Change in the Key Expansion Function of AES

Gaurav Kumar, Kunwar Pal, Dilbahar Singh

Abstract — This paper contains the new changes in key expansion function in Advanced Encryption Standard (AES). AES is vulnerable of various attacks theoretically. All the functions for substitution permutation and confusion-diffusion are applied only in the main part of the algorithm but there is no prefect security for the key expansion function. The related key attack, related sub keys attack and long biclique with meet in the middle attacks are applied on AES because of the weak key expansion function. Authors of AES accepted that the key expansion function of AES is comparatively weak. Here we are trying to remove the weaknesses of AES by changing some basic functions of AES key expansion function. For the security of related key attack and related sub keys attack, we are adding some new function for security of the key expansion. We are changing the Rcon matrix into an Rvar matrix by using given key. This will increase security of AES.

Index Terms — AES, Key Expansion Function, Rcon Matrix, Rvar Matrix, SSL, Encryption/Decryption, Security.

I. INTRODUCTION

Cryptography is the science of writing a message in secret code. Encryption/decryption is the root of cryptography. Before the digital age, the largest users of cryptography were governments and encryption/decryption was used particularly for military affairs. It played a major role in passing secret messages among the soldiers of the same country since they never wanted their enemy to understand the meaning of their messages even if they got their hands on them. Cryptography serves as one of the strongest and main tools for maintaining privacy, corporate security, trust, confidentiality, electronic payments, access control and many other functions. Cryptography provides a set of specific security requirements which are absolutely necessary for client/server and application to application communication. Now-a-days Advanced Encryption Standard Algorithm is used in symmetric key cryptography for encryption and decryption for data security. AES algorithm is a symmetric-key block cipher in which both the sender and receiver use a single key to encrypt and decrypt the information. In the AES as described in the FIPS 197 (NIST)\ [3] [2], the cipher takes a plaintext block size of 128 bits, or 16 bytes and the key length can be 16, 24 or 32 bytes (128, 192, or 256 bits). AES is the most usable encryption standard and has a variable key length. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. The input to the encryption and decryption algorithms is a single 128-bit block. The process consists of number of rounds. Where number of rounds depends on the key length: 14 rounds for a 32-byte key, 12 rounds for a 24-byte key and 10 rounds for a 16-byte key.

AES 128 is the fastest of these ciphers and AES 256 is the slowest as Shannon (1949) described in his study [1]. AES is used in most of web browser and banking work like ATM transaction, online transaction etc. In web browsers, AES works for the confidentiality of the content. It works through the code migration process. Most of the web browsers contain the fix table of AES and other secure algorithm. Secure Socket Layer (SSL) encrypt the segments of network connections at the Application Layer for the Transport Layer using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity. When user ask for the encryption, Secure socket layer is used for that and since browser contain the fixed part of the algorithm, the code of the algorithm is send to the web browser through the network and encryption take place. AES is used for the symmetric encryption for confidentiality of the content with the help of secure socket layer. Since AES is the most trusted algorithm and it is used for all the security propose but due to the new attacks like related sub keys attack, related key attack [8][4] and biclique attack [7], it is going to decrease in security. All these attacks are applied on AES because of the weak key expansion function and weak transformation function [4], [7], [8], [9], [10], [11], [12], [15]. So we are trying to remove these weaknesses of advanced encryption standard and trying to provide a more secure AES. If encryption algorithm is not secure then it can be injurious for whole the country as most of the things are kept secure with the encryption process keeping the data in the encrypted form. If security of algorithm is compromised then the whole country's security compromised. So, the algorithm used for the security should be more secure and it should not be compromised with any type of attack. As these attacks are of high complexity so they do not threaten the practical use of AES in any way but we cannot say that what will happen tomorrow. So we have to be prepared today for tomorrow so that if intruder is able to break the AES algorithm then what will do. So we are trying to remove the weaknesses of AES. Because of all the cryptanalysis, AES is not as secure as it was twelve years ago when it was chosen by NIST. [7]

A. AES Structure

AES is built on the basis of substitution permutation network (SPN). In a SPN, all the bits are changed in every round. In the first round of SPN, we are XOR the current state with the round key i.e. first round key. Then we go through a substitution layer, where blocks of Data are replaced with other blocks, and then we go through a permutation layer where bits are permuted and shuffled around. This process is done again and again. In the last round, we XOR with the very last round key, and then the output is produced. In AES the first N-1 rounds (where N is total number of rounds) consist of four distinct transformation functions:

Manuscript received March, 2013.

Mr. Gaurav Kumar, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.
Mr. Kunwar Pal, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.
Mr. Dilbahar Singh, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.

SubBytes, ShiftRows, MixColumns, and AddRoundKey. The final round contains only three transformation functions. There is an initial single transformation (AddRoundKey) before the first round, which can be considered round zero.

Each transformation takes one 4*4 matrices as input and produces a 4*4 matrix as output. For every round of AES there is a round key which generated by the key expansion function.

B. Key Expansion

Key Expansion function provides the long key for the AddRoundKey operation for each round. It converts a single key to eleven keys having sixteen bytes each. These keys are also a four by four matrix that XOR in AddRoundKey functions with the current state. For the expansion of key from one key matrix to eleven key matrixes, we took the last column of initial key matrix do a single byte shift from top to down and then perform S-Box operation and then XOR with one column of Rcon matrix, and first column of the initial key matrix. Result value is the first column for the next round key. For the second column of the second round key, XOR first column to second column of initial key matrix and for third XOR the second column to the third column and so on. For the third key repeat the procedure as for second but second key matrix is used on the place of first or initial key matrix. AES-256 should be most secure algorithm as the key length is more but it is not happening. AES-256 is vulnerable more attacks comparatively to the other variants of AES i.e. AES-128 and AES-192 because the mixing of bits in AES-256 is not so good by the present function.

II. RELETED PREVIUS WORK

Rijmen V. et.al (1997) explains square attack against square block cipher. In this a set of 256 plaintexts, where 1 active byte can take all values and the 15 other bytes are constant, after 3 rounds of Rijndael, the sum of each byte of the 256 ciphertexts equals zero. This distinguishing property can be used to mount efficient attacks up to 6 rounds. The first attack has a time complexity of 2^{72} encryptions and requires 2^{32} messages[5]. Ferguson et al. (2000) improved the attack by time complexity 2^{46}. They recover the seven rounds of Rijndael under 192-bit and 256-bit keys [6]. Gilbert and Minier (2000) shows that this property can be made more precise using functions of the active byte, which allows to built a distinguisher on 3 rounds. The main idea is to consider the set of functions mapping one active byte to one byte after 3 rounds. This set depends on 9 one byte parameters so that the whole set can be described using a table of 272 entries of a 256 byte sequence. Their attack allows to break 7 rounds of AES-192 and AES-256 with a marginal time complexity over exhaustive search [14]. Demirci H. et.al (2009), has generalised this idea using meet-in-the-middle techniques and able to recover the key of AES till 7^{th} round for all variants [15]. Takahashi J. and Fukunaga T. (2007) based on key expansion and suggested that with byte level fault, a minimum of two faulty cipher texts and a brute force search of 48 and 40 bits respectively reveal the AES key. Through simulations it has been shown that the attack reduced the AES-128 key space to 2^{32} using a single faulty cipher text [9]. Thomas Roche et.al (2011) combined the fault model with side channel attack and compared to state-of-the-art attacks, this fault model advantage is to relax constraints on the fault location, and then reduce a priori knowledge on the implementation. The fault attack is combined with side-channel analysis in order to defeat fault injection resistant and masked AES implementations. This fault injection attack works well even when the attacker has only access to the faulty cipher texts through a side-channel [10]. Eli Biham (1994) explained the influence of key scheduling algorithms on the strength of block ciphers and the key scheduling algorithms of many block ciphers inherit obvious relationships between keys. This can be of two types: one is chosen plaintext reductions of the complexity of exhaustive search attacks and second is low complexity chosen key attacks. These attacks were independent of the number of rounds of the cryptosystems and of the details of the round function [4]. Biryukov and Dmitry (2009) applied the related key attack model on AES. In this attack, attacker knows or chooses a relation between several keys and is given access to encryption/decryption functions with all these keys. The relation between the keys can be an arbitrary bijective function (or even a family of such functions) chosen in advance by the attacker. In the simplest form of this attack, this relation is just an XOR with a constant, where the constant is chosen by the attacker. This type of relation allows the attacker to trace the propagation of XOR differences induced by the key difference through the key schedule of the cipher. However, more complex forms of this attack allow other (possibly non-linear) relations between the keys. This is practically verified. Shamir et.al (2009) explains a related sub keys attack and assume that there is no relation between the keys. As in related key attack, the XOR condition imposed on the key directly implied the same condition on the sub keys which were used in the whitening phase and in the first round. In this new attack they impose a XOR condition on the two sub keys and used in the first and second round. The key difference can then be defined by running the key schedule backwards. They were able to recover 56 bits of the key using only 2^{32} time and 2^{32} chosen cipher texts. The main problem seems to be the key schedule of AES-256, which is not of industrial strength. It does not mix the initial key succinctly, it is too linear, and as a result it has unusually long key differentials of probability 1. In addition, the similarity between the key schedule and the data encryption in AES makes it possible to repeatedly cancel data differences with corresponding key differences over many rounds. Ironically, the related sub keys attack works best against AES-256 (which was supposed to be the strongest member of the AES family), and do not currently seem to work against AES-128. These attacks show that the key scheduling algorithm should be carefully designed and its structure should not be too simple. DES is not vulnerable to the related keys attacks since the shift pattern in the key scheduling algorithm is not the same in all the rounds [11]. Bogdanov Andrew et.al (2011) explains a novel technique name as Biclique Cryptanalysis of block cipher with reference to all the variants of AES. For biclique, we do not need to assume any related keys. The only need a very small part of the codebook and small memory. These are practically verified to a large extent. Biclique attack is the advance version of meet-in-the-middle attack and also used with meet in the middle attack. Firstly, we apply the meet-in-the-middle attack on *n* round out of *r* round and then apply the biclique on the *r-n* round. The dimension of the bicilique decreases as r grows. Biclique is applied on last three rounds and recover the sub keys (total 2^{16}) within 2^9 computations.

This splits 2^{128} key space into groups of 2^{16} keys. To test all 2^{16} keys in a group: Perform a base computation and then pre-compute 2^{16} keys combine one forward 2^8 and one backward 2^8 computation for free (without any cost).All the 2^{16} keys in the group covered with only 2^9 computations. This is able to recover the key for all the round of AES-128, AES-192 and AES 256.

III. PROPOSED KEY EXPANSION FUNCTION

After analyzing all attacks on AES and as researcher conclude in their studies that the key expansion function is not so strong in AES. Related Key Attack and Related Subkeys Attack are easily applicable to AES. The reason behind to applicability of these attacks is the number of rotation of the byte in key expansion function. DES is secure against the related key attack. In this attack, there is no need to assume the related keys initially. But due the structure of AES if intruder is able to get any Sub key then he will get all the sub keys without any cost. So this is also the problem with AES. The third and most important attack is biclique attack which is applied with meet in the middle attack and able to cryptanalysis of all the variants of AES. This is also applicable due the weaknesses of AES key expansion function. For the biclique attack there is no need to consider any related keys or sub keys. It is simply apply on the AES transformation function in both sides and able to get the sub keys for all the variants. The main objective of our study is to remove the weaknesses of AES as it is compromised the security. We are

trying to remove the problem of AES which makes the AES intruder accessible. As discus above AES has some problem with key expansion function and due to that it compromise its security. In AES all the functions for substitution permutation and confusion and diffusion are applied only in the main part of the algorithm but there is no prefect security for the key expansion function. So, we are trying to make the AES more secure by adding some new function for security of the key expansion. Advanced Encryption Standard has the problem with weak key expansion function. If we look at the key expansion function of AES then we analyse that they had use a fix Rcon matrix. Also we can change some functions as discuss below:

i. Use S-Box function for each column and then XOR with the previous key column as the basic structure of AES.
ii. Change the rotation for every round of the key expansion function like for first key matrix we choose one rotation, for second choose two rotation and then again one rotation or also one rotation for few round and two rotation for some round as we do in DES.
iii. Change the Rcon matrix from fixed to a variable by using multiplication of key byte (from initial key matrix) in GF(2^8).

New key expansion function is better than existing one as it uses Rvar matrix on the place of Rcon matrix. On the other hand we are using S-Box for every column so that it increases the security of the key expansion function. So the proposed key expansion is to enhance the security of AES algorithm. It is also mixing the key bits of the initial key for the subkeys in AES-192, and AES-256.

IV. CONCLUSION AND FUTURE WORK

In the new key expansion function use of Rvar matrix on the place of Rcon matrix and S-Box for every sub keys column will increase the security of the key expansion function with increasing the complexity of AES. But in future as day by day speed of processors is going to increase with decreasing the cost so it can be used for future. For the future, if complexity of AES remains same with improved security then it will be the more secure algorithm. And it should be tested on the different environment with different test cases.

REFERENCES

1. Shannon, (1949) “Communication Theory of Secrecy Systems,” Bell System Technical Journal, vol. 28, pp. 656-715.
2. Daemen Joan and Rijmen Vincent (2010) “The First 10 Years of Advanced Encryption”, IEEE Security & Privacy 8(6), pp. 72-74.
3. FIPS Publication (2001) “Advanced Encryption Standard”, NIST (2001).
4. Biham Eli (1994) “New Types of Cryptanalytic Attacks Using Related Keys”, in Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, EUROCRYPT ’93, May 23–27, pp. 398-409.
5. Daemen, J., Knudsen, L.R., Rijmen, V. (1997) “The Block Cipher SQUARE”, In Biham, E., ed.: Fse. Volume 1267 of Lecture Notes in Computer Science, Springer,pp. 149–165.
6. Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D., Whiting D. (2000) “Improved Cryptanalysis of Rijndael”, In Schneier B., ed. FSE. Volume 1978 of Lecture Notes in Computer Science, Springer pp. 213–230.
7. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger (2011) “Biclique Cryptanalysis of the Full AES”, in ASIACRYPT 2011. pp 344-371.
8. Biryukov Alex, Dunkelman Orr, Keller Nathan, Khovratovich Dmitry, and Shamir Adi (2009) “Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds”, Cryptology ePrint Archive: Report 2009/374, August 2009.
9. Takahashi J., Fukunaga T. and Yamakoshi K. (2007) “Differential Fault Analysis on the AES Key Schedule”, in Proceedings of 4th International Workshop on Fault Detection and Tolerance in Cryptography, FDTC, 2007, Springer, pp. 62–72.
10. Thomas Roche, Victor Lomne and Karim Khalfallah (2011) “Combined Fault and Side-Channel Attack on Protected Implementations of AES”, in 10th IFIP WG 8.8/11.2
11. Demirci H., Taskin I., Coban M., Baysal A. (2009) “Improved Meet-in-the-Middle Attacks on AES” In Roy, B.K., Sendrier, N., eds.: Indocrypt. 5922 of Lecture Notes in Computer Science, Springer, pp.144–156.
12. Biham E. and Keller N. (2000) “Cryptanalysis of Reduced Variants of Rijndael”, technical report, Computer Science Department, Technion – Israel Institute of Technology.
13. Patrick Derbez, Pierre-Alain Fouque, Delphine Leresteux (2011) “Meet-in-the-Middle and Impossible Differential Fault Analysis on AES”, in 13th International Workshop, Nara, Japan, September28–October1, 2011. pp 274-291.
14. Gilbert H. and Minier M. (2000) “A Collision Attack on 7 Rounds of Rijndael”, In AES Candidate Conference, pp. 230–241.
15. Alex Biryukov and Dmitry Khovratovich.(2009); Related-key cryptanalysis of the full AES-192 and AES-256. In ASIACRYPT'09, Springer, pp. 1-18.
16. E. Biham and A. Shamir (1997) “Differential Fault Analysis of Secret Key Cryptosystems”, in Advances in Cryptology, Crypto 1997; LNCS 1294.

AUTHORS PROFILE

Mr. Gaurav kumar has completed master (M.Sc) in mathematics from HNB Garhwal University, Srinagar in 2010 and pursuing his M.Tech in Computer Science and Engineering from Lovely Professional University, Phagwara, Punjab, India. He has keen interest in Pure Mathematics, Cryptography, Data Mining and Cloud Computing.

Mr. Kunwar Pal has completed B.Tech in Computer Science & Engineering from K.N.I.T Sultanpur (U.P.T.U Lucknow) and completed his M.Tech Computer Science & Engineering from P.E.C Chandigarh. Presently he is working as a ASSt Prof in Lovely Professional University. He has a list of publications and currently working in various field of research in cryptography and network security in wired and wireless network. He has keen interest in Cryptography and Network Security, Routing Protocol, and wireless mesh network.

Mr. Dilbahar Singh has completed graduation (B.Tech) in Computer Science Engineering from CCS University, Meerut in 2011. Currently, he is pursuing his Master Degree (M.Tech) in Computer Science and Engineering from Lovely Professional University. He has keen interest in data mining, data warehousing, cryptography and Cloud computing fields.