Int. J. Contemp. Math. Sciences, Vol. 5, 2010, no. 26, 1263 - 1270

A New Algorithm to Construct Secure Keys for AES

Iqtadar Hussain

Department of Mathematics
Quaid-i-Azam University, Islamabad, Pakistan
a_662@yahoo.com

Tariq Shah

Department of Mathematics
Quaid-i-Azam University, Islamabad, Pakistan
stariqshah@qau.edu.pk

Hasan Mahmood

Department of Electronics
Quaid-i-Azam University, Islamabad, Pakistan
hasan@qau.edu.pk

Abstract

In this paper we present new S_8 S-boxes by using the action of symmetric group S_8 on Advanced Encryption Standard S-box [3,] and use these S-boxes to construct 40320^{40320} keys. We apply these keys to Advanced Encryption Standard and propose a key exchange communication algorithm to make it more secure. This algorithm is suitable to exchange keys on insecure communication channels in order to achieve secure communications.

Keywords: Advanced Encryption Standard, Symmetric Group S_8, S-Box.

1. Introduction

Rijndael Block Cipher [3], is based on 128 bits developed by cryptographers, Joan Daemen and Vincent Rijmen, was adopted as Advanced Encryption

Standard (AES) by National Institute of Standards and Technology (NIST) on October 2, 2000 and published as FIPS 197 [11] on 26 November 2001. Currently AES is one of the most popular algorithms used in symmetric key cryptography [6].

Apart from S-box transformation, other transformations such as Sub Byte, Shift Row Operation, and Add Round Key in AES are GF(2) linear, where GF(2)={0, 1} is a prime field of order 2. Therefore, S-box is the only non-linear component of the algorithm to provide confusion [13] capability for AES.

Many cryptanalysts have studied structural properties of AES. In [4], Gerguson et al. presented the simple algebraic description of AES and it's S-box. The most important and necessary algebraic structure within AES was further analyzed in [9], and the polynomial description of AES was introduced in [12].

The S-box has an important role in AES, therefore, most of the work is focused on S-box improvement. In this paper we present new S_8 S-boxes, by using action of symmetric group S_8 on AES S-box [3]. Furthermore, we use these S-boxes to construct 40320^{40320} secret keys from S_8 S-boxes, and then we use these keys in AES and propose an algorithm which is more secure when two parties wish to communicate over an insecure line of communication.

This paper is structured as follows. In Section 2, we briefly present the basic structure and the algebraic expressions for the original S-box as used in AES. In Section 3, we introduce the proposed new S_8 S-boxes. The section 4 presents some important properties such as nonlinearity, differential uniformity, bijective property, and algebraic complexity of these S-boxes. We explain the new algorithm in section 5 and demonstrate why this algorithm is more secure. The conclusions are presented in section 6.

2. Algebraic Expression of AES S-box

In [14], an algebraic expression for original AES S-box is presented. These expressions are derived from the function in $GF(2^8)$. As $GF(2^8)$ is a finite field, therefore, the multiplicative inverse of every element exists and 0→0. This multiplicative inversion for the function $F(x)$ is as follows:

$$F(x) = \begin{cases} x^{-1}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

The affine transformation is decomposed in to two steps: 1) $L(x)$ be a linear transformation in $GF(2^8)$ given as

$$y = L(x)$$

and 2) the AES S-box construction is the addition with the constant value of 99. We define the affine function $H(x)$ in $GF(2^8)$ as

$$H(x) = x \oplus 99$$

The original S-box of AES is the composition of these functions given as,

$$Sbox_{AES} = H \circ L \circ F \tag{1}$$

3. New S-boxes

In this section, we apply the permutations of S_8 on the original S-box [14], and sequentially construct 40320 new S-boxes. The procedure is shown in Table 1.

Table 1: Action of S_8 on S-box

$\pi_1(Sbox_{\text{AES}})$	=	$Sbox_1$
$\pi_2(Sbox_{\text{AES}})$	=	$Sbox_2$
…	…	…
…	…	…
…	…	…
$\pi_{40320}(Sbox_{\text{AES}})$	=	$Sbox_{40320}$

Where $\pi_1, \pi_2, \pi_3, \ldots, \pi_{40320}$ are in S_8. The algorithm to compute S_8 S-boxes is presented in Table 2.

Table 2: Algorithm for S_8 S-boxes

AES S-box
↓
Convert elements of AES S-box into binary form
↓
Apply permutations of S_8 on elements
↓
We get 40320 S_8 S-boxes

An example to construct new AES S_8 S-boxes from the original S-box is shown in Figure 1. The permutation used in the construction is π=(8, 7, 6, 5, 4, 3, 2, 1). Additional 40319 S-boxes can be constructed by applying permutations as given in Table 1.

4. Analysis of S_8 S-Boxes

We present some common properties found in different S-boxes to demonstrate the strength of proposed algorithm.

4.1. Algebraic complexity

Algebraic complexity of S_8 AES S-box, is remains the same as AES S-box [3]. As we are applying permutations on S-box which does not effect the algebraic complexity of S-box.

4.2. S_8 S-boxes are Bijective

In $GF(2^8)$, if all the elements are input of a S-box, the output always takes unique values in $GF(2^8)$. S_8 S-boxes are bijective.

Table 3: An example of bijective S_8 S-Box

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	209	118	215	243	91	241	245	204	18	128	213	177	127	207	185	87
1	105	9	232	246	123	226	197	90	188	78	25	189	46	28	83	72
2	159	254	139	21	23	183	223	108	22	156	220	218	210	106	146	134
3	4	205	145	201	34	15	132	43	133	3	8	89	249	149	27	214
4	160	137	52	35	163	117	99	24	67	179	79	155	176	217	181	12
5	195	202	0	252	16	126	154	227	113	233	63	178	97	100	98	237
6	74	253	57	251	193	228	147	140	196	250	1	247	66	54	175	56
7	194	153	64	173	11	174	50	222	62	31	107	144	2	255	219	75
8	236	36	131	124	231	143	68	135	76	157	119	182	84	230	162	211
9	80	136	229	110	17	49	10	40	69	125	58	6	111	103	161	235
10	88	19	51	33	224	5	20	102	73	203	60	81	138	142	92	242
11	221	104	151	244	172	206	101	184	116	71	94	121	212	115	61	32
12	59	114	148	53	38	29	30	77	120	238	86	167	225	190	169	41
13	82	55	158	85	96	129	95	37	208	150	199	186	13	200	166	47
14	216	122	42	130	240	234	45	14	171	39	141	248	109	198	48	239
15	44	152	168	164	191	93	65	112	192	170	180	165	26	70	187	7

4.3. Nonlinearity

The upper bound of nonlinearity is: $N(f)=2^{n-1}-2^{n/2-1}$ [5] for S-box in $GF(2^n)$. As S-box in AES is in $GF(2^8)$, the optimal value of N is 120. In this case $N(\pi_i(H \circ L \circ F))$=112. The S_8 S-box is not completely a nonlinear function, therefore, its nonlinearity approaches the upper bound. As a result, it can effectively resist

linear cryptanalysis [8].

4.4. Differential uniformity

Definition: Consider two finite abelian groups G_1 and G_2 and define a mapping $f:G_1 \rightarrow G_2$. This mapping is differentially δ-uniform if for all $\alpha \in G_1$, $\alpha \neq 0$ and $\beta \in G_2$, and

$$|\{z \in G_1 \mid f(z+a) - f(z) = \beta\}| \leq \delta$$

As presented in [6], the lower bound of differential uniformity of $n \times m$ S-box is $\delta = 2^{n-m+1}$. This class of S-boxes is called almost perfect nonlinear [1].

Now we prove this property for our S_8 S-box. Proof: Let $A = H \circ L$ be an affine over $GF(2^8)$. S_8 S-box is constructed as $\pi_i\ (A \circ F)$ where $\pi_i \in S_8$ and F is inversion function. As AES S-box is differentially 4-uniform [10], so our S_8 S-box is also differentially 4-uniform because π_i: $GF(2^8) \rightarrow GF(2^8)$ is also differentially 4-uniform.

Table 4: Properties of S_8 S-box

S-box	Non-linearity	Differential Uniformity	Algebraic Complexity	Bijection
Opt. Value	120	4	255 terms	Yes
AES	112	4	9 terms	Yes
S_8 S-box	112	4	9 terms	Yes

5. Use of S_8 S-boxes for construction of secret keys

The aim of S_8 S-boxes is to construct secret keys for AES. The proposed algorithm is as follows:

We consider a set $|X|$ which consists of *SubBytes*

$$X = \{SubByte_1, SubByte_2 ... SubByte_n\}$$
$$where, n \leq 40320$$

and a set Y of S_8 S-boxes

$$Y = \{S_8 S - box_i\}$$
$$where, i = 1,2,3 ... 40320$$

And define a function

$$f : X \to Y$$

We can define n^{40320} functions between X and Y [15] where $n=|X|$. The basic purpose of this function is to substitute S_8 S-boxes in *SubBytes*, therefore, we have n^{40320} options to substitute S-boxes in *SubByte* when |X|=40320, we have total options of 40320^{40320} functions. In addition, it is important that every *SubByte* takes a single S-box. If f is a singleton function then $f(a_i)=a$, where a is a fixed S-box and every *SubByte* uses S-box a. If f is injective function then every *SubByte* uses a different S-box with the condition that $|X| \leq |Y|$. The keys are initially defined as,

$$a_i = f_i : X \to Y$$

where f_i are functions, this implies that we have n^{40320} secret keys. Now we use these keys in Advanced Encryption Standard.

In order to demonstrate the proposed algorithm, suppose we wish to exchange a secret message across an insecure communication line. The secret key is also exchanged during the communication process over this insecure line. This can be accomplished as follows.
Both the originator and the receiver of message must have these keys defined prior the start of communications. Using the AES with a particular key, say a_1, the originator of the message encrypts his data of length 16 and sends it across an insecure line of communication. The sender also informs the receiver about the particular key (in this case a_1), with which he/she is encrypting the message, and as a consequence, the receiver can decrypt this message by using the defined key.

Remark: If the keys are encoded using injective functions, the proposed algorithm performs better as compared to other algorithms which use non injective function.

Table 5: Proposed Algorithm

Round Data In
↓
SubByte
$a_1, a_2, a_3 ..., a_n$ where $n \leq 40320^{40320}$
↓
Shift Row
↓
Mixed Column
↓
Add Round Key
↓
Round Data Out

6. Conclusion

The encryption method presented in this paper is more secure for a system in which two parties attempt to establish a secure channel. The exchange of secret messages via an insecure line of communication utilizes n^{40320} key options available at the initiator. The originator of the communication session has the option to change the keys with every message of length 16. If someone wishes to break the code of this system, two options are available: either he checks all n^{40320} keys or he observes the alphabet frequency of encrypted message, In case 1 if we consider simplest option for |X|=n=2 then we can have 2^{40320} (which is extremely large) secret keys, and if code breaker make millions of calculations per second even then he needs thousands of years to decrypt the message. In second case, this code provides similar complexity as AES.

Acknowledgements. This work is supported in part by HEC Grant No. 1-308/ILPUFU/HEC/2009.

References

[1] T. Beth and C. Ding, "On almost perfect nonlinear permutations," *In EUROCRYPT93, LNCS 765,* pages 65-76, 1994.

[2] L. Cui and Y. Cao, "A new S-box structure named Affine-Power-Affine," *International Journal of Innovative Computing*, *Information and Control*, 3(3), 2007.

[3] J. Daemen and V. Rijmen, "AES proposal: Rijndael AES algorithm submission," 1999.

[4] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," *In Selected Areas in Cryptography SAC01, LNCS2259*, pages 103--111, 2001.

[5] D. Feng and W. Wu, "Design and Analysis of Block Ciphers," *Tsinghua University Press*, 2000.

[6] M.T Tran, D.K.Bui, A.D Duong, "Gray S-Box for Advanced Encryption Standard," *Computational Intelligence and Security, 2008. CIS '08. International Conference on*, Volume 1, 13-17 Dec. 2008 Page(s):253 – 258 Digital Object Identifier 10.1109/CIS.2008.205

[7] J. Liu, B. Wai, X. Cheng, and X. Wang, "An AES S-box to increase complexity and cryptographic analysis," *In Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05),* Volume 1, pages 724-728, 2005.

[8] M. Matsui, "Linear cryptanalysis method for DES cipher." *In EUPOCRYPT93, LNCS 765*, pages 386-397, 1994.

[9] S. Murphy and M. J. Robshaw, "Essential algebraic structure within the AES," *In Crypto'02, LNCS 2442,* pages 1-16, 2002.

[10] K. Nyberg, "Differentially uniform mapping for cryptography," *In EUROCRYPT93, LNCS 765*, pages 386-397,1994.

[11] National Institute of Standards and Technology. FIPS,197, "Announcing the Advanced Encryption Standard (AES)," 2001.

[12] J. Rosenthal, "A polynomial description of the Rijndael Advanced Encryption Standard," *Journal of Algebra and its Applications*, 2(2):223--236, 2003.

[13] C. E. Shanon, "Communication theory of secrecy systems," *In Bell System Technical Journal*, volume 28(4), pages 656-- 715, 1949.

[14] M. T. Tran, D. K. Bui, and A. D. Doung, "Gray S-box for Advanced Encryption Standard," *International Conference on Computational Intelligence and Security*, Pages 253-256, 2008.

[15] http://demonstrations.wolfram.com/, Relations And Functions Between Small Sets/.

Received: November, 2009