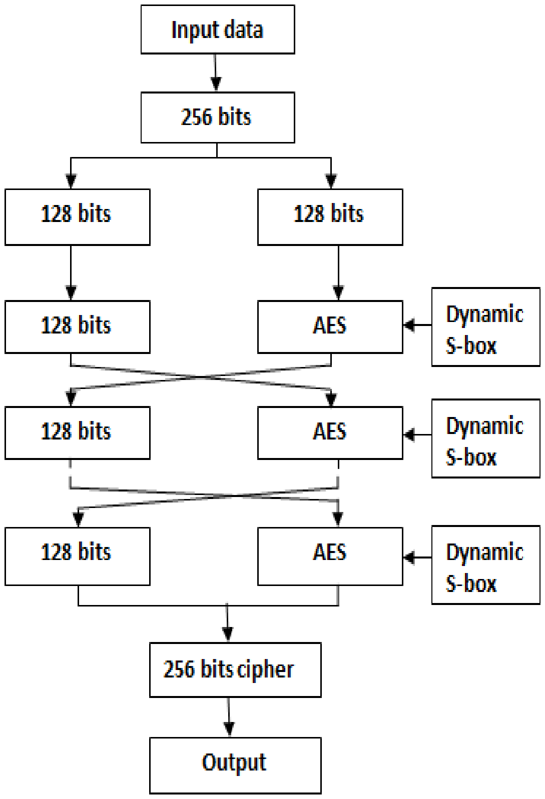

Fig. 3. Round AES with Dynamic S-box

IV. EXPERIMENTAL RESULTS

The results carried out till the date is based on encryption time and throughput.

A. *Encryption time on input text file, image, audio and video file*

Time taken to encrypt same amount of data in one round of Round AES network will be much lesser than AES. If we use two rounds of Round structure, we can get more complexity than AES-CBC with same encryption time.

Computer Configurations used are Microsoft Windows 7, Intel i5 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a.

For text file, "plaintext.txt" of 82 bytes, the number of bits is 656 and key is "feistel aes key enhanced aes key".

The results are tabulated as shown below.

TABLE I. BASED ON ENCRYPTION TIME ON TEXT FILE

Algorithm	Bits in one block	Total no of bits	encryption time	decryption time
AES	128	656	0.008353	0.002977
AES with dynamic S-box	128	656	0.008489	0.003302
Round structured AES with dynamic S-box	256	656	0.009198	0.016122

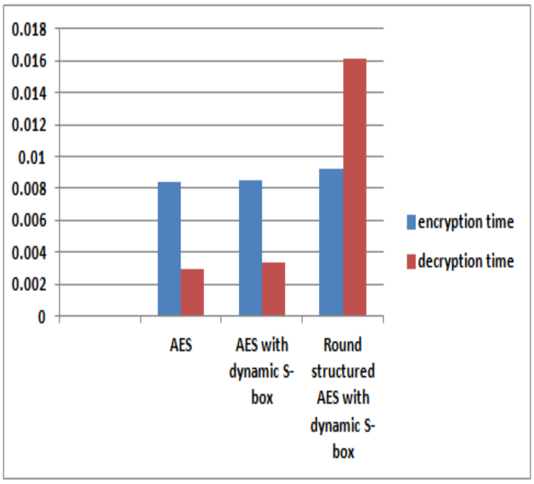

Fig. 4. Graphical representation of results based on encryption time on input text file

For Image file, “smiley.jpg” of 2.35 KB, the number of bits is 19328 and key is “feistel aes key enhanced aes key”.

TABLE II. BASED ON ENCRYPTION TIME ON IMAGE FILE

Algorithm	Bits in one block	Total no of bits	encryption time	decryption time
AES	128	19328	0.211753	0.195217
AES with dynamic S-box	128	19328	0.223669	0.195904
Round structured AES with dynamic S-box	256	19328	1.327422	1.338974

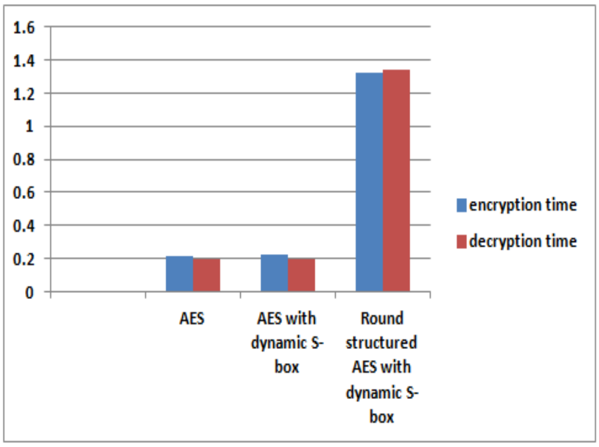

Fig. 5. Graphical representation of results based on encryption time on image file

For Audio file, “Laser.wav” of 3.54 KB, the number of bits is 29040 and key is “feistel aes key enhanced aes key”.

TABLE III. BASED ON ENCRYPTION TIME ON AUDIO FILE

Algorithm	Bits in one block	Total no of bits	encryption time	decryption time
AES	128	29040	0.02392	0.018441
AES with dynamic S-box	128	29040	0.025291	0.020151
Round structured AES with dynamic S-box	256	29040	0.091021	0.095382

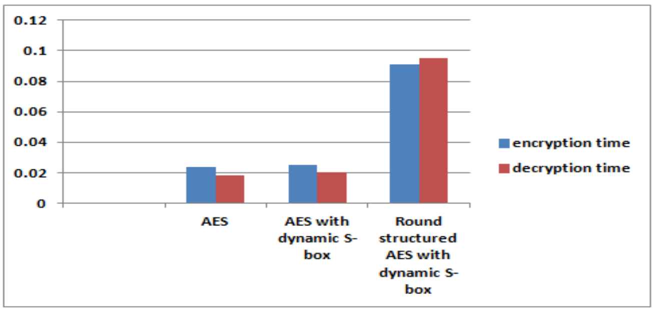

Fig. 6. Graphical representation of results based on encryption time on audio file

For Video file, “composite.avi” of 384 KB, the number of bits is 393728 and key is “feistel aes key enhanced aes key”.

TABLE IV. BASED ON ENCRYPTION TIME ON VIDEO FILE

Algorithm	Bits in one block	Total no of bits	encryption time	decryption time
AES	128	393728	17.61908	17.73196
AES with dynamic S-box	128	393728	17.58008	17.95355
Round structured AES with dynamic S-box	256	393728	17.70852	17.6768

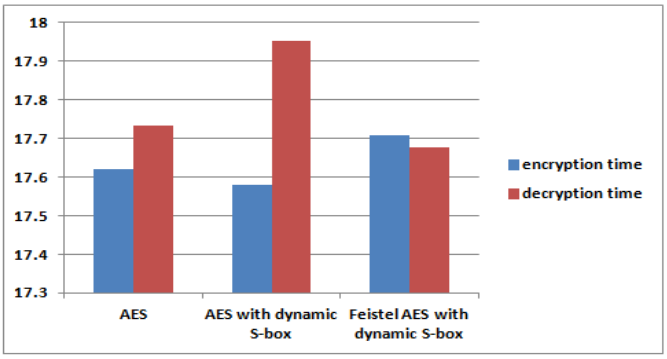

Fig. 7. Graphical representation of results based on encryption time on video file

B. Throughput on input text file, image, audio and video file.

An encryption algorithm is required which can cope up with the speed because 3G and 4G networks works on high data rate.

Computer Configurations used are Microsoft Windows 7, Intel i5 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a.

For text file, “plaintext.txt” of 82 bytes, the number of bits is 656 and key is “feistel aes key enhanced aes key”.

TABLE I. BASED ON THROUGHPUT ON INPUT TEXT FILE

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	656	78.534	220.356
AES with dynamic S-box	128	656	77.276	198.667
Round structured AES with dynamic S-box	256	656	71.319	40.689

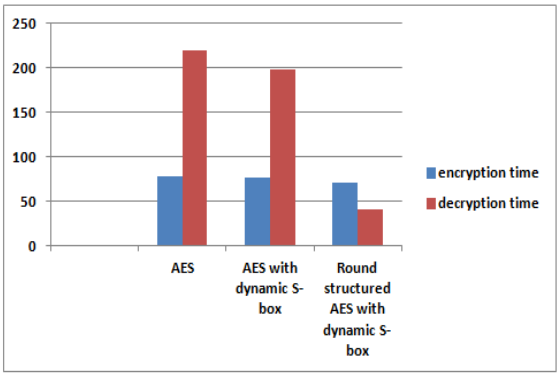

Fig. 8. Graphical representation of results based on encryption timeThroughput on input text file

For Image file, “smiley.jpg” of 2.35 KB, the number of bits is 19328 and key is “feistel aes key enhanced aes key”.

TABLE II. BASED ON THROUGHPUT ON IMAGE FILE

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	19328	91.276	99.007
AES with dynamic S-box	128	19328	86.413	98.66
Round structured AES with dynamic S-box	256	19328	14.56	14.434

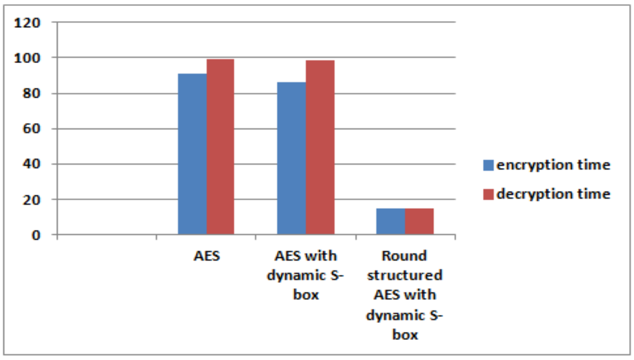

Fig. 9.Graphical representation of results based on encryption timeThroughput on image file

For Audio file, “Laser.wav” of 3.54 KB, the number of bits is 29040 and key is “feistel aes key enhanced aes key”.

TABLE III. BASED ON THROUGHPUT ON AUDIO FILE

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	29040	1214.046	1574.751
AES with dynamic S-box	128	29040	1148.234	1441.119
Round structured AES with dynamic S-box	256	29040	319.047	304.459

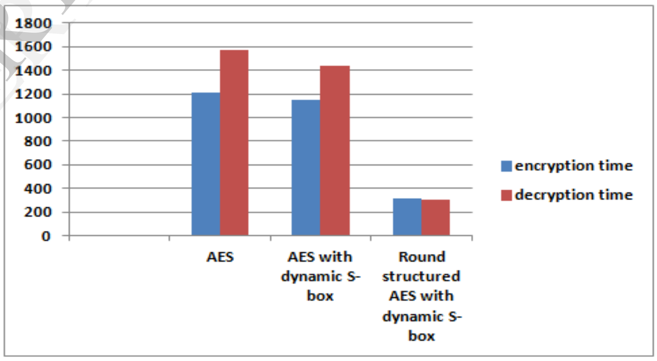

Fig. 10.Graphical representation of results based on encryption timeThroughput on audio file

For Video file, “composite.avi” of 384 KB, the number of bits is 393728 and key is “feistel aes key enhanced aes key”.

TABLE IV. BASED ON THROUGHPUT ON VIDEO FILE

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	393728	22.346	22.204
AES with dynamic S-box	128	393728	22.396	21.93
Round structured AES with dynamic S-box	256	393728	22.233	22.273

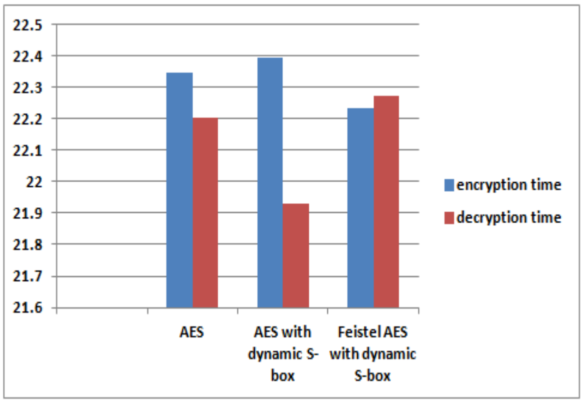

Fig. 11.Graphical representation of results based on encryption timeThroughput on video file

V. CONCLUSION

4G networks have end-to-end security issue hence a solution has to be proposed for the same using SSL/TLS. SSL/TLS SSH, VPN, or a similar mechanism should be provided for security of data. Hence TLS is used here with AES as an encryption algorithm for security. To increase the complexity of system, an AES Round structure is used. Increasing complexity will make the system attack resistant and secure data from attackers. AES is enhanced by converting static S-box into dynamic using cipher key to make cryptography more strong. Hence we have concluded from the results that, when number of bits is increased, the encryption time is increased and throughput is decreased as shown in the tables. Though encryption and decryption time is increased, the complexity of network is increased with the number of bits in one block. So this system can be used in the application where time is not the constraint. 3G and 4G requires high data transmission rate in order to send image and the proposed algorithm encrypts the data in acceptable time.

We also hope to work on reducing attacks on TLS like Renegotiation attack, Version rollback attack, Truncation attack etc. and this will be the future scope of the work.

REFERENCES

[1] Qing Xiuhua, Cheng Chuanhui, Wang Li, "A Study of Some Key Technologies of 4G System*", Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference.

[2] Xinxin Fan, Gaung Gong, "Specification of the stream cipher WG-16 based confidentiality and integrity algorithm", http://cacr.uwaterloo.ca/techreports/2013/cacr2013-06.pdf

[3] Sasan Adibi, Amin Mobasher, Mostafa Tofighbakhsh, Fourth-Generation Wireless Networks: Applications and Innovations, IGI Global, December 31, 2009

[4] The Verizon Wireless 4G LTE Network: Transforming Business with Next-Generation Technology, Verizon Wireless,

http://business.verizonwireless.com/content /dam/b2b/resources/LTE_FutureMobileTech_WP.pdf

[5] Yu Zheng, Dake He, Xiaohu Tang and Hongxia Wang, "AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform", ICICS 2005

[6] Anirudh Ramaswamy Ganesh, Naveen Manikandan P, Sethu S Pl, Sundararajan R, Pargunarajan K.," An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity based Wireless Sensor networks", IEEE conference on Recent Trends in Information Technology (ICRTIT), 2011

[7] Anastasios N. Bikos, Nicolas Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks", IEEE Security & Privacy, 2013

[8] Ghada Zaibi, Abdennaceur Kachouri, Fabrice Peyrard, Daniele Fournier-Prunaret, "On Dynamic chaotic S-BOX", IEEE 2009

[9] Mobile 4G: The Revolution Is Here Now., http://m2m.sprint.com/media/78386/4g_the_revolution_is_now.pdf

[10] Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae, Raphael Phan, "Providing Security in 4G Systems: Unveiling the Challenges", IEEE 2010

[11] N. Seddigh, B. Nandy, R. Makkar, J.F. Beaumont, "Security Advances and Challenges in 4G Wireless Networks", IEEE 2010

[12] Yu Zheng, Dake He, Weichi Yu and Xiaohu Tang,"Trusted Computing-Based Security Architecture For 4G Mobile Networks", IEEE 2005

[13] Saif Al-alak, Zuriati Ahmed, Azizol Abdullah and Shamala Subramiam "AES and ECC Mixed for ZigBee Wireless Sensor Security", World Academy of Science, Engineering and Technology 2011

[14] Razi Hosseinkhani, H. Haj Seyyed Javadi, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (1) : 2012

[15] Krishnamurthy G N, V Ramaswamy," Making AES Stronger: AES with Key Dependent S-Box", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008

[16] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS, "Key-Dependent S-Box Generation in AES Block Cipher System", INFORMATICA, 2009, Vol. 20, No. 1, 23–34, 2009

[17] Shirbhate D.D. , Kale A.R., "Providing Security Challenges In 4g Systems", Bioinfo Security Informatics Volume 2, Issue 1, 2012

[18] M.B. Vishnu, S.K. Tiong, M. Zaini, S.P. Koh, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", APCC 2008

[19] M.Kaleem Iqbal, M.Bilal Iqbal, Iftikhar Rasheed, Abdullah Sandhu, "4G Evolution and Multiplexing Techniques with solution to implementation challenges", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012

[20] Shabaan Sahmoud, Wisam Elmasry and Shadi Abdulfa, "Enhancement the security of AES against modern attacks by using variable key block cipher", International Arab Journel of e-technology, Vol 3,No. 1, January 2013

[21] Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman, "A Proposal for Improving AES S-box with Rotation and Key-dependent", Cyber Warfare and Digital Forensic (CyberSec) international conference, 2012

[22] What are 1G, 2G, 3G and 4G networks ?

http://www.speedguide.net/faq_in_q.php?qid=365

[23] Manuel Mogollon, Cryptography and Security Services: Mechanisms and applications, IGI Global, January 31, 2008

[24] Jivesh Govil, Jivika Govil "4G : Functionalities Development And An Analysis Of Mobile Wireless Grid" First International Conference on Emerging Trends in Engineering and Technology, ICETET.2008 IEEE 2008