A Proposed Solutions to Two Possible Attacks over AEGIS Authenticated Encryption Algorithm

Ayman Y. El-Hadary, Mohamed Helmy Megahed, and Mohamed H. Abd ElAzeem

***Abstract*—Authenticated Encryption (AE) is a technique combines both security and authenticity of data. This paper introduces two possible attacks over AEGIS AE algorithm, which are error propagation and tag changing attacks. The first attack is sending incorrect ciphertext for error propagation, that will results in incorrect decryption of all next ciphertexts then retransmission is done which leads to large time delay. The second attack is changing the sent authenticated tag that will result incorrect tag calculation at the receiver. Tag Generation functions dependent on XOR function (linear function) as in AEGIS make the encryption algorithms vulnerable to tag changing attack. In the introduced paper, the proposed solutions are done regarding two security mechanisms which are tag partitioning and check tag resulted from nonlinear function. Tag partitioning is a process to divide the tag into parts this will reduce the time delay of retransmission and non-linear function usage to overcome XOR function problems.**

***Index Terms*—AEGIS, AE, check tag, tag authentication, tag generation, tag partitioning.**

I. Introduction

Data Protection requires the protection of both confidentiality and authenticity. Many solutions for the privacy and authentication problems have existed for decades, and the traditional approach to solving both simultaneously has been to combine them in a straightforward manner using so-called "generic composition." However, recently there have been a number of new constructions which achieve both privacy and authenticity simultaneously, often much faster than any solution which uses generic composition. Authenticated Encryption (AE) [1] is a technique used to provide both secrecy and authenticity of transported information. An AE scheme is usually more complicated than confidentiality-only or authenticity-only schemes. However, it is easier to use, because it usually needs only a single key, and is more robust, because there is less freedom for the user to do something wrong.

At transmitter side, AE algorithms generally generate Ciphertext (C) and then generate the Authentication Tag (T) after the encryption process [2] to ensure data integrity. Both encryption and authentication are done at the same time. The Tag is a message that authenticates the transmitted ciphertext, to make sure that this cipher did not changed. The most well-known Authenticated Encryption Algorithm AEGIS [3] generates the authentication Tag by Xoring the five internal states with each other's as in Fig. 1. Xoring the five internal states with each other's to generate the Authentication Tag makes the algorithm susceptible to tag changing attack where attacker can change one ciphertext to change the five internal states at receiver this results in incorrect decryption on proceeding ciphertexts as in (1-9). Using XOR (Linear) function to generate the Authentication Tag is a Wrong security procedure as shown in the following equations:

$$S_{i+1,\ 0} = \text{AESRound}\ (S_{i,4},\ S_{i,}0 \oplus \text{m}_{i}); \qquad (1)$$

$$S_{i+1,\ 1} = \text{AESRound}\ (S_{i,0},\ S_{i,1}) \qquad (2)$$

$$S_{i+1,\ 2} = \text{AESRound}\ (S_{i,1},\ S_{i,2}) \qquad (3)$$

$$S_{i+1,\ 3} = \text{AESRound}\ (S_{i,2},\ S_{i,3}) \qquad (4)$$

$$S_{i+1,\ 4} = \text{AESRound}\ (S_{i,3},\ S_{i,4}) \qquad (5)$$

$$C_{i} = P_{i} \oplus S_{u+i,1} \oplus S_{u+i,4} \oplus (S_{u+i,2}\ \&\ S_{u+i,3}) \qquad (6)$$

$$S_{u+i+1} = \text{StateUpdate128}\ (S_{u+i}\ ,\ P_{i}) \qquad (7)$$

$$P_{i} = C_{i} \oplus S_{u+i,\ 1} \oplus S_{u+i,\ 4} \oplus (S_{u+i,2}\ \&\ S_{u+i,3}) \qquad (8)$$

$$T = \oplus_{i=0}^{4}\ S_{u+v+7,\ i} \qquad (9)$$

where:

m_{i}... is a 16-byte message block.

$S_{i+1,\ n}$ ... is the output number n (n from 0 to 4) that will be XORed to get the tag.

$S_{i,\ n}$ ... is the internal state number n.

C_{i}... output ciphertext number n.

P_{i}... output plaintext number n.

T... Authentication Tag.

u,v ...u = [adlen/ 128] (adlen is the associated data length), v = [msglen /128] (msglen is the message length).

Therefore, when the attacker changes one output ciphertext (C_{out}) or more, this attack will result in a serious problem in AEGIS algorithm where all internal states will be changed resulted in incorrect decryption. Also, when the attacker sends incorrect ciphertext, this will result in error propagation at receiver side. In AEGIS the decryption of new ciphertext depends on the previous ciphertext. Therefore, in case of changing one ciphertext, error propagation will occur as in (10).

$$C_{i} = P_{i} \oplus S_{u+i,1} \oplus S_{u+i,4} \oplus (S_{u+i,2}\ \&\ S_{u+i,3}) \qquad (10)$$

Instead of using ($S_{i+1,\ 0}$) in equation (1) the attacker will

Manuscript received October 27, 2018; revised December 12, 2018.

Ayman Yousry El-Hadary is with the Department of Electronics and Communication, Cairo, Egypt (e-mail: a.elhadary99@yahoo.co.uk).

Mohamed Helmy Megahed is with the Communications Department of Canadian International College (CIC), Cairo, Egypt (e-mail: mmega080@uottawa.ca).

Mohamed Hassan Abd ElAzeim is with the Department of Electronics and Communication of Arab Academy for Science Technology and Maritime Transport (AASTMT), Cairo, Egypt (e-mail: mhabdazeem@hotmail.com).

DOI: 10.7763/IJCTE.2018.V10.1223

use ($S'_{i+1,0}$) this will change all the other internal states to be S'_1, S'_2, S'_3 and S'_4.In this paper, a new and secure Tag generation and Tag partitioning is introduced. The generated Tag is a check tag for output ciphertexts which is generated from nonlinear function as a new security layer for Authentication. This check value is a result of Non-Linear Keyed Modulo Multiplication Function [4] that works with pre-shared Key between the transmitter and receiver. This check tag will be generated at the transmitter side and will be checked at the receiver side by comparing the received check tag with the generated check tag at receiver. AEGIS tag depends on the five internal states as in Fig. 1. Two opposite changes in two internal states will result in the same tag. These changes will result in different ciphertext with the same tag. The importance of Non-Linear Modulo Multiplication Function is introduced regarding that the tag depends on ciphertexts in non-linear function not XOR linear function on the internal states. Also, in this paper a tag partitioning mechanism is introduced to mitigate error propagation attack in AEGIS. Tag partitioning is introduced to reduce the time delay of retransmitting the wrong blocks during transmission where every 1024 blocks plaintext has a separate Tag.

A. Contributions

The contributions in the proposed model are two mechanisms:

B. Tag Generation Depending on Non-linear Function

In this paper, a check tag value resulted from Non-Linear Modulo Multiplication function is introduced. The check tag value is generated from:

- Every 1024 output ciphertexts are XORed to get $C_{\text{equivalent}}$.
- $C_{\text{equivalent}}$ split into 8 parts (E_1, E_2... E_8).
- Every E_n (n= 1, 2... 8) is modulo (2^{16}+1) multiplied with pre-shared key (K) to get T_n.
- $T_{\text{equivalent}}$ is the check tag value which resulted from concatenating T_1 to T_8.

C. Tag Partitioning

Tag Partitioning is a technique used to reduce the time delay of retransmitting the wrong blocks during transmission. In the proposed Tag Partitioning method, every 1024 output ciphertexts are segmented and has a Tag. The Authentication Tag (AT) is created and attached to the related segment in the padding of the IP communication protocol to reduce the size of transmission then sent to the receiver side. This Tag Partitioning method will decrease the time delay of transmission of wrong ciphertexts.

D. Outline of the Paper

Section II introduces the related work. Section III introduces the Proposed Models. Section IV presents the Security Analysis. Section 5 presents a comparison between AGEIS and Modified AEGIS. And section 6concludes the paper.

II. Related Works

In this section, related works are introduced as the following:

E. AEGIS

AEGIS [3] is AE online mode of operation which provides both authenticity and confidentiality in one shot. AEGIS is constructed on the basis of using AES encryption round function. There are 3 types of AEGIS which are AEGIS-128L, AEGIS-128 and AEGIS-256. AEGIS-128L uses eight AES round functions to process a 32-byte message block (one step). AEGIS-128 processes a 16-byte message block with 5 AES round functions, and AEGIS-256 uses 6 AES round functions. The computational cost of AEGIS is about half that of AES. In AEGIS the message used to update the state of the cipher text as shown in Fig. 1. AEGIS is very fast. AEGIS-128L, AEGIS-128 and AEGIS-256 are about 0.48cpb, 0.66 cpb and 0.70 cpb, respectively. The speed of AEGIS-128L is faster than that of AES in counter (CTR) mode, and is about 8 times than that of AES encryption in CBC mode. AEGIS algorithm provides high security. As long as the nonce is not reused, it is hard to recover the AEGIS state and key faster than exhaustive key search (under the assumption that a 128-bit authentication tag is used, and the forgery attack cannot be repeated for the same key for more than 2128 times). Usually AEGIS is used for network communication to protect a packet while leaving the packet header unencrypted.

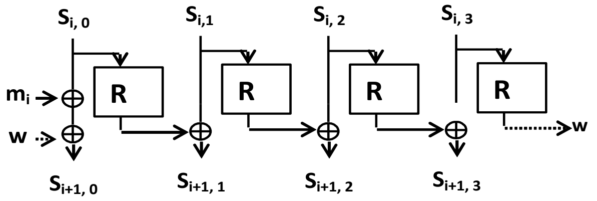

Fig. 1. State update function in AEGIS-128. R indicates AES rounds without XORing with the round key and w is temporary 16-byte word.

F. Tag Generation in AEGIS

In AEGIS After generation of all ciphertext, the Authentication Tag (T) is generated by Xoring the internal states S to generate the Authentication Tag, as in equations (1- 9).

G. Attacks on Authenticated Encryption Algorithms

There are many attacks [5]-[11] that may encounter Authenticated Encryption Algorithms. We make these under consideration when proposing the Tag generation function. Examples of these attacks are:

1. Side-Channel Attack
2. Cross –Site Tracing Attack
3. Forgery Attack
4. Key-Recovery Attack
5. Square Attack (Integral Attack)
6. Truncated Differential Cryptanalysis
7. Related Key Attack
8. Saturation Attack
9. Interpolation Attack

III. Proposed Model

A. Traditional Data Integrity Check

The authentication tag is generated by Xoring all output ciphertexts (C) as in (11):

$$C_1 \oplus C_2 \oplus \ldots \oplus C_n = \text{Authentication Tag } (T) \qquad (11)$$

where n is the number of all output ciphertexts.

B. Attacked Data Integrity

From (11) C_{total} equals:

$$C_1 \oplus C_2 \oplus \ldots \oplus C_{n-1} = C_{\text{total}} \qquad (12)$$

Then T is the result of XORing C_{total} with C_n as in (13):

$$C_{\text{total}} \oplus C_n = T \qquad (13)$$

Attacker will get C_{total} by Xoring equation (13) with C_n as following:

$$C_{\text{total}} \oplus C_n \oplus C_n = \bar{C}_{\text{total}} \qquad (14)$$

Note that ($x \oplus x = \bar{x}$ "complement value", to get x ($\bar{\bar{x}} = x$))

Now the attacker has $\bar{C}_{total}$, then, he can get ($\bar{\bar{C}}_{total} = C_{total}$), if he changes C_n to $\boldsymbol{C_n'}$ and change T to T_{attacked}, equation (13) will be:

$$C_{\text{total}} \oplus C_n' = T_{\text{attacked}} \qquad (15)$$

The receiver side will receive C_n' and the associated T_{attacked} and will not notice any changes.

C. Proposed Data Integrity Check

In the proposed data integrity check, we get the check tag value ($T_{\text{equivalent}}$) as follows:

$$C_1 \oplus C_2 \oplus \ldots \oplus C_{1024} = C_{\text{equivalent}} \qquad (16)$$

$$C_{\text{equivalent}} = E_1 \| E_2 \| \ldots \| E_8 \qquad (17)$$

where, $C_{\text{equivalent}}$ splits into eight parts (E_i ... i from 1 to 8).

$$\text{Key} \bullet E_i \bmod(2^{16}+1) = \text{check tag } (T_i) \qquad (18)$$

$$T_1 \| T_2 \| \ldots \| T_8 = T_{\text{equivalent}} \qquad (19)$$

In the proposed data integrity check, attacker will not be able to change the tag without detecting this change at receiver side. Also, the attacker will face hard complications to be able to change the tag as the tag is the output of Non-Linear Keyed Modulo function.

D. Check Tag Generation in Modified AEGIS

In the proposed paper, the inputs of the Check Tag function ($C_{\text{equivalent}}$) are the output ciphertexts ($C_{1,\,2,\,3\ldots\,1024}$) XORed with each other, as in (20) and Fig. 2.

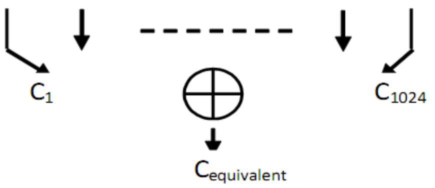

Fig. 2. XORing ciphertexts to get equivalent ciphertext value.

$$C_1 \oplus C_2 \oplus C_3 \oplus \ldots \oplus C_{1024} = C_{\text{equivalent}} \qquad (20)$$

$C_{\text{equivalent}}$ is divided into parts of 16 bits (from part E_1 to part E_8)

The output $C_{equivalent}$ split into 8 parts (from E_1 to E_8) each of 16-bits. Each part of these 8 parts is modulo multiplied (modulo 2^{16}+1) with a key (K) to get a check tag value T_i (i= 1, 2 ...8), as in (21) and Fig. 3. Check tag values from T_1 to T_8 with length 16-bit are concatenated to result in the final check tag value ($T_{\text{equivalent}}$) of lenght128-bit, as shown in Fig. 4. $T_{\text{equivalent}}$ value is generated in transmitter side and sent to the receiver side. The receiver side also generates this value and compares the received value with the generated value at the receiver. If the two values are not identical request for retransmission of associated ciphertext is sent to the transmitter side. This Check Tag value provides a further secure authenticity to AEGIS encryption algorithm as it depends on the output ciphertexts not on the internal states.

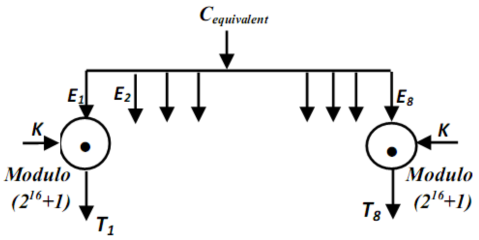

Fig. 3. Generating check value tags from T_1 to T_8.

$$E_i \bullet \text{Key modulo multiplication } (2^{16}+1) = \text{Check Tag Value } (T_i) \qquad (21)$$

where (i from 1 to 8).

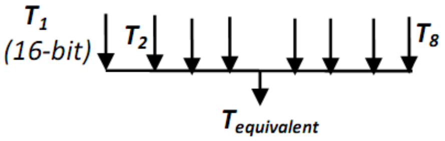

Fig. 4. Generating check value Tequivalent.

E. Tag Partitioning

In the introduced Tag Partitioning method, every 1024 output ciphertexts are segmented and have a Check Tag value ($T_{\text{equivalent}}$). The Check Tag value ($T_{\text{equivalent}}$) is generated and attached to the relative segment in the padding of IP communication protocol [12] to reduce the size of transmission, and then sent to the receiver side. Also, $T_{\text{equivalent}}$ is generated at receiver side, the received $T_{\text{equivalent}}$ and the generated $T_{\text{equivalent}}$ at the receiver side will be compared. If they are identical, request for retransmitting the associated segment will not be sent, if not, a request for retransmitting the segment will be sent to the transmitter side. The introduced Tag Partitioning method reduces the time delay of retransmitting the wrong blocks during transmission.

F. Tag Insertion

The check Tag value is inserted in the unused frame of IP protocol to make no overhead on the communication channel [13].

IV. Security Analysis

A. Error Propagation Attack

In error propagation attack, the attacker send incorrect ciphertext, as mentioned before in AEGIS the decryption of new ciphertext depends on the previous ciphertext; this will result in error propagation at receiver side as in equation (10), and request for retransmitting the whole file will be sent by the receiver side to the transmitter side. In the introduced paper, we overcome the error propagation attack by introducing Tag Partitioning technique, where, if the attacker sent incorrect ciphertext the associated authenticated tag will be changed and detected by the receiver and a request for retransmitting only the associated 1024 ciphertexts not all message will be sent to the transmitter.

B. Tag Changing Attack

In AEGIS, the authentication Tag is generated by Xoring the five internal states with each other. If an attacker changes one ciphertext and the associated authentication tag as in equations (12 – 15) the receiver will not discover this change. This made the algorithm vulnerable to tag changing attack. Also, by changing one ciphertext the five internal states of AEGIS algorithm will change at the receiver side, this will results-in incorrect decryption of the proceeding ciphertexts and then error propagation. In the introduced paper, we overcome Tag Changing attack by making the Authentication Tag depend on ciphertexts not on the internal states, and the check tag value is generated as a result of Non-Linear keyed Modulo function which is immune to tag changing attack.

V. Comparison between AEGIS and Modified AEGIS

A comparison between standard AEGIS and the proposed Modified AEGIS after applying the two solutions is done as shown in Table I.

TABLE I: Comparison between AEGIS and the Introduced Modified AEGIS

No.	Point of view	Modified AEGIS	AEGIS
1	Error Propagation for whole file	NO	Yes
2	Error Propagation for part of file	Yes	Yes
3	Time Delay for retransmission	Resend small part of the file	Resend whole file
4	Tag Partitioning	Yes	No
5	Tag Dependant on Ciphertext	Yes	Yes
6	Non-Linear function for Tag Generation	Yes	No
7	Security	Defeat the two possible attacks	Vulnerable to the two possible attacks

As shown in Table I, the modified AEGIS is favorable over the slandered AEGIS, as in modified AEGIS there is no error propagation in the whole transmitted file. Also, the time delay due to retransmission of faulty or changed blocks is smaller than that in standard AEGIS due to the use of tag partitioning. The use of non-linear function in modified AEGIS instead of normal XOR function to generate the tag made the modified AEGIS more secure and robust to the proposed two possible attacks over AEGIS.

VI. Conclusion

In this paper, we mitigate the effect of two attacks on AEGIS encryption algorithm which are error propagation attack and tag changing attack. New Check Tag authentication Function and Tag Partitioning method are introduced using Non-Linear Keyed Modulo Function to overcome these attacks. These solutions provide high security and authenticity levels, and made AEGIS immune to the proposed two attacks. Also, these contributions made AEGIS perform faster. Tag Partitioning concept is introduced to reduce the time delay of retransmission of wrong authenticated files, and check Tag function is introduced to make the Tag generation dependent on Non-Linear Function with ciphertexts as inputs, not on the internal states, to detect any changes in ciphertexts during the transmission through the communication channel and to overcome the lack of security due to using XOR function (linear function) to get the authentication tag.

Acknowledgment

This research was supported by the authors. We are thankful to Arab Academy for Science and Technology and Maritime Transport Department of Communications who encouraged us to work hard.

References

[1] M. Bellare, P. Rogaway, and D. Wagner, "A conventional authenticated-encryption mode," National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), pp. 1-3, April 13, 2003.

[2] M. Bellare and C. Namprempre, "Authenticated encryption: relations among notions and analysis of the generic composition paradigm," in *Proc. Springer 6th International Conference on the Theory and Application of Cryptology and Information Security*, December 2000.

[3] H. Wu and B. Preneel, "AEGIS: Fast authenticated encryption algorithm," SAC, School of Physical and Mathematical Sciences Nanyang Technological University, 2013.

[4] Non-Linear Key Modulo Function. (2018). [Online]. Available: https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-multiplication

[5] D. Page, "Defending against cache-based side-channel attacks," Information Security Technical Report, vol. 8, issue 1, pp. 30-44, March 2003.

[6] Y. Li, M. Chen, and J. Wang, "Introduction to side channel attacks and fault attacks," in *Proc. IEEE 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, July 2016.

[7] V. Nithya, S. L. Pandian, and C. Malarvizhi, "A Survey on detection and prevention of cross-site scripting attack," *International Journal of Security and Its Applications (IJSIA)*, vol. 9, no. 3, pp. 139-152, September 2015.

[8] H. Shahriar and M. Zulkernine, "Client-side detection of cross-site request forgery attacks," in *Proc. IEEE 21st International Symposium on Software Reliability Engineering*, vol. 21, no. 48, pp. 358-367, November 2010.

[9] T. Isobe and K. Shibutani, "Generic key recovery attack on feistel scheme," in *Proc. Springer 19th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology-ASIACRYPT*, December 2013.

[10] A. R. Kazmi, M. Afzal, M. F. Amjad, and A. Rashdi, "Combining algebraic and side channel attacks on stream ciphers," in *Proc. IEEE International Conference on Communication Technologies (ComTech)*, April 2017.

[11] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993, pp. 11-31.

[12] B. A. Forouzan, *Data Communications and Networking*, 5th ed. 2013, Ch. 19, pp. 562 - 573.

[13] J. N. Laneman and B. P. Dunn, “Communications overhead as the cost of constraints,” *IEEE Information Theory Workshop*, no. 78, pp. 365-369, Oct 2011.

Ayman Yousry El-hadary was born in Cairo 1990. El-Hadary received his B.Sc. in July 2012 from Radar and Communication Department, Military Technical College. El-Hadary’s major field of study is cryptography and security.

He is a master’s student at Arab academy for science and technology and maritime transport. He is working to develop new trends for security of 4G chatting. He developed a new Authenticated Encryption Algorithm and published this work in the military technical college International Conference in Electrical Engineering (ICEENG) with paper title “Design and simulation of new and fast authenticated encryption architecture (AESSEA3)”, April 2018. The author current interest is the cryptography and security field.

Mohamed Helmy Megahed was born in Cairo-Egypt at 23/07/1975. Dr. Megahed received his B.Sc. in July 1997 from Egyptian Military Technical College Communications Department. Dr. Megahed received his master’s in May 2003 from Egyptian Military Technical College in the field of security and cryptography. Dr. Megahed received his PhD from university of Ottawa in 2014.

He invented the unpredictability concept in cryptography to design computationally secure cipher systems and unconditionally secure cipher systems. He was a doctor in Communications Department in the Egyptian Military Technical College. He is currently working at Canadian International College (CIC) in Cairo. His works is focusing on security of communications systems and networks, cryptography, cyber security and embedded systems.

Dr. Mohamed Megahed last work was IEEE paper providing the architecture of Authenticated Encryption One Time Pad Algorithm.

Mohammed Hassan Abd El-Azeem was born in Cairo-Egypt 1962. Prof. AbdEl-Azeem received his B.Sc. in June 1985 from Egyptian Military Technical College Communications Department. Prof. Abd El-Azeem received his master’s in 1993 from Egyptian Military Technical College in the field of microstrip mixers. Prof. Abd El-Azeem received his PhD from University of Kent in 1996.

He is a member in the scientific committee of the International Conference of Electrical Engineering (ICEENG) and the International Conference of Aerospace Science and Aviation Technology (ASAT). He is currently a vice dean for Engineering Faculty and professor in Communication and Electronic Department in Arab Academy for Science, Technology and Maritime Transport (AASTMT) in Cairo. His work is focusing on security of communications systems and networks, security, microstrip technology and antennas.

Prof. Abd El-Azeem’s last work was a paper in IEEE AP-S Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting with a title “Pharaonic Ankh-Key Millimeter Wave Broadband Antenna Design and Fabrication for 5G Applications”.