RESEARCH ARTICLE OPEN ACCESS

Modifying Authentication Techniques in Mobile Communication Systems

Zakaria Zakaria Hassan, Talaat A. Elgarf, Abdelhalim Zekry
Communication Engineering Department Higher Technological Institute Cairo, Egypt
Communication Engineering Department Higher Technological Institute Cairo, Egypt
Communication Engineering Department Faculty of Engineering Ain shams University Cairo, Egypt

Abstract
Milenage algorithm applies the block cipher Rijnadael (AES) with 128 bit key and 128 bit block size. This algorithm is used in the 3GPP authentication and key generation functions (f1, f1*, f2, f3, f4, f5 and f5*) for mobile communication systems (GSM/UMTS/LTE). In this paper a modification of Milenage algorithm is proposed through a dynamic change of S-box in AES depending on secret key. To get a new secret key for every authentication process we add the random number (RAND) transmitted from the authentication center (AUC) to the contents of the fixed stored secret key (Ki) and thus the initialization of the AES will be different each new authentication process . For every change in secret key a new S-box is derived from the standard one by permuting its rows and columns with the help of a new designed PN sequence generator. A complete simulation of modified Milenage and PN sequence generator is done using Microcontroller (PIC18F452). security analysis is applied using Avalanche test to compare between the original and modified Milenage . Tests proved that the modified algorithm is more secure than the original one due to the dynamic behavior of S-box with every change of the secret key and immunity against linear and differential cryptanalysis using Avalanche tests. This makes the modified Milenage more suitable for the applications of authentication techniques specially for mobile communication systems.

Keywords—Authentication vector (AV), Modified MILENAGE Algorithm for AKA Functions (F_1,F_1*,F_2,F_3,F_4,F_5,F_5*), AES ,Dynamic S-BOX and PN Sequence Generator(LFSR).

I. INTRODUCTION

Authentication includes the authenticity of the subscriber as well as the network. Authentication of mobile subscribers and network operators is a challenge of future researchers due to increasing security threats and attacks with the enhanced volume of wireless traffic. Authentication schemes in mobile communication systems are initiated during IMSI attach, location registration, location update with serving network change, call setup (MOC, MTC), activation of connectionless supplementary services and short message services (SMS).

Milenage algorithm is used for generating authentication and key agreement of cryptographic generating functions (MAC, XRES, CK and IK). The main core of Milenage algorithm is the Advanced Encryption Standard (AES) [1] which launched as a symmetrical cryptographic standard algorithm by the National Institute of Standard and Technology (NIST) in October 2000, after a four year effort to replace the aging DES. The Rijndael proposal for AES defined a cipher in which the key length can be independently specified to be 128 , 192 or 256 bits but the input and output block length is 128 bits.[2],[3].Four different stages are used in AES :Sub Byte transformation, Shift Rows, Mix Columns and Add Round Key. For both encryption and decryption, the cipher begins with an Add Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.[4].

This paper is organized as follows: In Section II, authentication schemes in mobile communications are described. In Section III, a proposed authentication scheme is presented depending on the dynamic change of S-box in AES , the new Secret key for every authentication process and the new PN sequence generator. In Section IV, a complete simulation of the modified Milenage algorithm and the Avalanche test results are introduced. Discussions and Conclusions are presented in Section V.

II. AUTHENTICATION SCHEMES IN MOBILE COMMUNICATIONS.

(i) GSM/GPRS Authentication and Key Agreement vectors .

There exists a permanent, shared secret key Ki for each subscriber. This permanent key is stored in two locations: in the subscriber’s SIM card and in the Authentication Centre (AuC). The key Ki is never moved from either of these two locations. Authentication of the subscriber is done by checking that the subscriber has access to Ki. This can be achieved by challenging the subscriber by sending a random 128-bit string (RAND) to the terminal. The terminal has to respond by computing a one-way function with inputs of RAND and the key Ki, and returning the 32-bit output Signed Response (SRES) to the network. Inside the terminal, the computation of this one-way function, denoted by A3, happens in the SIM card. During the authentication procedure, a temporary session key Kc is generated as an output of another one-way function A8. The input parameters for A8 are the same as for A3: Ki and RAND. The session key Kc is subsequently used to encrypt communication on the radio interface. The serving network does not have direct access to the permanent key Ki, so it cannot perform the authentication alone. Instead, all relevant parameters, so called the authentication triplet (RAND, SRES and Kc) are sent to the serving network element Mobile Switching Centre/Visitor Location Register (MSC/VLR) (or Serving GPRS Support Node (SGSN) in the case of GPRS) from the AuC. [5], [6].

(ii) UMTS/LTE/Advanced LTE Authentication and Key Agreement Vectors.

. UMTS Generation of Authentication vectors (Quintets) in the AUC.

Upon the receipt of the authentication data request from the VLR/SGSN, The HLR/AuC sends an authentication response back to the VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n). The HLR/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND. The authentication vectors are ordered based on sequence number. [5].

There are eight Cryptographic functions used in UMTS/LTE/Advanced LTE Authentication and Key Agreement to generate Authentication vector (AV). f_0 is the random challenge-generating function. It should be a pseudo random number-generating function and map the internal state of the generator to the challenge value RAND , the length of RAND is 128 bits. The f_1 is the network authentication function, f_1* is the re-synchronization message authentication function, it is used to provide data origin authentication for synchronization failure information sent by the USIM to the AuC, f_2 is the user authentication function, f_3 is the cipher key derivation function , f_4 is the integrity key derivation function, f_5 is the anonymity key derivation function for normal operation and f_5* is the anonymity key derivation function for re-synchronization, f_5* is only used to provide user identity confidentiality during resynchronization. K is the subscriber authentication key stored in the USIM and at the AuC, The length of K is 128 bits. [5],[7],[8].

To generate authentication quintuple, the HLR\AUC computes a message authentication code for authentication MAC-A= f_1k (SQN || RAND || AMF), the length of MAC-A is 64bits. an expected response XRES = f_2k (RAND), the length of XRES is 64bits.. a cipher key CK = f_3k (RAND). the length of CK is 128bits . an integrity key IK = f_4k (RAND) the length of IK is 128bits and an anonymity key AK = f_5k (RAND), the length of AK is 48bits that is used to conceale sequence number SQN, the length of SQN is 48bits, SQN= SQN ⊕ AK. the HLR/AuC aggregates the authentication token AUTN = SQN [⊕ AK] || AMF(16bits) || MAC-A, the lengths of AUTN is 128bits that forms the quintet Q =AV= (RAND, XRES, CK, IK, AUTN). [7], [8], [9].

. Authentication and key derivation in the USIM.

Upon receipt of a (RAND, AUTN), the USIM computes the anonymity key AK = f_5k (RAND) and retrieves the unconcealed sequence number SQN = (SQN ⊕AK) ⊕ AK, XMAC-A = f_1k (SQN || RAND|| AMF), the response RES = f_2k (RAND), the cipher key CK = f_3k (RAND) and the integrity key IK = f_4k (RAND) as shown in fig.2. [5], [6]**.**

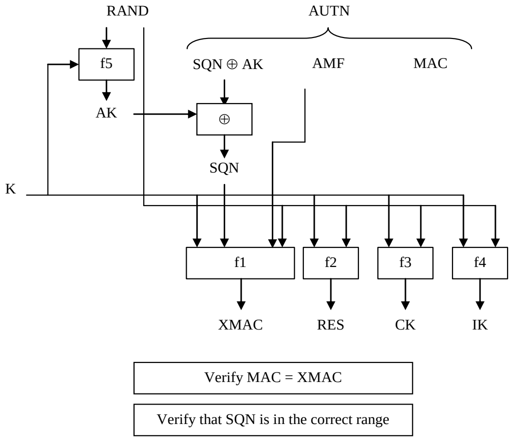
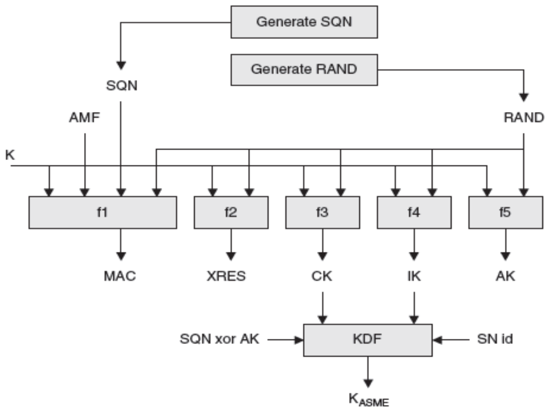


Figure1. Authentication and key derivation in the USIM.[7].

(iii) LTE\AdvancedLTE Generation of Authentication Vectors in the HSS.

The LTE architecture is built on the existing architecture from UMTS. LTE standards reuse the authentication and key-agreement of UMTS. The LTE/Advanced LTE AKA protocol also known as the Evolved Packet System (EPS) AKA protocol. The EPS-AKA protocol is executed between UE and the MME instead of between the USIM and the VLR/SGSN. The AuC generates UMTS AVs for EPS AKA in exactly the same format as for UMTS AKA. The HSS part outside the AuC derives KASME from the CK and IK. EPS AV consists of [RAND, XRES, a local master key KASME and an AUTN] as shown in fig.1. [10], [11], [12].



AUTN = [SQN ⊕ AK || AMF || MAC].
UMTS (AV) = [RAND || XRES || CK || IK || AUTN].
EPS (AV) = [RAND || XRES || KASME|| AUTN].

Figure2. Generation of UMTS and EPS authentication vectors. [6].

III. Proposed Authentication Scheme in Mobile Communication.

A modification of Milenage algorithm is proposed through a dynamic change of S-box in AES depending on the new secret key. To get a new secret key for every authentication process we add the random number (RAND) transmitted from the authentication center (AUC) to the contents of the fixed stored secret key (Ki) and so, the initialization of the AES will be different for each authentication process. For every change in secret key a new S-box is derived from the standard one by permuting its columns and rows with the help of a new designed PN sequence generator. Finally to get a strong Milenage algorithm generating all functions f_1, f_1*, f_2, f_3, f_4, f_5, and f_5* and the outputs of the various functions used in User Authentication, Network Authentication, Data Integrity Check and Ciphering data. The outputs of the various functions are then defined as shown in fig.3.

- Output of f_1 = MAC-A, where MAC-A[0] .. MAC-A[63] = OUT1[0] .. OUT1[63]
- Output of f_1* = MAC-S, where MAC-S[0] .. MAC-S[63] = OUT1[64] .. OUT1[127]
- Output of f_2 = RES, where RES[0] .. RES[63] = OUT2[64] .. OUT2[127]
- Output of f_3 = CK, where CK[0] .. CK[127] = OUT3[0] .. OUT3[127]
- Output of f_4= IK, where IK[0] .. IK[127] = OUT4[0] .. OUT4[127]
- Output of f_5= AK, where AK[0] .. AK[47] = OUT2[0] .. OUT2[47]
- Output of f_5* = AK, where AK[0] .. AK[47] = OUT5[0] .. OUT5[47]

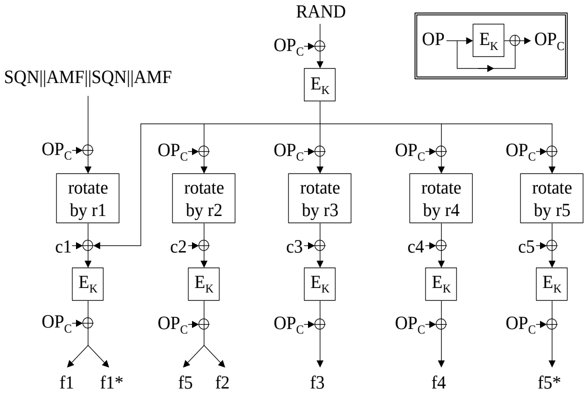


Figure 3. Computation of the MILENAGE functions. [13].

Upgrade of S-box (Dynamic S-box) depends on the new secret key (Key⊕RAND) for every authentication process and the new PN Random sequence generator[14] . The suggested generator consists of three Maximal length Linear Feedback Shift Register (LFSR) with thirty two, seventeen and fifteen taps. The period of this PN sequence= $(2^{32}-1)$ $(2^{17}-1)$ $(2^{15}-1)$ the 1st 128 bits of the PN sequence generator is taken as the secret key to upgrade the s-box. The 1st 64 bits to rearrange the columns and the 2nd 64 bits to rearrange the rows of original S-box. The feedback functions of the LFSRs are: [15].

LFSR 1: $F_1=X^{15}+X^{14}+1$
LFSR 2: $F_2=X^{32}+X^{22}+X^2+X+1$
LFSR 3 : $F_3= X^{17}+X^{14}+1$

To initialize the PN sequence generator as shown fig.4, the new secret key is divided into two vectors of 64 bit length that are XORed to produce the initial state of the PN sequence generator (64bits). Let the fixed stored authentication key Ki = [9E5944 AE A94B8116 5C82FBF9 F32DB751] and the RAND =[CE83DBC54AC0274A157C17F8D017BD6], the new secret key = Ki⊕RAND =[50DA9 F6BE38BA65C49FEEC01FE2CCC87].

The initialization vector of the PN sequence generator (reshaped new secret key) =[50DA9F6BE38BA6 5C]⊕[49FEEC01FE2CCC87] = [1924736A1D A76ADB]. The 1st 64 bits of the PN sequence generator will be [09AE48DBC37F5612] used to rearrange columns of S-box and the 2nd 64 bits of the PN sequence generator will be[B9DE60C327 458F1A] to rearrange the rows of S-box to have the final modified form.

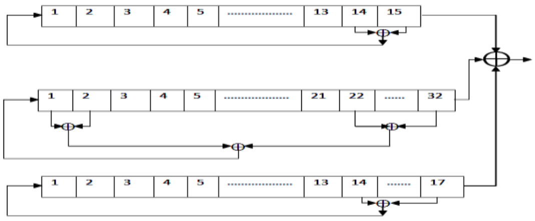


Figure 4. PN random sequence generator.

Table 1. AES standard S-BOX.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 2. For COLUMN Dynamic S-box after arrangement = [09AE48DBC37F5612].

Arr.col.	0	9	A	E	4	8	D	B	C	3	7	F	5	6	1	2
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	01	67	AB	F2	30	D7	2B	FE	7B	C5	76	6B	6F	7C	77
1	CA	D4	A2	72	FA	AD	A4	AF	9C	7D	F0	C0	59	47	82	C9
2	B7	A5	E5	31	36	34	D8	F1	71	26	CC	15	3F	F7	FD	93
3	04	12	80	B2	18	07	27	E2	EB	C3	9A	75	96	05	C7	23
4	09	3B	D6	2F	1B	52	E3	B3	29	1A	A0	84	6E	5A	83	2C
5	53	CB	BE	58	20	6A	4C	39	4A	ED	5B	CF	FC	B1	D1	00
6	D0	F9	02	9F	43	45	3C	7F	50	FB	85	A8	4D	33	EF	AA
7	51	B6	DA	F3	92	BC	FF	21	10	8F	F5	D2	9D	38	A3	40
8	CD	A7	7E	19	5F	C4	5D	3D	64	EC	17	73	97	44	0C	13
9	60	EE	B8	0B	22	46	5E	14	DE	DC	88	DB	2A	90	81	4F
A	E0	D3	AC	E4	49	C2	95	62	91	0A	5C	79	06	24	32	3A
B	E7	56	F4	AE	8D	6C	7A	EA	65	6D	A9	08	D5	4E	C8	37
C	BA	DD	74	8B	1C	E8	BD	1F	4B	2E	C6	8A	A6	B4	78	25
D	70	35	57	1D	48	61	C1	B9	86	66	0E	9E	03	F6	3E	B5
E	E1	1E	87	28	69	9B	55	E9	CE	11	94	DF	D9	8E	F8	98
F	8C	99	2D	BB	BF	41	54	0F	B0	0D	68	16	E6	42	A1	89

Table3. Final S-box ROWs after arrangement =[B9DE60C327458F1A] that used in Modified Milenage Algorithm during the new secret key to generate a new s-box so called [Dynamic Key (S-box)].

Arr.row		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
B	0	E7	56	F4	AE	8D	6C	7A	EA	65	6D	A9	08	D5	4E	C8	37
9	1	60	EE	B8	0B	22	46	5E	14	DE	DC	88	DB	2A	90	81	4F
D	2	70	35	57	1D	48	61	C1	B9	86	66	0E	9E	03	F6	3E	B5
E	3	E1	1E	87	28	69	9B	55	E9	CE	11	94	DF	D9	8E	F8	98
6	4	D0	F9	02	9F	43	45	3C	7F	50	FB	85	A8	4D	33	EF	AA
0	5	63	01	67	AB	F2	30	D7	2B	FE	7B	C5	76	6B	6F	7C	77
C	6	BA	DD	74	8B	1C	E8	BD	1F	4B	2E	C6	8A	A6	B4	78	25
3	7	04	12	80	B2	18	07	27	E2	EB	C3	9A	75	96	05	C7	23
2	8	B7	A5	E5	31	36	34	D8	F1	71	26	CC	15	3F	F7	FD	93
7	9	51	B6	DA	F3	92	BC	FF	21	10	8F	F5	D2	9D	38	A3	40
4	A	09	3B	D6	2F	1B	52	E3	B3	29	1A	A0	84	6E	5A	83	2C
5	B	53	CB	BE	58	20	6A	4C	39	4A	ED	5B	CF	FC	B1	D1	00
8	C	CD	A7	7E	19	5F	C4	5D	3D	64	EC	17	73	97	44	0C	13
F	D	8C	99	2D	BB	BF	41	54	0F	B0	0D	68	16	E6	42	A1	89
1	E	CA	D4	A2	72	FA	AD	A4	AF	9C	7D	F0	C0	59	47	82	C9
A	F	E0	D3	AC	E4	49	C2	95	62	91	0A	5C	79	06	24	32	3A

IV. SIMULAION AND RESULTS

A complete simulation of the modified Milenage algorithm is achieved using Microcontroller (PIC18F452). The Avalanche tests are introduced to compare between the original and modified milenage.

(i) For AES standard – 128

Plain text = [CF574710 2773651A6E238818 A27CB9EF], Secret Key=[885C3649 B840D9E0 06D061F5F6FC6046] and Cipher Text = [B218A58FA18EB4B764737D51 83378B4E].

(ii) For Modified AES-128

[Dynamic S-box] using PN sequence random generator. Reshaped Secret Key 64 bit= [8E8C57BC 4EBCB9A6], Column dynamic S-box after arrangement = [6093B714F2AEDC58] and final dynamic S-box ROWs after arrangement = [A14FC 8D65B09E372].

Table 4. Modified AES (Dynamic S-box) – 128.

Plain text = CF 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EF
Secret Key = 88 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = 38 B1 4D 2A 56 81 2F 13 FF EE 38 69 FA A4 77 40

(iii) Avalanche test

Table 5. Results of Avalanche test due to change one bit in plain text in standard AES.

Changed one bit (1)
Plain text = 4F 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EF
Cipher Text= 23 B0 6F 4D 38 93 19 64 B4 DD 8A DE 7A 16 0A BC
Difference value = 91 A8 CA C2 99 1D AD D3 D0 AE F7 8F F9 21 81 F2 Ratio=51.56%
Changed one bit (15)
Plain text = CF 55 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EF
Cipher Text= 51 75 5C B4 E9 B5 FD AF C1 CA F3 FE F5 B4 5E E2
Difference value = E3 6D F9 3B 48 3B 49 18 A5 B9 8E AF 76 83 D5 AC Ratio=53.90%
Changed one bit (69)
Plain text = CF 57 47 10 27 73 65 1A 66 23 88 18 A2 7C B9 EF
Cipher Text= 9F BB 05 72 7E 08 28 23 77 DE 80 21 2B 68 A1 BA
Difference value = 2D A3 A0 FD DF 86 9C 94 13 AD FD 70 A8 5F 2A F4 Ratio=53.90%
Changed one bit (115)
Plain text = CF 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C 99 EF
Cipher Text= DC 7F 25 84 3F 5D 38 46 73 86 0E 3B F7 54 AB 09
Difference value = 6E 67 80 0B 9E D3 8C F1 17 F5 73 6A 74 63 20 47 Ratio=50.00%
Changed one bit (128)
Plain text = CF 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EE
Cipher Text= 8B B7 62 9E 65 73 58 29 38

A0 2E C9 42 CE DB F9
Difference value = 39 AF C7 11 C4 FD EC 9E 5C D3 53 98 C1 F9 50 B7 **Ratio=54.68%**

Table 6. Results of Avalanche test due to change one bit in plain text in modified AES.

Changed one bit (1)
Plain text = 4F 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EF
Cipher Text = A6 3B 8A BD B0 84 37 EA BF 7E F5 A4 1D 8F F9 0C
Difference Value = 9E 8A C7 97 E6 05 18 F9 40 90 CD CD E7 2B 8E 4C Ratio=49.21%
Changed one bit (15)
Plain text = CF 55 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EF
Cipher Text = 5F EC 44 96 1B C5 F4 36 52 F2 E4 72 5E 25 22 9B
Difference Value = 67 5D 09 BC 4D 44 DB 25 AD 1C DC 1B A4 81 55 DB **Ratio=50.00%**
Changed one bit (69)
Plain text = CF 57 47 10 27 73 65 1A 66 23 88 18 A2 7C B9 EF
Cipher Text = 3B E8 CF 4F 38 2C 25 26 C1 7E B7 B1 4C 9F 81 C7
Difference Value = 03 59 82 65 6E AD 0A 35 3E 90 8F D8 B6 3B F6 87 **Ratio=50.00%**
Changed one bit (115)
Plain text = CF 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C 99 EF
Cipher Text = 70 F7 F4 7C 5D AD FE E1 08 02 F4 13 1C 2E DE 62
Difference Value = 48 46 B9 56 0B 2C D1 F2 F7 EC CC 7A E6 8A A9 22 **Ratio=50.00%**
Changed one bit (128)
Plain text = CF 57 47 10 27 73 65 1A 6E 23 88 18 A2 7C B9 EE
Cipher Text = E6 58 E8 C3 91 53 46 B6 CA F4 A9 BC 6C A2 D8 56
Difference Value = DE E9 A5 E9 C7 D2 69 A5 35 1A 91 D5 96 06 AF 16 **Ratio=52.34%**

Table 7. Samples of Avalanche test due to change one bit in Secret Key of AES-128 standard.

Changed one bit (1)
Secret key = 08 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = 06 90 6A 74 99 D1 28 4C 74 C5 B7 D4 BB 8A 3B C3
Difference value = B4 88 CF FB 38 5F 9C FB 10 B6 CA 85 38 BD B0 8D **Ratio=53.12%**
Changed one bit (2)
Secret key = C8 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = B3 3B 73 D4 77 9C F5 CB B5 0A DD FB 4F 27 70 47
Difference value = 01 23 D6 5B D6 12 41 7C D1 79 A0 AA CC 10 FB 09 **Ratio=44.53%**
Changed one bit (16)
Secret key = 88 5D 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = C7 43 E5 6C 4C D6 65 F1 60 31 D9 43 E5 0D 0E 65
Difference value = 75 5B 40 E3 ED 58 D1 46 04 42 A4 12 66 3A 85 2B **Ratio=42.96%**
Changed one bit (99)
Secret key = 88 5C 36 49 B8 40 D9 E0 06 D0 61 F5 D6 FC 60 46
Cipher Text = CB 67 F2 A1 C9 4D B7 21 C0 06 A1 4C DC D6 9B 05
Difference value = 79 7F 57 2E 68 C3 03 96 A4 75 DC 1D 5F E1 10 4B **Ratio=51.56%**
Changed one bit (128)
Secret key = 88 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 47
Cipher Text = 5D F7 E1 35 B8 9D 17 77 68 17 02 CB 12 EF 61 33
Difference value = EF EF 44 BA 19 13 A3 C0 0C 64 7F 9A 91 D8 EA 7D **Ratio=52.34%**

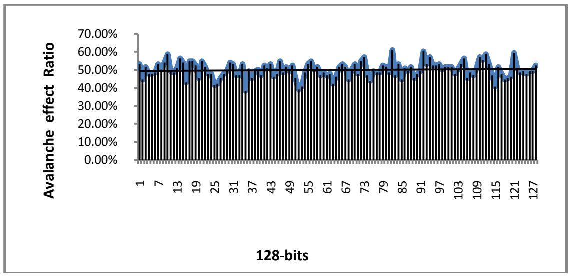


Figure 5. Avalanche effects of AES standard due to change one bit in Secret Key.

Table 8. Samples of Avalanche test due to change one bit in Secret Key of Modified AES.

Changed one bit (1)
Secret key = 08 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = 10 8D DA 81 C6 9C 0A F1 70 58 10 9A 79 04 08 07
Difference value = 28 3C 97 AB 90 1D 25 E2 8F B6 28 F3 83 A0 7F 47 Ratio = 49.21%
Changed one bit (2)
Secret key = C8 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = 7A 0F EA 22 23 2A 1B 89 94 8B 23 16 02 A8 6A 74
Difference value = 42 BE A7 08 75 AB 34 9A 6B 65 1B 7F F8 0C 1D 34 Ratio = 50.78%
Changed one bit (16)
Secret key = 88 5D 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 46
Cipher Text = 80 D1 05 BD 8B A4 40 40 6C 05 28 36 A2 8B 0C F1
Difference value = B8 60 48 97 DD 25 6F 53 93 EB 10 5F 58 2F 7B B1 Ratio = 52.34%
Changed one bit (99)
Secret key = 88 5C 36 49 B8 40 D9 E0 06 D0 61 F5 D6 FC 60 46
Cipher Text = 4A 6C 51 DC 6D B9 99 13 69 B3 72 43 21 7E C3 E6
Difference value = 72 DD 1C F6 3B 38 B6 00 96 5D 4A 2A DB DA B4 A6 Ratio = 51.56%
Changed one bit (128)
Secret key = 88 5C 36 49 B8 40 D9 E0 06 D0 61 F5 F6 FC 60 47
Cipher Text = 00 A6 7B 81 86 50 04 40 94 5E 64 9A 0F 57 18 03
Difference value = 38 17 36 AB D0 D1 2B 53 6B B0 5C F3 F5 F3 6F 43 Ratio = 54.68%

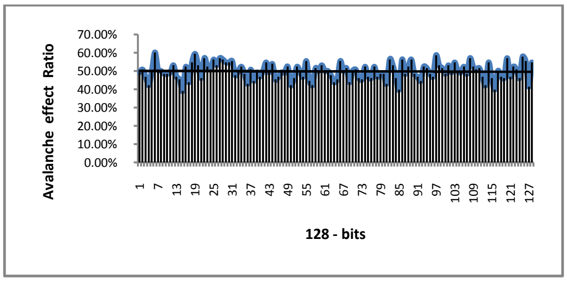


Figure 6. Avalanche effects of Modified AES due to change one bit in Secret Key.

Table 9. Result Outputs of Modified MILENAGE Algorthim to derive a stronger Authentication Vector (AV) than Output of standard Milenage Algorthim (Authentication Vector) in 3GPP. [16], [17].

Key	**9E5944AE A94B8116 5C82FBF9 F32DB751**
RAND	**CE83DBC54AC0274A 157C17F8 D017BD6**
Dynamic Key	**50DA9F6BE38BA65C49FEEC01FE 2CCC87**
SQN	**0B604A81 ECA8**
AMF	**9E09**
OP	**223014C5806694C0 07CA1EEE F57F004F**
OPC	**1B3D2E3E625213D9BC49DBC552 BCDE 4C**
TEMP	**C8B662E237F3E58D24E7B5A96D2 C2C9F**
OUT1	**BA328BB5831B71029111AC8D2332 E862**
OUT2	**13DD09518BE63818E23EDE87AC 73F109**
OUT3	**EF3523C87886D0637FD2B501D02 E3BA2**
OUT4	**0FE930F07931B15882B88BEB4F4D E654**
OUT5	**93A92189A493A876B8F1801A9F8A B8C3**
F1(MAC-A)	**BA328BB5831B7102**
F1*(MAC -S)	**9111AC8D2332E862**
F2(RES)	**E23EDE87AC73F109**
F3(CK)	**EF3523C87886D0637FD2B501D02 E3BA2**
F4(IK)	**0FE930F07931B15882B88BEB4F4D E654**
F5(AK)	**13DD09518BE6**
F5*(AK)	**93A92189A493**
AUTN	**18BD43D0674E9E09BA328BB5831 B7102**
AV	**CE83DBC54AC0274A157C17F80D 017BD6E23EDE87AC73F109EF352 3C87886D063EF3523C87886D0637 FD2B501D02E3BA20FE930F07931 B15882B88BEB4F4DE65418BD43D 0674E9E09BA328BB5831B7102**

V. DISCUSSION AND CONCLUSIONS

(i) The main weakness in Milenage, as stated by the Cryptanalysts, is the use bit rotations and constant XORs in the middle part of the milenage specially if the kernel block cipher in milenage algorithm is susceptible to differential cryptanalysis, then an attacker is capable to proceed a variety of attacks on

milenage algorithm. An attacker cannot predict any useful information if the kernel block cipher in milenage algorithm is a strong secure.

This paper modifies the standard Milenage Authentication algorithm through the dynamic change of the kernel block cipher AES. For every Authentication process a new S-box will be generated using a combination of received random sequence number (RAND), stored Authentication key (Ki) and PN sequence generator to rearrange the columns and rows of standard S-box in AES. Tests proved that the modified AES is more secure than the standard one due to its dynamic structure in addition to increasing its immunity to linear and differential cryptanalysis as shown by avalanche test results in table 12.

Table 10. Average value of avalanche tests for (plain text – Secret key) in AES and Modified AES.

Input type of data	Type of algorithm	Avalanche average value
Plaintext	Modified AES	50.15%
Plaintext	AES	49.71%
Secret key	Modified AES	49.86%
Secret key	AES	49.84%

(ii) Execution time can be reduced as follows:

The implementation of the modified authentication algorithm required more operation than the standard one due to the dynamic nature of its S-box. Using the PIC18F452 microcontroller, the execution time of the modified algorithm can be greatly decreased to about 50.333 ms (instead of 500ms taken by the standard algorithm using IC card. [19]).

REFERENCES

[1] P. Kitsos*, N. Sklavos, O. Koufopavlou "UMTS security: system architecture and hardware implementation" in Wireless Communications and Mobile Computing.- May 2007.-Issue (4):Vol. (7).-pp. 483-494.

[2] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.

[3] J. Daemen and V. Rijmen, The blocks cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.

[4] Reshma Nadaf and Veena Desai "Hardware Implementation of Modified AES with Key Dependent Dynamic S-Box" IEEE ICARET 2012.

[5] Valterri Niemi and Kaisa Nyberg "UMTS security". England: John Wiley & Sons Ltd, the Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, ISBN 0-470-84794-8, 2003.

[6] Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller and Valtteri Niemi."LTE security". United Kingdom: John Wiley & Sons Ltd, the Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, 2013.

[7] 3GPP TS 33.102 V11.5.1 (2013-06) Technical Specification; Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 11).

[8] 3GPP TS 33.105 V11.0.0 (2012-09) Technical Specification; Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic algorithm requirements (Release 11).

[9] Stefan Pütz, Roland Schmitz, Tobias Martin "Security Mechanisms in UMTS" DBLP: journals/dud/PutzSM01, Vol.25, No.6, June 2001.

[10] 3GPP TS 33.401 V12.9.0 (2013-09) Technical Specification; Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE);Security architecture (Release 12).

[11] Sebastian Banescu and Simona Posea "Security of 3G and LTE". Faculty of Computer Science , Eindhoven University of Technology.

[12] Mun, H., Han, K., & Kim, K. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA. Wireless Telecommunications Symposium. WTS2009 (pp. 18). IEEE. (2009).

[13] 3GPP TS 35.206 V11.0.0 (2012-09) Technical Specification; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification (Release 11).

[14] khaled suwais and Azman samsudin "New Classification of Existing Stream Ciphers" INTECH Journal ,1 Feb.2010. [15] Shinsaku Kiyomoto , Toshiaki Tanaka and Kouichi Sakurai "K2: A Stream Cipher Algorithm using Dynamic Feedback Control" Springer, Communications in Computer and Information Science,, Vol.23, 2009, pp 214-226.

[16] 3GPP TS 35.207 V11.0.0 (2012-09) Technical Specification; 3G Security; Specification of the MILENAGE Algorithm

Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test Data (Release 11).

[17] 3GPP TS 35.208 V11.0.0 (2012-09) Technical Specification; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design Conformance Test Data (Release 11).

[18] S3-010014 3GPP TSG SA WG3 Security "Analysis of the Milenage Algorithm Set."QUALCOMM International, Gothenburg, Sweden, 27 February - 02 March, 2001.

[19] 3GPP TS 35.909 V10.0.0 (2011-03) Technical Report; 3G Security; Specification of the MILENAGE Algorithm Set: Document 5: Summary and results of design and evaluation (Release 10).