Defence Science Journal, Vol. 67, No. 3, May 2017, pp. 276-281, DOI : 10.14429/dsj.67.10118

Integrating Non-linear and Linear Diffusion Techniques to Prevent Fault Attacks in Advanced Encryption Standard to Enhance Security of 4G-LTE Networks

Senthilkumar Mathi*, Pavittra Kalyaan, Kanimozhi S., and Bhuvaneshwari S.

Department of Computer Science and Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amrita University Coimbatore - 641 112, India
**E-mail: m_senthil@cb.amrita.edu*

ABSTRACT

Long term evolution based fourth generation (4G) mobile technology has provided a platform for fast and efficient wireless communication. The advanced encryption standard (AES) is one of the three cryptographic algorithms used in 4G networks for encryption of sensitive data. In spite of offering high immunity, AES is still vulnerable to few attacks. This weakness in AES algorithm makes 4G susceptible to several security issues. This paper specifically focuses on fault attacks performed on AES. A fault induced in any one of the rounds of AES helps the attacker to derive information about the secret key. In this manner, these fault attacks pose a serious threat to wireless mobile communication as he or she may gain access to any network that is encrypted with AES. In earlier works, various countermeasures have been suggested to prevent them. However, each of these preventive measures has their own limitations and vulnerabilities. This paper proposes an enhanced method of preventing fault attacks in AES by incorporating a combination of non-linear and linear diffusion techniques. This method identifies if a fault has been injected and diffuses the fault well into the matrix, providing no information about the secret key to the attacker. The performance evaluation proves that the proposed prevention method outperforms the others in terms of time, cost and efficiency.

Keywords: Long term evolution; Fault attack; Diffusion technique; Advanced encryption standard

1. INTRODUCTION

The wireless network systems and the Internet are two basic and crucial systems of present generation networking[1]. The increasing demand for improvement in wireless communication to meet various requirements of mobile multi-media operations for extensive internet browsing, uninterrupted online audio and video streaming, interactive gaming, mobile TV etc., led to standardisation of third generation partnership project[2-3]. The next generation broadband wireless mobile network system standardised as 4G has an architectural design with less network elements, but improves security, speed, reliability, capacity, coverage and performance as a whole[4]. The LTE network architecture comprises of three main components as shown in Fig. 1.

The first component, user equipment (UE), is a mobile equipment (ME). The evolved base stations, called eNodeB (eNB) that control the mobiles in one or more cells are part of the second component, the evolved UMTS terrestrial radio access network (E-UTRAN). The radio communications between the UE and the evolved packet core (EPC) are controlled by E-UTRAN. The third component EPC consists of four entities: Home subscriber server (HSS) that stores details about the network operator's subscribers, mobility management entity (MME) which interacts with HSS to provide authentication for the UE, packet data network gateway (P-GW) that communicates with packet data networks using SGi interface, and serving gateway (S-GW) which is responsible for forwarding data between P-GW and the base station.

In spite of the increased security, 4G network is still open to attacks and has security issues. The trusted and non-trusted locations of 4G architecture are also described in Fig. 1. Cryptographic protection is required in the link that connects eNB to the core network where internet key exchange and the IP security protocol are employed. The eNB is the prime location susceptible to attacks where user traffic is threatened to be exposed. Hence it is necessary that it offers a secure environment for the execution of critical operations, like the encryption or decryption of data and handling key storage for secure user communication. One must also take into account that if an attack is successful on eNB, the attackers gain control of eNB operations, which in turn will affect its signalling to UEs and other nodes.

To ensure protection against such attacks, 4G LTE uses three sets of cryptographic algorithms, as packet system encryption algorithms (EEA) and evolved packet system integrity algorithms (EIA). The first set is 128-EEA1/128-EIA1, based on SNOW 3G algorithms, the second is 128-EEA2/128-EIA2, based on advanced encryption standard

Received : 25 May 2016, Revised : 02 December 2016
Accepted : 11 January 2017, Online published : 24 April 2017

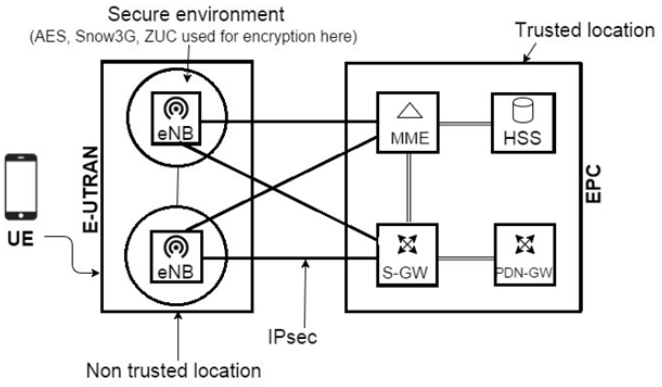

Figure 1. Core network of LTE.

(AES) algorithm and uses 128 bits, 192 bits, or 256 bits with a 128-bit input message, and the third is 128-EEA3/128-EIA3, based on ZUC algorithm. However, these algorithms have their own drawbacks which can compromise the security of the LTE network[5]. Attackers practice and perform cryptanalysis, which is a study of mathematical and algebraic techniques that make use of vulnerabilities in cryptographic algorithms. Some of the attacks such as collision attack, meet-in-the-middle, differential fault attack (DFA) on ZUC and SNOW 3G and particle swarm optimisation attack on AES[6-10] can successfully retrieve the key and crack into the network. Here, diagonal fault attack, a type of DFA, performed on AES is focussed in this paper.

The advanced encryption standard (AES) has been a popular target for fault attacks as it is the global standard for sensitive data encryption. The basic principle of a fault attack is to induce faults into cryptographic implementations to reveal their internal states and hence find the secret key using different fault injection methods which include variation of temperature, clock frequency and supply voltage, clock glitches etc. Moradi[9], *et al.* suggested two fault models that cover all the possible faults on the input of Mix Columns in round 9 of AES-128. Both the models were shown to be successful and have high coverage rates. Subsequently, Dusart[10], *et al.* revealed that AES is sensitive to fault analysis by implementing this attack on a personal computer. The investigation retrieved the full AES-128 key by analysing less than 50 cipher texts.

Subsequently, an execution of a fault attack on AES-128 by injecting a fault in one of the diagonals of the state matrix was examined by Saha[11], *et al*. Here, the diagonal fault attack was introduced by inducing a fault in the 8th round as shown in Fig. 2. After byte sub, shift row and mix column operations of the 8th round, the fault spread to the entire column. By the end of the 9th round, the fault spread to the entire state matrix. However, the bytes of each of the four columns of the matrix show some inter-relations among them, which can be exploited to reduce the key space. After the final i.e. the 10th round, we obtain a faulty cipher text. An exclusive-OR (XOR) operation is performed on the faulty cipher text and a fault-free cipher text, each with the tenth round key matrix and the two results are further applied to XOR to provide us the derived sub-key as shown in Fig. 3.

The key matrix used in tenth round is as follows,

$$K_{10} = \begin{bmatrix} K_{00} & K_{01} & K_{02} & K_{03} \\ K_{10} & K_{11} & K_{12} & K_{13} \\ K_{20} & K_{21} & K_{22} & K_{23} \\ K_{30} & K_{31} & K_{32} & K_{33} \end{bmatrix} K$$

Four sets of equations were derived while considering the fault in the first diagonal of the state matrix b^{11}. The attacker obtains reduced solution spaces for the unknowns K_{00}, K_{13}, K_{22} and K_{31} using the first set of equations as follows,

$$ISB(c1 + K_{00}) + ISB(c1 + T1 + K_{00}) = 2[ISB(c8 + K_{13}) + ISB(c8 + T5 + K_{13})] \quad (1)$$

$$ISB(c8 + K_{13}) + ISB(c8 + T5 + K_{13}) = ISB(c11 + K_{22}) + ISB(c11 + T9 + K_{22}) \quad (2)$$

$$ISB(c14 + K_{31}) + ISB(c14 + T13 + K_{31}) = 2[ISB(c8 + K_{13}) + ISB(c8 + T5 + K_{13})] + [ISB(c8 + K_{13}) + ISB(c8 + T5 + K_{13})] \quad (3)$$

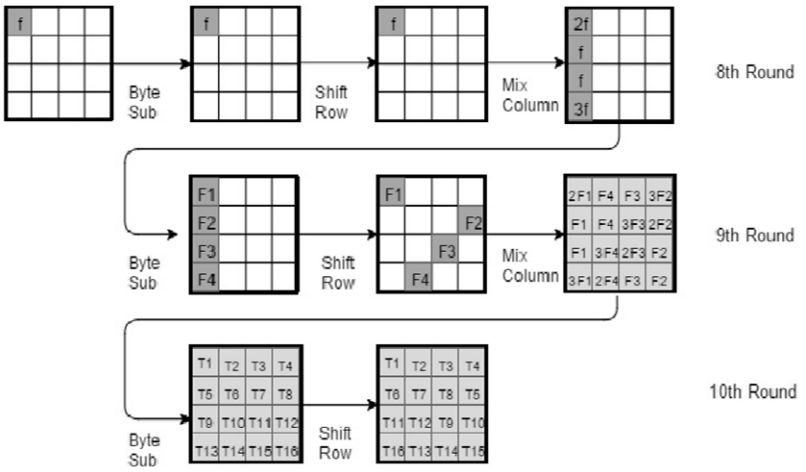

Figure 2. Fault induced in round 8 propagates throughout the matrix in the subsequent rounds.

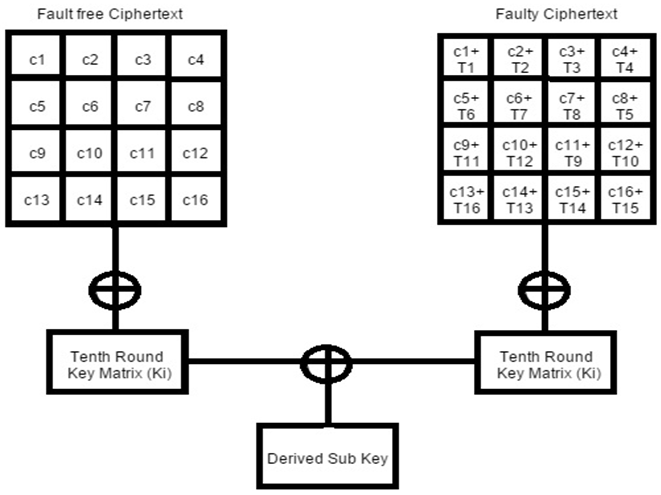

Figure 3. Sub-key derivation from fault-free and faulty cipher text.

Here ISB denotes inverse substitute bytes operation of AES. The unknowns (K_{01}, K_{10}, K_{23}, K_{32}), (K_{02}, K_{11}, K_{20}, K_{33}) and (K_{03}, K_{12}, K_{21}, K_{30}) are obtained by three more similar sets of equations.

Various prevention methods were proposed to increase the security of AES against fault attacks; by adding redundant and dummy rounds as discussed by Gierlichs[12], *et al*. by suggesting randomised infective countermeasures[13]. In this paper, an enhanced preventive countermeasure is proposed by integrating non-linear and linear diffusion techniques to make AES less prone to fault attacks and therefore increasing the protection in the secure environment where AES is used for encryption.

2. RELATED WORK

The introduction of fault attacks has encouraged researchers to explore different ways to prevent them. Preventive measures that make use of infective computation given by Gierlichs[12], *et al.* ensures that if an attacker injects a fault into dummy or redundant round it will not prove useful in obtaining sensitive information on the AES key. Hence it would not be required for AES to perform a check on whether a fault has occurred.

However, the localisation of fault diffusion has proven this method vulnerable, which led Ghosh[13], *et al* to propose a practical solution for DFA using linear diffusion function (LDF) and randomised non-linear mixing function. A linear function that satisfies the strict avalanche criterion is known to have a higher diffusion power. A random mask was introduced with the diffused fault from LDF using some nonlinear function because non-linearity will protect against attackers using algebraic and differential attacks on the linear function. Nevertheless, the hardware setup used for this method is not cost efficient. Also employing LDF increases the number of rounds where diffusion is performed and all these rounds will run every time whether or not a fault has been encountered.

Furthermore, according to Panda[14], *et al*. the AES is more secure if there is a higher number of non-linear operations being performed. Thus they incorporate the two fundamental principles of cryptography: Confusion (nonlinear Cellular Automata rule) and Diffusion (linear Cellular Automata rule) operations. The authors have made use of Periodic Boundary Cellular Automata rules and other non-linear functions that provide permutation and transposition of the state matrix. But the algorithm by Panda et al has come up with an idea to replace AES as such.

Hence, our proposed method suggests on enhancing the current fault attack prevention method in AES by introducing a new function, *DiffuseFault* which is a combination of linear and nonlinear cellular automata rules (achieving efficient diffusion of the fault), performed for subsequent rounds after the fault has been identified. This ensures that the attacker will not be able to retrieve the plain text even if he or she is aware of the fault location as the fault has been sufficiently diffused into the state matrix.

3. PROPOSED METHOD

The prevention method described by Ghosh[13], *et al* assumes two inputs, a faulty cipher text and a fault-free cipher text and then feeds that output to their linear diffusion function. In the case that a fault is not injected, the linear diffusion and randomised mixing functions are called anyway, though not required. Our proposed method does not consider that assumption and detects the fault as soon as it has been injected with the help of redundant rounds. Redundant rounds (every round is repeated with the output of the previous round, in order to check for a disparity in outputs) help to make certain that a fault was not entered into the current round. It is repeated after every round as it is possible that the fault may have been injected in any of the ten rounds of AES. As given in Fig. 4, if the fault has been detected, the resulting output of the current round is fed into a function, *DiffuseFault(),* which with the help of linear cellular automata rules and non-linear functions guarantees that the fault is diffused well into the state matrix.

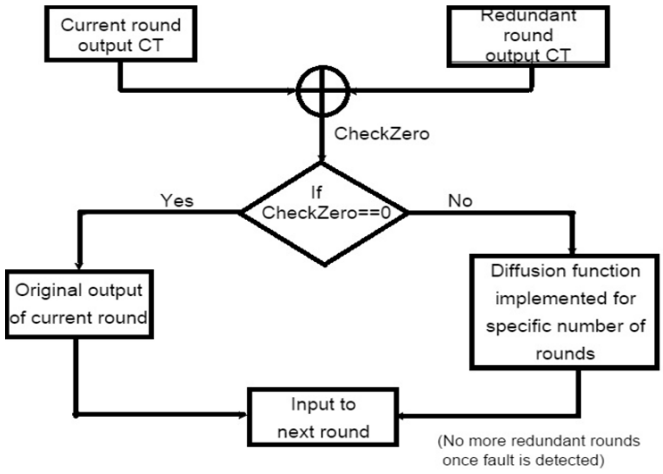

Figure 4. Proposed method: Block diagram.

In contrast to the existing countermeasure, our method also ensures that a fault-free cipher text is not made to enter into any other function, allowing the rounds of AES to proceed as usual.

In the pseudocode given in Fig. 5, when *i* is less than or equal to *n*, normal operations of AES like Sub Bytes, Shift Rows, Mix Columns, Add Round Key take place. However, if the XOR of the outputs of the current round and redundant round inside the *CheckZero* function does not return 0, the program breaks and control is immediately transferred to the *DiffuseFault* function. If the result of *CheckZero* is 0, the

```
Input: Plain Text
Output: Cipher Text
    While i <= n ,          //where i denotes round number
        AES Operations: Sub Bytes1, Shift Rows1, Mix Columns1, Add Round Key1
        CT[i] <- CT1 after current round
        Perform redundant round:  Sub Bytes2, Shift Rows2, Mix Columns2, Add Round Key2
        CTR[i] <- CT2 after redundant round
        CheckZero = CT[i] XOR CTR[i]
        If CheckZero is not Zero,
                DiffuseFault();
        Else,
                Continue;
    End
```

Figure 5. Pseudocode - modification in AES.

program continues normally, executing the next rounds of AES.

DiffuseFault() function

As described by Panda[14], *et al*. a function is said to be linear if it satisfies: $f(x+y)= f(x) +f(y)$ Non-linear functions are those that do not satisfy this property. A variation of the method proposed by Panda[14], *et al*. is employed in the proposed system to bring about the fault diffusion procedure. The linear functions used are periodic boundary cellular automata (PBCA), and 6XOR operation in PBCA. The non-linear functions used are Complement and Substitute Bytes operation. Cellular automata (CA) rules define how the next state of the particular cell value is affected by the current state of its neighbours[15]. In 2D eight neighbourhood CA, the value in the cell is affected by its eight neighbours by eight CA rules, also known as the fundamental rules of CA given in Fig. 6.

64	128	256
32	1	2
16	8	4

Figure 6. Cellular automata rules.

The PBCA is the type of CA where the boundaries of the matrix are connected, which is the second step of the DiffuseFault procedure, as shown in Fig. 7. The diffusion procedure is iterated eight times and finally, the fault diffused cipher text is made visible to the attacker.

```
Function 2: DiffuseFault
Input: integer NumRounds //indicates how many times loop should operate
Ouput: Fault Diffused CipherText
    While i <= NumRounds
        Complement the CT[i]
        Apply Periodic Boundary Cellular Automata Rule 8 on CT[i]
        Perform Periodic Boundary Cellular Automata Rule 8 on Key[i]
        CT[i] XOR Key[i]
        Apply Substitute Bytes
        Apply Periodic Boundary Cellular Automata Rule 128 on CT[i]
        Perform Periodic Boundary Cellular Automata Rule 32 on CT[i]
    End.
```

Figure 7. Pseudocode – *DiffuseFault*().

4. PERFORMANCE EVALUATION

This section describes the performance evaluation of the existing countermeasure and the proposed method.

Linear functions can provide good diffusion property if iterated sufficient number of times. However, using only linear functions would not prove useful as the attacker might be able to use efficient algebraic attacks to recover the key. Hence, the authors[13] have implemented a randomised non-linear mixing function (also iterated specific number of times) that provides some non-linearity in the output cipher text. If the non-linear function is compromised, it would be easier for the attacker to derive the key. Our method combines the properties of both linear and non-linear functions within a single function itself, entangling the key within the cipher text, thereby complicating the relationship between the key, plaintext and cipher text. It does the need for separate functions to perform both operations, and also diffuses the fault effectively and rapidly throughout the state matrix in fewer numbers of rounds as shown in Table 1.

Table 1. Comparison analysis of types of operations

	Countermeasure using fault randomisation[13]	**Proposed method**
No. of iterations of CA in a single round of diffusion function	15	4
No. of non-linear operations in a single round of diffusion function	- (randomised non-linear mixing is performed after linear diffusion function)	3 (Non-linear operations integrated with linear diffusion within same function)
Number of operations in a single round of diffusion function	15	7
Number of rounds required for efficient diffusion	17	8

The total number of rounds required for diffusion of the fault in the existing countermeasure is constant regardless of whether a fault has been injected, or in which round it has been injected. As mentioned earlier, in case of no fault injection, the proposed method allows AES to continue its operations as per usual, with only the inclusion of redundant rounds. This is a significant reduction in the time taken for the prevention mechanism in the case of fault-free cipher text when compared to the existing countermeasure which would call its diffusion and randomised non-linear mixing operations anyway. In the proposed method, the total number of rounds required for prevention also varies with the round in which the fault has been injected, which is not the case in the existing method, as depicted in Fig. 8.

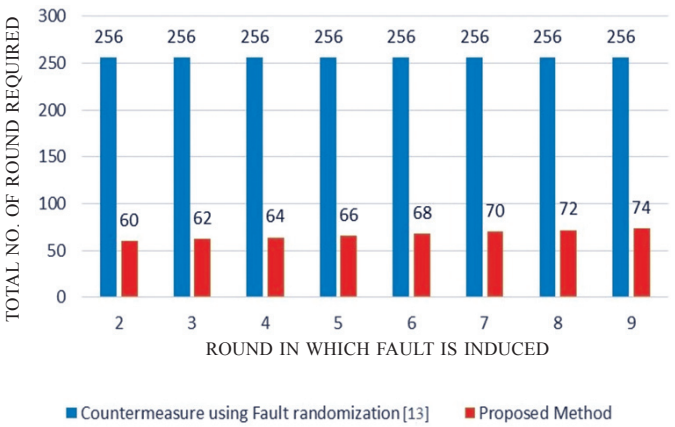

Figure 8. Number of rounds required to spread the fault throughout the matrix.

Though AES is already a combination of linear and non-linear functions, the interrelations among the rows of the matrix have made it vulnerable to fault attacks, as shown in detail in Section 2. However, this specific combination of linear functions that are based on cellular automata rules and non-linear functions ensures that there are no inter-relations among them and hence cannot be exploited to gather information about the key.

The proposed method is a software implementation, developed and executed on a personal computer. Software based encryptions are more prevalent today than hardware based encryptions, as they are more scalable, easy to use and understand, and importantly, are cost effective. The field programmable gate array (FPGA) platform used in[13] is expensive and impractical to be incorporated into AES for wide use. Linear diffusion and fault randomisation involves execution of a loop multiple number of times for many rounds, which would take considerable amount of time. Usage of FPGAs would result in lesser computation time, and as a result, provide better performance for complex operations. However, the proposed method involves the computation of much less number of rounds, as compared to the existing system, and can be easily implemented in software, with the execution times as shown in Table 2.

Table 2. Fault induced in round vs execution time

Fault induced in round number	Execution time (s)
2	0.438
3	0.516
4	0.641
5	1.29
6	1.344
7	1.47
8	1.625
9	1.647

From Fig. 9, it is seen that if the fault is induced in a later round, the algorithm would take more time to execute. This is evident as the algorithm stops its execution and switches control to the prevention operation (*DiffuseFault*) once the fault has been identified.

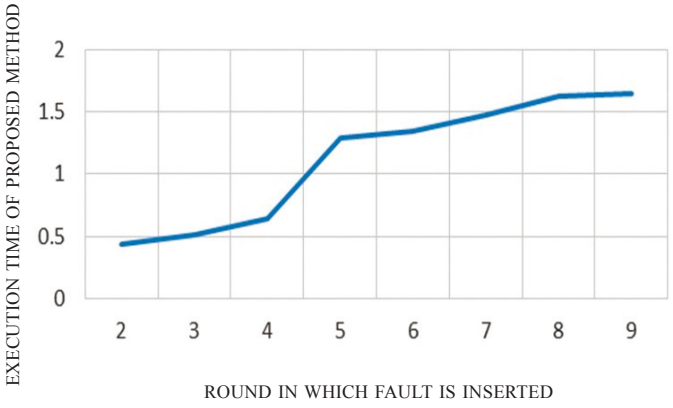

Figure 9. Relation between execution time and the round in which fault is inserted.

These values indicate that execution of AES along with the proposed prevention mechanism is very much feasible in software. It is efficient, consumes less time, with no space overhead. With fewer numbers of rounds used for diffusion and the low price factor, software solutions for preventing fault attacks in AES can certainly be preferred over hardware.

5. CONCLUSION

In this paper, an enhanced method for preventing fault attacks in AES is proposed. As proved in the literature, AES is prone to fault attacks which enable the attacker to obtain the encryption key by injecting faults into its state matrix. Since AES is one of the three main algorithms used to encrypt 4G-LTE networks, it is evident that an attack on AES could compromise the security of the 4G network itself. The proposed method integrates a combination of non-linear and linear diffusion techniques within a single function, which ensures that even if a fault has been injected, it is diffused well into the state matrix, such that an attacker would not be able to recover any information about the secret key. The software implementation of the proposed method is developed and compared with the existing solutions. After analysing the performance, the proposed method proves to be considerably better than the existing methods in terms of time, cost and efficiency.

REFERENCES

1. Mathi, S.K. & Valarmathi, M.L. An efficacious and secure registration for internet protocol mobility. *Def. Sci. J.,* 2013, **63**(5), 502-507. doi: 10.14429/dsj.63.4003
2. Krishnamoorthy, V. & Mathi, S. Security enhancement of handover key management based on media access control address in 4G LTE networks. *In* Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research, 2015, pp.1-5. doi: 10.1109/ICCIC.2015.7435819
3. Cao, J.; Ma, M.; Li, H.; Zhang, Y. & Luo, Z. A survey on security aspects for LTE and LTE-A networks. *Commun. Surv. Tutorials, IEEE*, 2014, **16**(1), 283-302. doi: 10.1109/SURV.2013.041513.00174
4. Dharuman, La. & Mathi, S. A Time-invariant Scheme for handover key management using identity based encryption in 4G LTE networks. *Int. J. Contr. Theor. App*, 2015, **8**(5), 1823-1830.
5. Ghanim, A. & Alshaikhli, I.F.T. Comparative study on 4G/LTE cryptographic algorithms based on different factors. *Int. J. Comput. Sci. Telecommun.*, 2014, **5**(7), 7-10.
6. Ding, L.; Liu, S.K.; Zhang, Z.Y. & Guan, J. Guess and determine attack on zuc based on solving nonlinear equations. *In* Proceedings of the 1st International workshop on ZUC algorithm, 2010.
7. Gilbert, H. & Minier, M. A collisions attack on the 7-rounds Rijndael. *In* AES Candidate Conference, 2000. doi: 10.1.1.476.4952
8. Vimalathithan, R. & Valarmathi, M.L. Cryptanalysis of simplified-AES using particle swarm optimisation. *Def. Sci. J.,* 2012, **62**(2), 117-121.

doi: 10.14429/dsj.62.778

9. Moradi, A.; Shalmani, M.T.M.; & Salmasizadeh, M. A generalized method of differential fault attack against AES cryptosystem. *In* Cryptographic Hardware and Embedded Systems (CHES 2006), Springer Berlin Heidelberg, 2006, 91-100.
10. Dusart, P.; Letourneux, G. & Vivolo, O. Differential fault analysis on AES. *In* Applied Cryptography and Network Security, Springer Berlin Heidelberg, 2003, 293-306. doi: 10.1007/978-3-540-45203-4_23
11. Saha, D.; Mukhopadhyay, D. & Chowdhury, D.R. A diagonal fault attack on the advanced encryption standard. *IACR Cryptology ePrint Archive*, 2009, 581. doi: 10.1.1.215.3853
12. Gierlichs, B.; Schmidt, J.M. & Tunstall, M. Infective computation and dummy rounds: fault protection for block ciphers without check-before-output. *In* Progress in Cryptology–LATINCRYPT*,* Springer Berlin Heidelberg, 2012*,* 305-321. doi: 10.1007/978-3-642-33481-8_17
13. Ghosh, S.; Saha, D.; Sengupta, A. & Chowdhury, D.R. Preventing fault attacks using fault randomisation with a case study on AES. *In* Information Security and Privacy, Springer International Publishing, 2015, 343-355. doi: 10.1007/978-3-319-19962-7_20
14. Panda, S.P.; Sahu, M.; Rout, U.P. & Nanda, S.K. Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography. *Int. J. Commun. Network Security*, 2011, **1**, 18-23.
15. Banik, S. & Bogdanov, A. Cryptanalysis of two fault countermeasure schemes. *In* Proceedings of the International Conference in Cryptology in India. Springer International publishing, 2015. 241-252. doi: 10.1007/978-3-319-26617-6_13

CONTRIBUTORS

Dr Senthilkumar Mathi received his BE (Computer Science and Engineering) from Tamilnadu College of Engineering and ME (Computer Science and Engineering) from Government College of Technology. And PhD (Computer Science and Engineering) from Anna University, Chennai. He is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, India. His current research interests include: Mobile IP, MIPv6, wireless networks, communication security, 4G LTE networks and distributed mobility management.
His contribution in the current study includes, modification of AES and their study.

Ms Pavittra Kalyaan received her BTech (Computer Science and Engineering) Amrita School of Engineering, Coimbatore, India. Her current research interests include: 4G LTE networks, distributed mobility management and information security.
Her contribution in the current study includes, designing of the diffusion function and its implementation in the modified AES.

Ms Kanimozhi S. received her BTech (Computer Science and Engineering) from Amrita School of Engineering, Coimbatore, India. Her current research interests include: 4G LTE networks, wireless networks and communication security.
Her contribution in the current study includes, analyzing of previous methods on preventing fault attacks. The analysis of cellular automata and concluding to periodic boundary cellular automata and complete.

Ms Bhuvaneshwari S. received her BTech (Computer Science and Engineering) from Amrita School of Engineering, Coimbatore, India and currently, pursuing her MTech (Computer Science and Engineering). Her current research interests include: 4G LTE networks, wireless networks and system security.
Her contribution in the current study includes, performance investigation on each stage of the proposed method.