Design of F8 Encryption Algorithm Based on Customized Kasumi Block Cipher

Nabil H. Shaker, Hanady H. Issa, Khaled A. Shehata, and Somaia N. Hashem

***Abstract*—Governmental bodies, such as military and national security agencies, keep looking for proprietary encryption algorithms to secure their confidential communication applications. Customizing published encryption algorithms is a trend to acquire proprietary encryption algorithms at affordable research and development cost. Cost, here, may be represented by the required efforts for designing and testing the customized algorithm. The security architecture of the 3rd Generation Partnership Project (3GPP) mobile communications includes a standardized encryption algorithm F8 which is based on the KASUMI block cipher algorithm. In this paper we propose a newly customized version of the KASUMI block cipher. The customization is targeting the S-boxes of KASUMI. New S-Boxes are generated and tested to verify the required cryptographic features.**

***Index Terms*—KASUMI block cipher algorithm, 3GPP, strict avalanche criterion, UMTS.**

I. Introduction

In the last decade there has been an exponential rise in the use of mobile services. The Universal Mobile Telecomm-unications System (UMTS) is the most popular 3G mobile communication systems, which introducing high quality services while retaining the essential and robust security features of the preceding systems [1]. Security is a vital requirement in today's mobile communication services. F8 encryption algorithm is introduced for 3G security to encrypt the user's and signaling data sent over the radio link to provide secrecy. F8 is implemented in both the handset and the radio network controller. F8 is a symmetric synchronous stream cipher used for ciphering frames with different lengths. The keystream generator used in F8 is based on the block cipher KASUMI that is specified in [2]-[3]. KASUMI is used in a form of output-feedback (OFB) mode and generates the output keystream in multiples of 64-bits chunks.

In this paper we present a customized version of KASUMI block cipher to suit proprietary data encryption applications for governmental and national security agencies. The structure of the proposed paper is as follows: Section II presents the F8 algorithm. Section III introduces the customized KASUMI block cipher. The evaluation of the new S-boxes in the customized KASUMI is presented in Section IV. Simulation results of the new S-boxes evaluation are presented in Section V. Finally, Section VI addresses the final conclusions.

II. F8 Encryption Algorithm

The F8 algorithm is based on the KASUMI block cipher and specified by 3GPP to be used in 3G mobile systems as the core algorithm for secrecy and integrity tools [4]-[5]. F8 is a symmetric synchronous stream cipher encryption algorithm which is applied to achieve user's and signaling data over the radio link. Consequently, any sensitive information such as telephone numbers; user data, voice calls and other user-generated data over the radio path is protected. The primary input to the F8 is a 128-bit secret Cipher Key (CK). A 5-bit identity BEARER input, a 32-bit frame dependent COUNT input and a 1-bit input transmission DIRECTION is used to apply uniqueness to input frames. The output of F8 algorithm is a stream of bits (key stream) having a length equal to the frame length. Finally the plain data (frame) is Xored with the generated keystream for encryption as shown in Fig. 1.

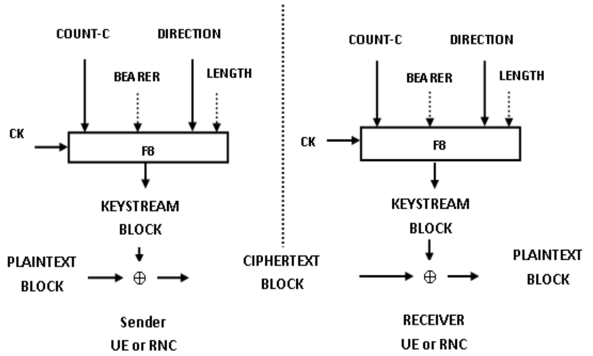

Fig. 1. Ciphering of user and signaling data using F8 algorithm.

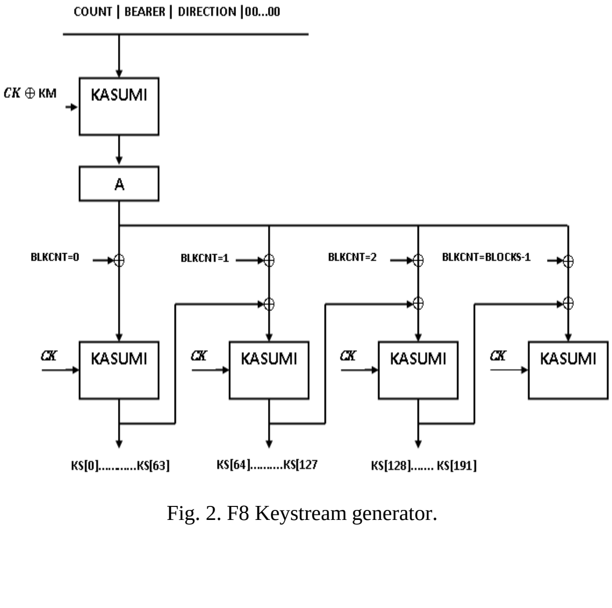

Fig. 2. F8 Keystream generator.

Manuscript received December 18, 2012; revised April 16, 2013.

N. H. Shaker is with the Electronics and Communication Department, MIU, Cairo, Egypt (e-mail: nabil.hamdy@miuegypt.edu.eg).

H. H. Issa, K. A. Shehat, and S. N. Hashem are with the Electronics and Communication Department, AAST, Cairo, Egypt (e-mail: hanady.hussien@ieee.org, k_shehata@aast.edu, somaia_nh@yahoo.com).

DOI: 10.7763/IJCCE.2013.V2.213

Fig. 2 represents the structural description of F8 algorithm [3]. It uses KASUMI block cipher as a keystream generator in a form of output-feedback mode (OFB). It generates key stream in form of multiple 64-bit blocks. The feedback data are modified by a static data held in a 64-bit register A and an incrementing 64-bit counter BLKCNT. KASUMI has a Feistel structure which comprises eight rounds [2]. Eight is not a random number since with the analysis it might be possible to find some attacks to 6 rounds, but not to the full 8-round KASUMI [6]. KASUMI operates on 64-bit data blocks and its processing is controlled by a 128-bit encryption key that derives the sub-keys KL, KO and KI for all rounds [2].

Fig. 3 shows the eight rounds of KASUMI, each round comprises two components FL and FO.

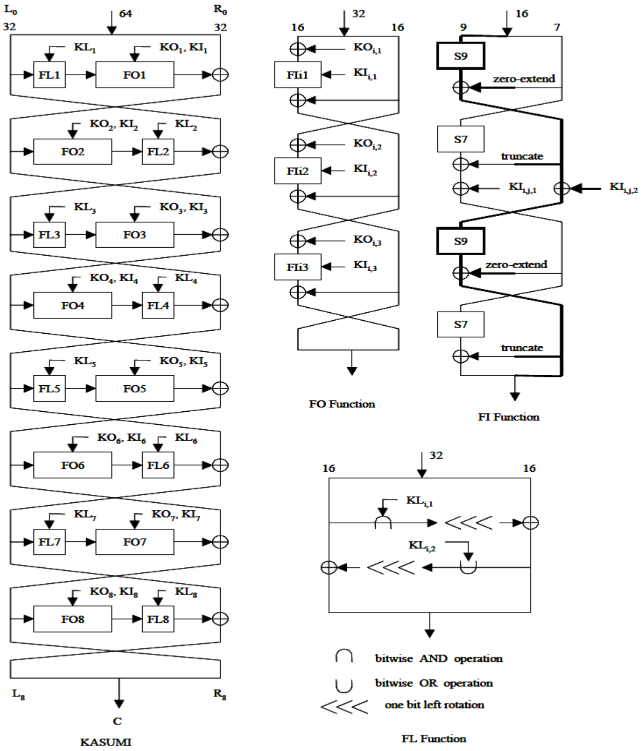

Fig. 3. KASUMI block cipher.

In odd rounds FL function is applied before FO, while in even rounds FO and FL are interchanged. The FL component is a linear function with simple and fast operations. Therefore the security of KASUMI and thus of F8 does not depend on this function. The main purpose of FL function is a low cost scrambler that makes tracking of individual bits through rounds harder. FL is applied on 32-bit data using subkeys KL. The FO function is a 32-bit non-linear mixing function. FO is an iterated "ladder-design" consisting of 3 rounds of a 16-bit non-linear mixing function FL. FO function satisfies the "Avalanche criteria", where, every output bit depends on all input bits, thus changing a single input bit makes major changes in the output. The FL Component consists of 4-round unbalanced Fiestel structure using non-linear look-up tables S7 and S9 (S-Boxes in KASUMI). FI is the basic randomizing function of KASUMI with 16 bits input and 16 bits output and satisfies the "Avalanche criteria" [6].

S-Boxes S7 and S9 had been designed in such a way to avoid the linear structures in FI. Contents of S7 and S9 are permutations of integer numbers, S7 is a 128-element permutation from 0 to 127, and S9 is a 512-element permutation from 0 to 511, listings of the standard S7 and S9 are shown in [2].

III. Customized KASUMI Block Cipher

The main difference between the customized KASUMI and the standard one is the used S-boxes. The idea beyond customizing the KASUMI block cipher is to generate new S-boxes for Fl. If the new S-boxes are kept secret, then the customized KASUMI has a new additional security dimension beside the used secret keys. This customization of KASUMI can be easily implemented by any governmental agency.

Substitution is a nonlinear cryptographic transformation which performs confusion and diffusion of bits. Nonlinear transformations are essential for every modern encryption algorithm and are proved to be strong cryptographic primitives against linear and differential cryptanalysis [7]. Generation of S-boxes can be achieved using one of four different methods. These methods are: random, random with testing, human-made, and math-made methods [8].

To keep the same security structure of the KASUMI algorithm, the new S-boxes have to be generated with the same features of the standard ones i.e. the S7-box contains a new 128-element permutation and S9-box contains a new 512-element permutation. Consequently, a random permutation generator is implemented and executed to create the new S-boxes. However, these S-boxes are randomly generated, in the following section, testing procedures are applied to evaluate their performance. Apparently, the random method with testing has been adopted in this paper to generate new S-boxes.

IV. Evaluation of the New S-Boxes

In [9]-[10] there are three addressed methods to verify the Strict Avalanche Criterion (SAC) as a tool for evaluating the strength of S-boxes. SAC can be evaluated analytically by three different graphical methods [9]-[10]:

1) Analysis of the frequency of various Hamming weights (Avalanche criteria).
2) Analysis of the frequency of various differential values ΔY (completeness);
3) Analysis of the Hamming weights according to the bit position (Strong S-box).

A. Analysis of the Frequency of Occurrence of Various Hamming Weights (Avalanche Criterion)

This analysis studies the avalanche criterion demonstrated in the outputs of the S-box. The output of S-box exhibits an Avalanche criteria if an average of one half of the output bits will be changed whenever a single input bit is complemented [9]. In this test the frequency of occurrence of various Hamming weights is analyzed in the S-box with length m, where m is the number of bits in the output of the S-box. The avalanche criteria test is performed in the following steps

Step 1: Choose a random number *x* in the range of S-box addresses, then find the corresponding output value of S-box

y where $y = s(x)$.

Step2: Choose another random number x', in the same range of x, then find the corresponding output value of S-box; y', where $y' = s(x')$.

Step 3: Compute the differential output Δy where $\Delta y = y \oplus y'$; where $\oplus$ is the bit-per-bit XOR function.

Step 4: Find the Hamming weight w of Δy where, Hamming weight of a binary string is defined as the number of ones in this string. Computing the Hamming weight of Δy is equivalent to computing the Hamming distance between y and y'.

Step 5: Repeat from step1 to step4 for ‘’*n*’’ trials of testing.

Step 6: Analyze the frequency of occurrence of various Δy.

If the frequencies of occurrence of various Hamming weights follow the Gaussian distribution, this means the S-box has good property of strict avalanche criterion [9].

B. Analysis of the Differential Values (Completeness)

This analysis finds out the dependency of output bits of the S-box on the input bits to the S-box. Thus, if each output bit of the S-box is dependent on all input bits of S-box this means that the corresponding S-box satisfies the completeness analysis [9]. The input to the completeness analysis is the S-box with length m, where m is the number of the output bits, while the output is the frequency of various differential Δy which is computed in previous test.

The completeness test is executed by performing the first five steps of IV.1, in step 6, the frequencies of different values of Δy are counted. If they are almost the same this means the S-box satisfies the completeness properties [9].

C. Analysis of Hamming Weight According to Bit Position (Strong S-box)

This analysis measures the strength of S-boxes. It considers the S-box as a strong one if the frequency of Hamming weight of the binary representation of Δy - according to the bit position- is constant [9]-[10]. In this test the differential outputs Δy’s are computed as in the first test, then the binary representations of all Δy are listed. The Hamming weights are calculated by summing the ones in each column of the binary representations of all Δy. If the Hamming weights of all columns are constant this indicates that the S-box is a strong one [9].

To verify that the newly generated S-boxes satisfy the SAC criteria, we chose to run SAC tests for 1536 and 2048 trials on S9-box, and 384 and 512 trials on S7-box, these numbers of trials are chosen to make sure that each output value will appear 3 times in average to give good statistics for these tests.

V. Simulation Results of the SAC Tests

A. Analysis of the Frequency of Occurrence of Various Hamming Weights (Avalanche Criterion)

The generated S7 and S9 boxes are subjected to this analysis for different counts of testing *n*. The simulation results show a Gaussian distribution as shown in Fig. 4. a, b, c, and d respectively. Consequently, the S-boxes satisfy the requirement of test-1 and show good properties of strict avalanche criterion [9]. Moreover the standard S-boxes are subjected to the same test for comparison .The simulation results are shown in Fig.s 4.e and 4.f respectively.

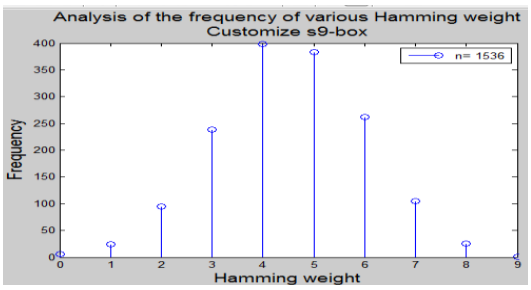

Fig. 4. a Matlab simulation result of the frequency of various hamming weights for new S9-box of *n*=1536.

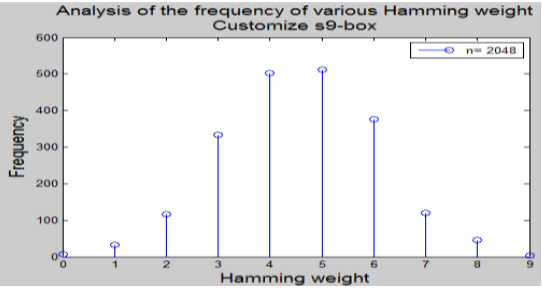

Fig. 4. b Matlab simulation result of the frequency of various hamming weights of new S9-box for *n*=2048.

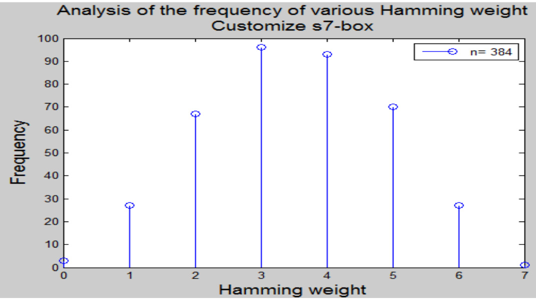

Fig. 4. c Matlab simulation result of the frequency of various hamming weights of new S7-box for *n*=384.

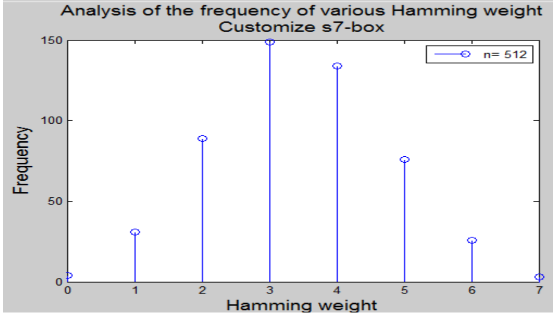

Fig. 4. d Matlab simulation result of the frequency of various hamming weights of new S7-box for *n*=512.

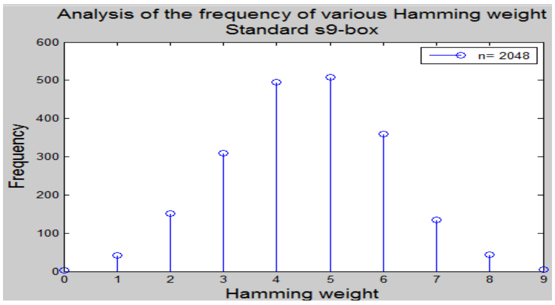

Fig. 4. e Matlab simulation result of the frequency of various hamming weights of standard S9-box for *n*=2048.

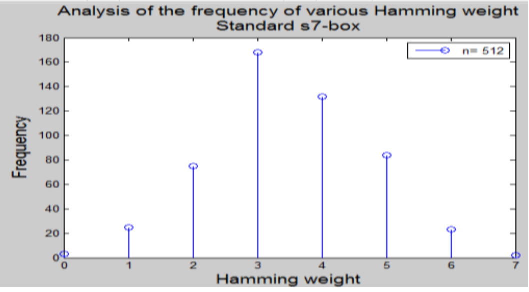

Fig. 4. f Matlab simulation result of the frequency of various hamming weights of standard S7-box for *n*=512.

B. Analysis of Differential Values (Completeness)

The analysis is applied to the standard and new S-boxes. Fig. 5. a, b, c and d show samples of these results. To analyze these results, the mean and standard deviation of the simulation results are calculated and compared with those of the standard S-box. For S7-boxes, the mean values of the standard and new S7-box equal 4 for *n* = 512 and the standard deviations equal to 1.97 and 1.81 respectively for the same value of *n*. For S9-boxes, the mean values of the standard and generated S9-boxes are the same and equal to 4 when *n* = 2048, while the standard deviations are equal to 2 and 1.99 respectively. These results show that the mean and standard deviation of the generated S-boxes are very close to the values given by standard S-boxes. As a conclusion, the generated S-boxes satisfy this criterion.

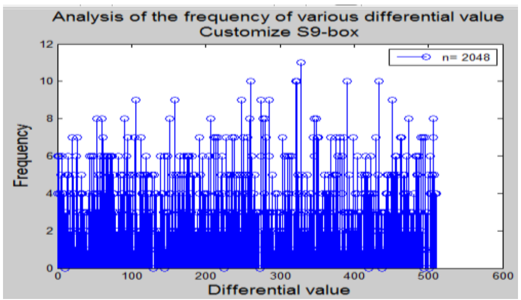

Fig. 5. a Testing result of completeness test for generated S9-box when *n*=2048.

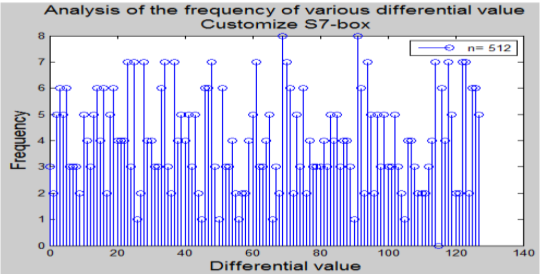

Fig. 5. b Testing result of completeness test for generated S7-box when *n*=512.

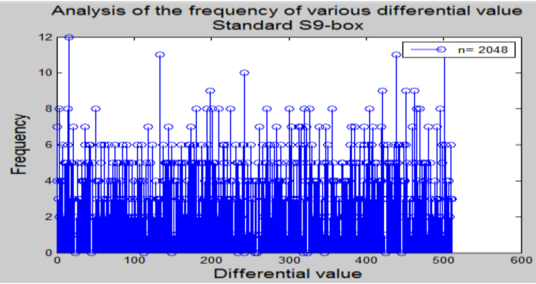

Fig. 5. c Testing result of completeness test for standard S9-box when *n*=2048.

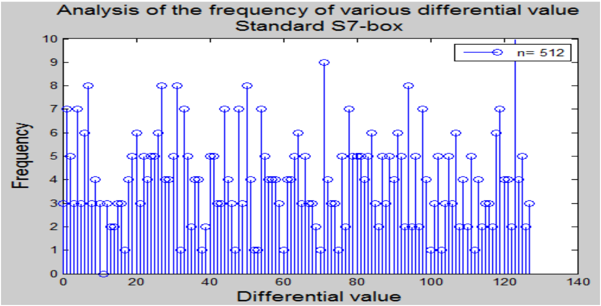

Fig. 5. d Testing result of completeness test for standard S7-box when n=512.

C. Analysis of Hamming Weight According to Bit Position (Strong S-box)

Testing the frequency of various Hamming weights according to bit position is performed on the standard and new S-boxes for different n. Samples of these results are shown in Fig.s 6.a, 6.b, and 6.c when n = 2048 and 512. All these simulation results for different n show that the Hamming weights for all Δy according to bit position are almost constant. As a conclusion, the generated S-boxes satisfy this criterion.

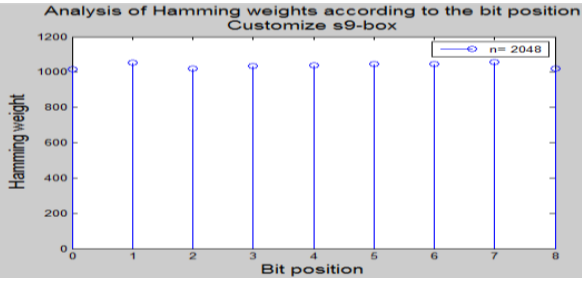

Fig. 6. a Simulation result of strong S-box test for generated S9-box when *n*=2048.

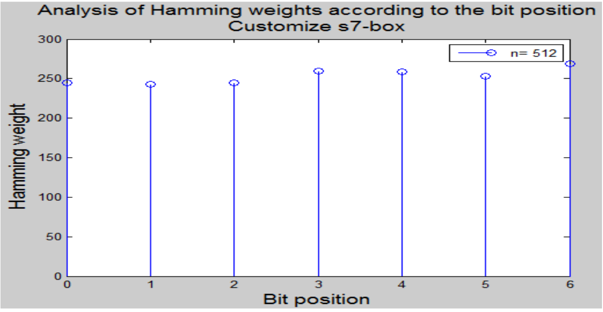

Fig. 6. b Simulation result of strong S-box test for generated S7-box when *n*=512.

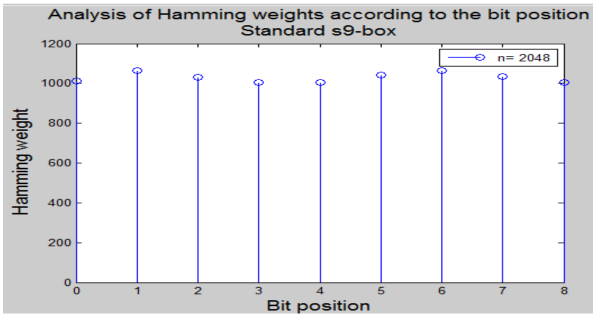

Fig. 6. c Simulation result of strong S-box test for stantard S9-box when *n*=2048.

VI. Conclusion

This paper introduces design of a new version of F8 algorithm based on customized KASUMI block cipher. The objective of this new version is to serve the needs of governmental bodies who are looking for proprietary encryption algorithms to secure their confidential applications. The customization process depends on generating new S-boxes that are used in FI function in the standard KASUMI algorithm. The new S-boxes are generated using the random with testing generation technique. Evaluation of the new S-boxes are carried out to insure that the new S-boxes contents satisfy the strict avalanche criterion SAC. The three methods used to test SAC are performed on both new and standard S-boxes. The new S-boxes have passed these tests for different runs and show a similar performance as standard boxes.

REFERENCES

[1] S. Prakash and S. Behera, "Study and implementation of 3g mobile security," National Institue of Technolog Rourkela, 2010.

[2] *3GPP TS 135.202 Version 7.0.0*, 3rd Generation Partnership Project; Specification of 3GPP confidentiality and integrity algorithms; 3G Security,KASUMI Specification, 2007.

[3] *3GPP TS 135.203 Version 4.0.0*, 3rd Generation Partnership Project; Specification of 3GPP confidentiality and integrity algorithms; 3G Security, implementors' test data, 2002.

[4] *3GPP TS 135.201 Version 7.0.0*, 3rd Generation Partnership Project; Specification of 3GPP confidentiality and integrity algorithms; 3G Security,F8 and f9 Specification, 2007.

[5] *3GPP TS 135.204 Version 6.0.0*, 3rd Generation Partnership Project; Specification of 3GPP confidentiality and integrity algorithms;Design conformance test data, 2004.

[6] E. Vrentzos, G. Kostopoulos, and O. Koufopavlou, "Hardware implementation of the A5/3 & A5/4 GSM encryption algorithms," vol. 3, June 2006.

[7] N. Hamdy, K. Shehata, and H. Eldemerdash, "Design and implementation of encryption unit based on customized AES algorithm," *International Journal of Video and Image Processing and Network Security IJVIPNS-IJENS*, vol. 11 no. 01, pp. 33-40, Feb 2011.

[8] W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th ed. Prentice Hall, 2005, Ch. 3.

[9] P. P. Mar and K. M. Latt, "New analysis methods on strict avalanche criterion of S-Boxes," *World Academy of Science, Engineering and Technology*, vol. 48, pp. 150-154, 2008.

[10] I. Hussain and Z. Mohmood, "Graphical strict avalanche criterion for kasuni sbox," *Canadian Journal on Computing in Mathematics, Natural Sciences, Engineering and Medicine*, vol. 1, no. 5, pp. 132-136, July 2010.

Nabil Hamdy was born in Egypt in 1955. He got the B.Sc. in Communication Engineering at The Military Technical College, Cairo, Egypt in 1978. He got the M.Sc. in Communication Security at Faculty of Engineering, Ain-Shams University, Cairo, Egypt in 1990. (Thesis title: Cryptanalysis of Ciphertext-Feedback Cipher Systems). He got the Ph.D. in Electrical Engineering at the Naval Postgraduate School, Montery, California, USA in 1997. He had served the Egyptian Military for 30 Years in the field of encryption and communication security systems. During the military service he conducted and supervised uncountable number of classified research and development projects for miltary cipher system. Dr. Nabil had retired from the Military in 2007. Since then, he joined the Faculty of engineering at Misr International University (MIU) in Cairo, Egypt as a lecturer in the field of communication systems, encryption, and information security systems.

Hanady H. Issa gartuated 1998, obtained her MSc. Degree 2002 in Electronics and Communication, from Arab Academy for Science and Technology (AAST), Alex., Egypt, then her PhD degree in Electronics and Communication Engineering from Ain Shams University in 2009. She worked as a teacher assistant in Electronics and Communication department in AAST since 1998. Currently she is working as at currently an assistant professor at AAST, Electronics and Communication department, Cairo, Egypt. Here research interests include Digital/Analog design, VHDL based FPGA design, simulation and synthesis.

Khaled Shehata received his BSc from Military Technical College, Cairo, Egypt in 1981. After working as a research assistant he got his MSc. from Cairo University, Egypt in 1991. He received his PhD. from Naval Postgraduate School, Monterey, California, USA in 1996. He worked as a researcher in Egypt, then a Director for the VLSI design center, AOI, Egypt, finally he is a professor in the Arab Academy for Science and Technology, College of Engineering since 2000 till now. His research interests include analog and digital VLSI design, electronic system design and have more than 80 scientific research papers in these areas. He is the Chairman of Electronics and Communication Department.

Somaia Nabil was born in Egypt in 1986. She obtained her MSc. Degree in Electronics and Communication, from Helwan University, Cairo in 2008. She is a master student at Arab Academy for Science (AAST). I prepare my master degree in Electronics and Communication field. Her research interests include cryptography and network security.