4G Network Security Algorithms: Overview

https://doi.org/10.3991/ijim.v15i16.24175

Rana M. Zaki(✉), Hala Bahjat Abdul wahab
University of Technology, Baghdad, Iraq
110074@uotechnology.edu.iq

Abstract—Long Term Evolution (LTE) of (Universal Mobile Telecommunication System) is one of the modern steps in series of mobile telecommunications systems. That appears to be a strong technology that meets the requirements of fourth-generation (4G) mobile networks and supports authentication and encryption mechanisms between User Equipment (UE) and Message Management Entity (MME). This paper provides an overview of the three most important algorithms that are considered the heart of LTE cryptographic algorithms (SNOW3G, AES, and ZUC) and a comparison between cipher key length and initial vector length to generate keystream depending on the structure used for each algorithm as each algorithm has a time of complexity and space of complexity that differs from the other security algorithm.

Keywords—LTE, cryptography, 4G, authentication, confidentiality, security, SNOW3G, AES, ZUC

1 Introduction

Mobile networks are considered among the technologies of rapid development in “modern communication systems” as the number of subscribers exceeded all expectations, The term “mobile network” refers to a technology that allows for wireless voice and data network communication through radio transmission. Mobile network applications include cell phones, laptops, and tablets. The cell phone is the most well-known application of mobile networking. In the past, wireless communications circuit switching was used to load voice over the network; nowadays, both data and voice are loaded over the network are entities that are sent over both packet and circuit-switched networks. To meet the demand for real-time data transport over open networks, communication security becomes more critical, according to Nodaway [1]. In our new life, we use the Universal Mobile Telecommunication System (UMTIS) [2] for all of our daily interactions and transactions. Long-Term Evolution (LTE) is a term used to describe the process of evolution and the developed standards for LTE are the three-generation and four-generation mobile networks that can mobile transmigrations of internet applications like “voice over IP (VoIP)”, video streaming, mobile TV, music. Long-term evolution (LTE) and LTE-Advanced networks support highly sophisticated authentication and encryption mechanisms.

2 4G network security

The fourth-generation (4G) has many benefits, which can be summarized as follows:

- 1- 4G services must be IP-based, combining elements of mobile, wireless, and fixed networks in a unified, user-friendly architecture.
- 2- For smartphone phones, the target data speeds must be 100 Mbps, and for travelers, 1 Gbps.
- 3- It is essential to fight for a worldwide common spectrum and accessible global standards.

LTE Security's goal is to provide strong protection against various types of Internet threats. Access, confidentiality, and integrity are provided by LTE's protection measures, which include an advanced framework for authentication, authorization, and encryption [3–5], as show Figure (1).

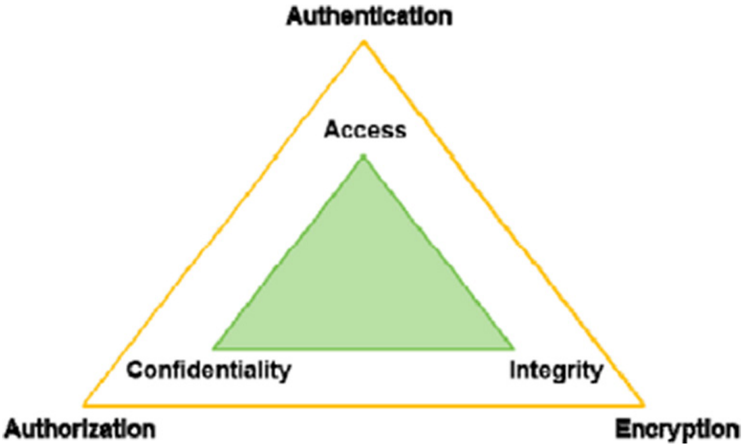

Fig. 1. Security technique in LTE [3]

Authentication and Access: In a typical scenario where A and B interact over a channel, they would both want to begin by introducing themselves. Authentication is the method of determining whether or not they are capable of establishing a relationship.

Authorization and confidentiality: Authorization determines who has access to what form of data and prevents various users from accessing all data.

Encryption and integrity: If all messages sent by Party A are similar to those received by Party B, and vice versa, the message is not modified reroute, and the communication's integrity is maintained, which cannot be accomplished without the use of encryption algorithms [3].

2.1 Stream cipher

The maximum different side between a block cipher and a stream cipher is that the block cipher is the fixed-size cipher of data input. T. On the other hand, the coding stream encodes in bit or byte [5, 6]

- **Block cipher:**

The typical cipher block size is 64 bits, 128 bits, or larger, and the larger the block size has, the secure the data [7, 8].

- **Stream cipher:**

The stream cipher produces the mainstream with a key rather than dealing with block data. Often a basic stream is implementing XOR in plaintext and the results can be used to do encryption [9].

2.2 LFSR and stream cipher

Linear Feedback Shift Registers are applied in many applications of cryptography, however, the main uses generally are in (stream ciphers and (pseudo-random number generators) PRNG). LFSR is used to produce output bit "at a time "to encrypt plaintext bitstream or generate one bit of a (random) number. The cyclic and predictable properties of (LFSR) cause single (LFSR) not to be used for generating a stream cipher. Single LFSR can be easily broken, the big mistake is to use only one LFSR. Therefore, multiple LFSRs can be used together in a parallel design to produce the system for each clock only, one bit is produced as output so internal information is kept [7].

3 4G security algorithms

LTE security algorithm, it can be said that the integrity and confidentiality algorithm are the two powerful flow algorithms that resist many different attacks and have the flexibility to do optimization to get higher performance and higher productivity than previous work Moreover, there are still some weaknesses in the secure algorithm and need improvement. This issue needs more research in the future to resist any new attack on mobile security. LTE such as its ancestry is threatened by several types of attacks like eavesdropping, fraudsters, viruses, and different attacker [7]. The search for a high degree of security continues. Two joint algorithms are as long as to guarantee data confidentiality and integrity by an air interface called" EEA (EPS Encryption Algorithm) and EIA (EPS Integration Algorithm)". These two algorithms were developed for LTE technology [10]. A showed up. The first is 128-EEA1/128-EIA1, which is based on the SNOW 3G algorithms, followed by 128-EEA2/128-EIA2, which is based on the AES algorithm, and finally, 128EEA3/128-EIA3, which is based on ZUC. As a result, this paper aims to perform a review study based on various factors of all basic LTE encryption algorithms such as SNOW 3G, ZUC, and AES to provide higher security [11–15].

3.1 SNOW3G algorithm

During the European Telecommunications Standards Institute (ETSI)/SAGE assessment, "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification" (2006) [13, 16, 17]. SNOW 2.0 has been improved to increase its resistance to forced attacks, and a new architecture, which is at the heart of both the confidentiality and honesty algorithms, UEA2 and UIA2, has been implemented. Because of its reliability when incorporated in smartphones, it allows for high-speed data speeds in mobile phones. SNOW3G is a cipher stream that uses a 128-bit cipher key to create a 32-bit word keystream. (0, *S*1, ..., 15). The second is the FSM layer which consists of three registers (1, 2, and 3) of 32 bits each. Figure (2) shows the detailed structure of "SNOW-3G" flow coding, where represents a monomeric XOR process and ⊞ is an adder arithmetic operator [13, 18].

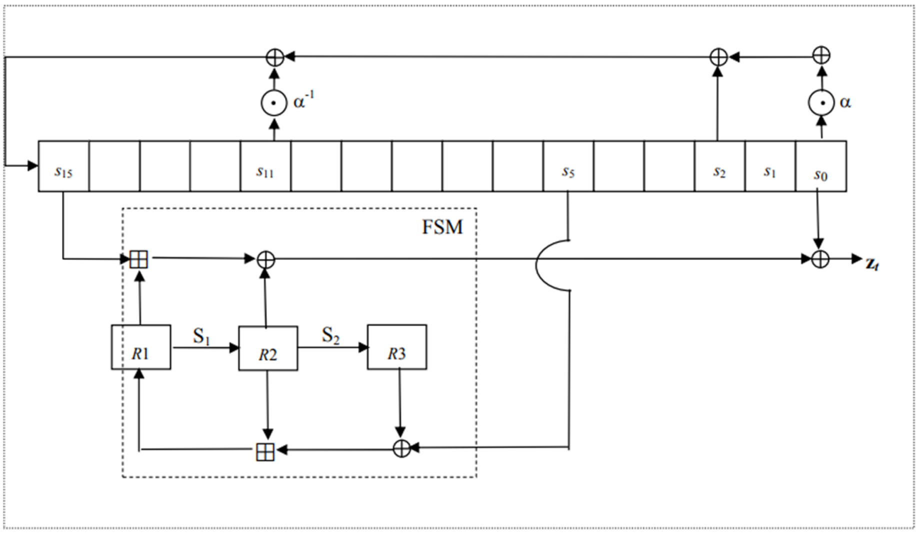

Fig. 2. SNOW 3G Generator [17]

Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang, proposal the Differential Resynchronization Attacks on Reduced Round SNOW $3G^{\oplus}$(**2010**) [19]. In this work exchange the two modulo additions in SNOW 3G by **xors**, to get SNOW $3G^{\oplus}$ [20]. The attacks on SNOW $3G^{\oplus}$ that are known to use IV and selection IV resynchronization. If there is no input from FSM to LFSR, it can attack spot several key/IV order rounds of SNOW $3G^{\oplus}$. The display key recovery attacks on up to 16 rounds of initialization and only a few keystream terms are possible with this input. According to the findings, roughly half of the attack's initialization rounds will detect a large number of key/IV setup rounds [21]. The long-term security margin, however, is significant, and thus these attacks pose no threat to SNOW 3G's security. Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang, proposal Multiset Collision Attacks on miniature-Round SNOW 3G and SNOW, in the same year (2010) [22] in this work showed chosen IV resynchronization attacks on SNOW3G and SNOW $3G^{\oplus}$ show full key-recovery attacks on up to 18 out of 33 initialization rounds of SNOW 3G using a multiset collision idea. The remaining security margin, however, is quite significant and thus these attacks pose no threat to the security of SNOW 3G, as shown in Table 1.

Table 1. $3G^{\oplus}$ result and SNOW 3G result [19]

Cipher	Round	Data	Time	Type
SNOW 3G	13	2^{8}	2^{8}	Distinguisher
SNOW $3G^{\oplus}$	14	2^{8}	2^{8}	Distinguisher
SNOW $3G^{\oplus}$	14	$2^{12.1}$	2^{27}	Full key recovery
SNOW $3G^{\oplus}$	15	$2^{32.1}$	$2^{32.4}$	Partial state recovery
SNOW $3G^{\oplus}$	18	2^{57}	2^{57}	Full key recovery

J. Molina-Gil1, P. Caballero-Gil, C. Caballero-Gil, and Amparo Fuster-Sabater, proposal Analysis and Implementation of the SNOW 3G generators Used in 4G/LTE Systems (2014) [22]. In this work includes theoretical study and practical analysis of SNOW 3G generator, included in this is a standard to protect confidentiality and integrity [23, 24]. By evaluating implementation and performance in mobile devices, many conclusions are obtained on how much to get better their efficiency.

Several studies have been conducted on the iPhone 3GS which are described in Table 2 main characteristics.

Table 2. The device used for the evaluation [22]

iPhone 3GS			
Architecture	CPU Frequency	Cache L1I/L1D/L2	RAM
Armv7-A	600 MHz	16 Kb/16 Kb/256 Kb	256 MB

Muhammad Arif Ali Wasi and Susila Windarta, the proposal "Modified SNOW 3G: Stream cipher algorithm using piecewise linear chaotic map" (2016) [24]. In this paper, the chaos function is used to modify the SNOW 3G stream cipher. Because of its properties including ergodicity, mixing, and sensitivity to initial conditions, the disorder is used in functions [24]. Modified SNOW 3G is supposed to be an asynchronous stream cipher with the addition of the PLCM function at the main initialization mode and a keystream generation mode when using the function, as shown in the Figure. (3). Since this is a basic chaos system that uses simple operations like multiplication, division, addition, and comparison in any chaos digital system iteration, a linear multiple definition function algorithm and a Chaos Map (PLCM) function are used.

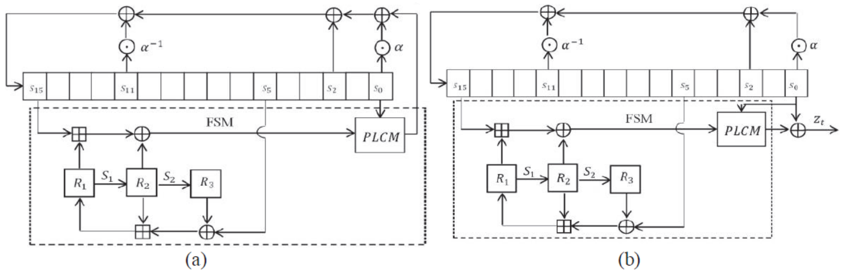

Fig. 3. (a) Modified key initialization method in SNOW 3G
(b) Modified keystream generation method in SNOW 3G [24]

Mahdi Madani, Ilyas Benkhaddra, Camel Tanougast, Salim Chitroub, and Loic Sieler, proposal Digital Implementation of an Improved LTE Stream Cipher Snow-3G Based on Hyperchaotic PRNG(2017) [25]. This work proposed to enhance the SNOW-3G cipher stream [26, 27] by using HCPRNG (Hyperchaotic Pseudo-Random Number Generator). The goal is to improve the complexity and randomness of the normal SNOW-3G encoding stream that is twice its initialization mode resulting in a fail based on the short key flow data set in the NIST test [28–30]. The digital disruption LFSR (Linear Feedback Shift Register) sequences and the digital production of the SNOW-3G uniform cipher element over one hyperchaotic generator used as a PRNG are depicted in figure (4) below to illustrate the proposed architecture (Pseudo- Random Number Generator).

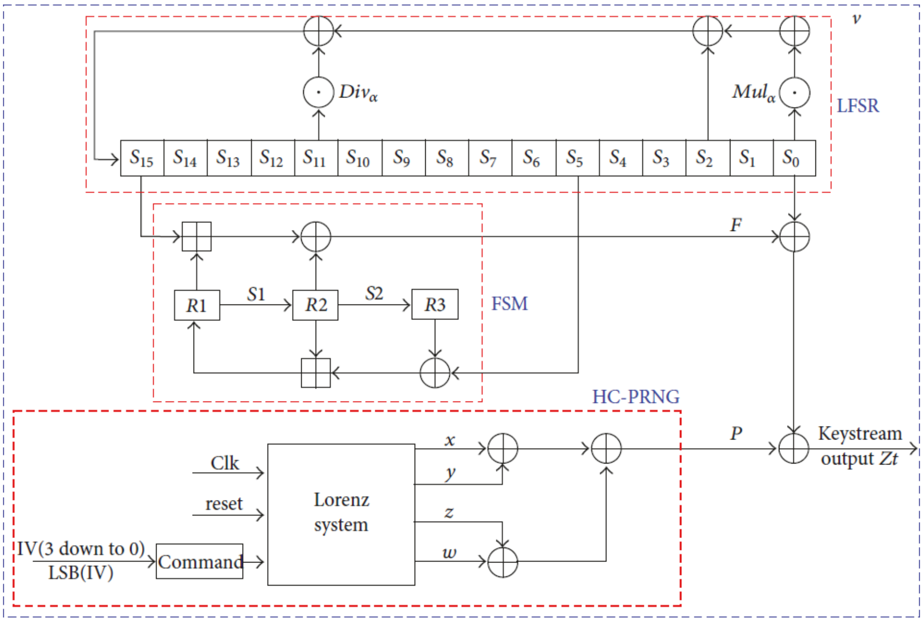

Fig. 4. The keystream architecture of our hyperchaotic SNOW-3G cipher stream method [25]

The results of the security and statistical tests show that the proposed stream cipher is more stable than the commonly used SNOW-3G encryption, assuming it passes all of the tests in this proposal. In this study SNOW-3G, a new hyperchaotic model was proposed. Digital stream encoding architecture that could be used as the foundation for honesty and confidentiality algorithms in UMTS and LTE networks. The proposed port architecture on the Virtex-5 FPGA uses a small amount of logical area while providing 922.88 Mbps throughput. Finally, the technology performs admirably and can be scaled up to 4G security by combining plain text The LTE 128-EEA1 confidentiality algorithm is combined with the EIA1-128 integrity control algorithm. N. B. Hulle, Prathiba B, Sarika R. Khope, K. Anuradha, Yogini Borole, D. Kotambkar, proposal Optimized for SNOW 3G(2021) [15, 30], In this work to progress the showing of the SNOW 3G algorithm. By using the architecture novel Modulo CLA more than 232 to reduce the publishing delay in the Federated States of Micronesia, which makes the decision decisive the algorithm of delay [15, 31–33] and the use of the novel architecture S Box. The offered research work uses two architectures for the achievement of the S-box. The primary architecture is shown in Figure (5) takes up less resource only is advantageous for least frequency application. The secondary architecture shown in Figure (6) consumes fewer resources compared to the standing architectures but requires more resources compared to the Novel S-box-1 architecture.

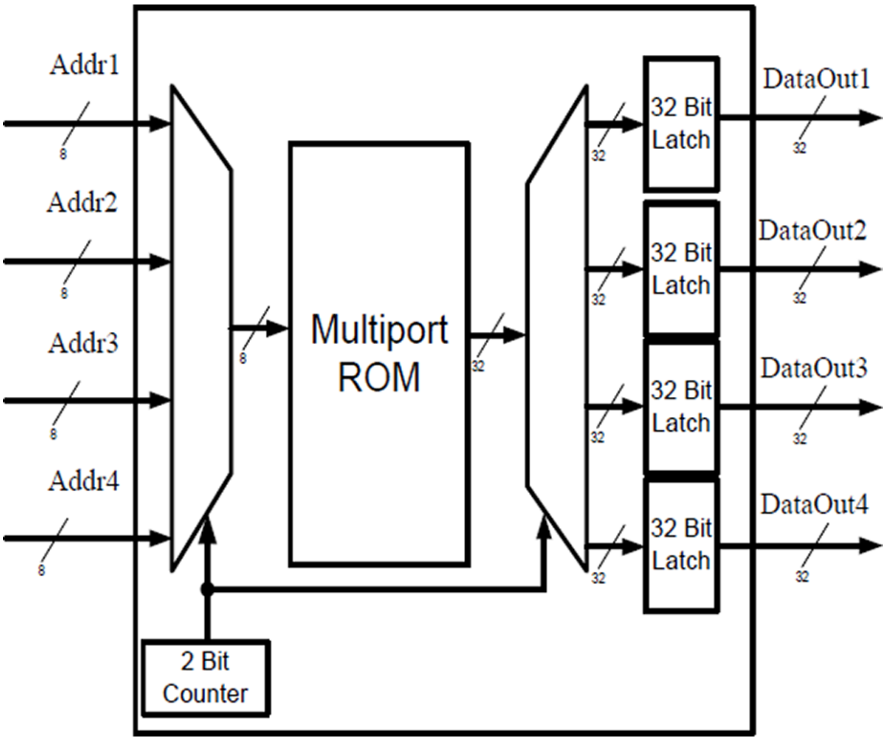

Fig. 5. New S-Box architecture1 [30]

These designs save 6 KB of memory as compared to existing designs. 6KB of memory is provided by Architecture-1 to s-box at the expense of extra hardware (two (4) I/p transmitters, one 2-bit counter, and four 32-bit latches). This architecture is four times slower than conventional architectures, making it suitable for applications with low frequency. The second architecture can be used at both low and high levels of complexity.

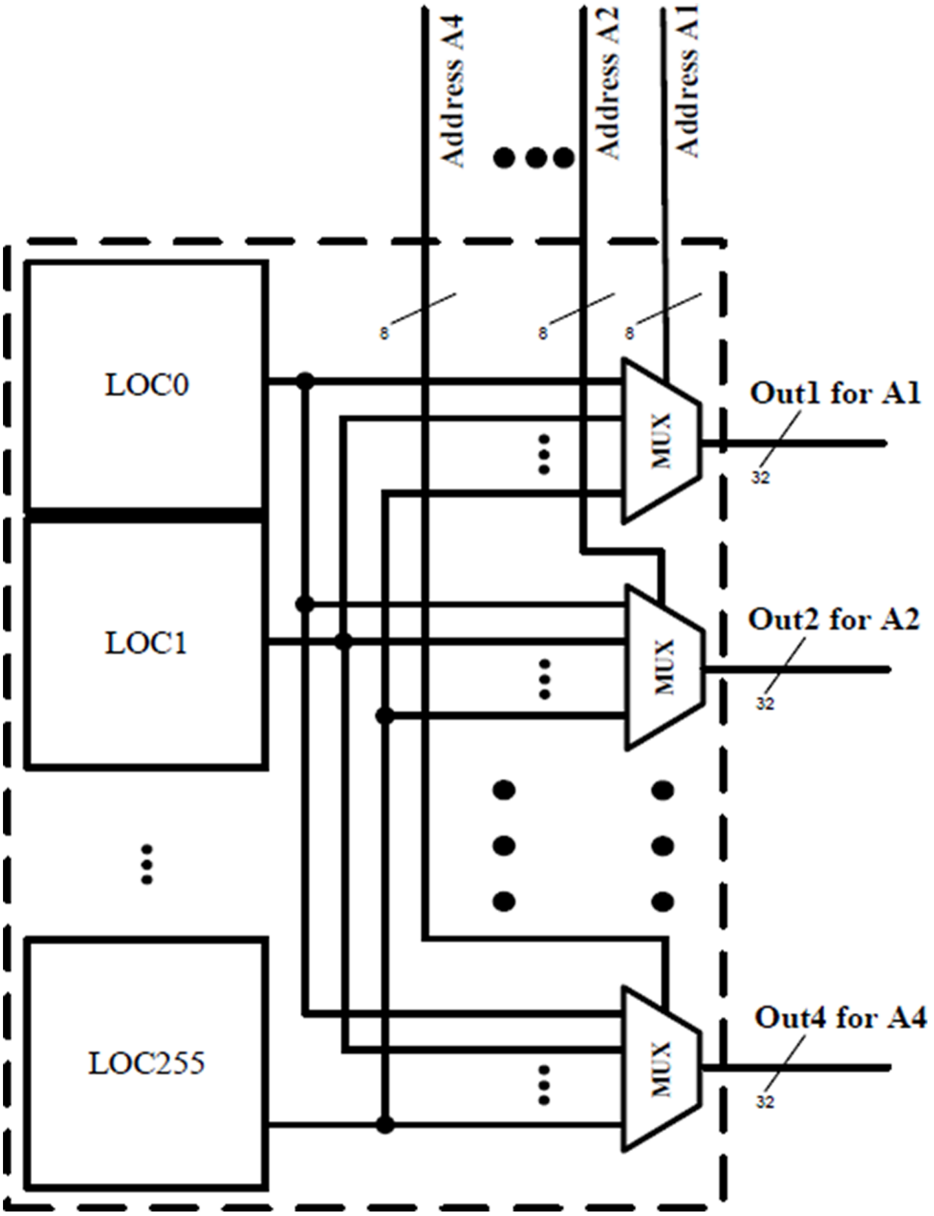

Fig. 6. New S-Box architecture 2 [30]

The optimization of SNOW 3G architecture is designed as shown in Figure (7) using the architecture new CLA and the S-Box architecture.

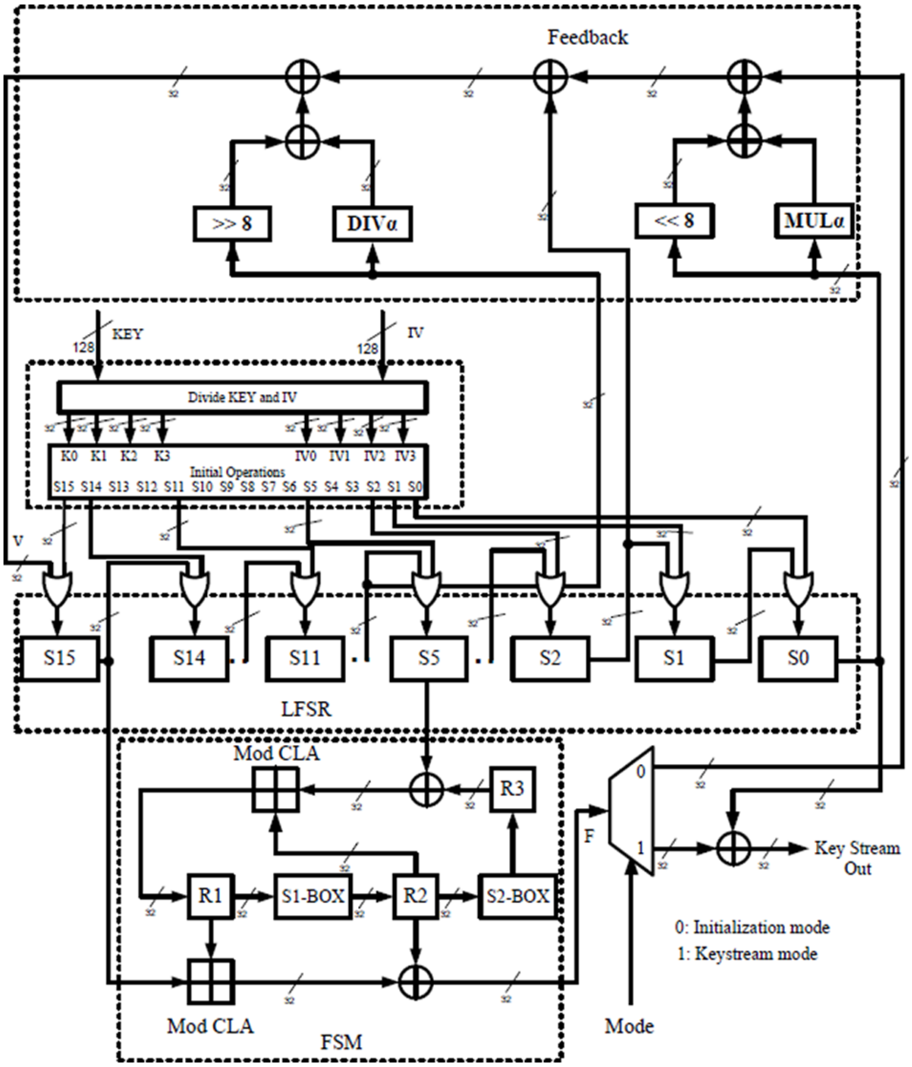

Fig. 7. Optimized SNOW 3G architecture of Internal block diagram [30]

3.2 ZUC algorithm

The "ZUC" cipher stream is used in the output algorithms (128 EEA3 and 128 EIA3), which is named after Zhou Zhongzhi, a famous Chinese historian. ZUC is a stream cipher that is word-oriented [33]. It takes a 128-bit primary key and a 128-bit primary vector as input and outputs a key flow of 32-bit words for usual (encryption and decryption), as shown in Figure (8).

There are two phases in ZUC implementation: the initiation phase and the work phase. In the first phase of the ZUC, it performs the procedure/"IV initialization key", it is registered and ciphered, but no output is generated. The working stage is the second stage, and with each clock pulse, the algorithm generates a 32-bit output word for each loop of the working stage [34].

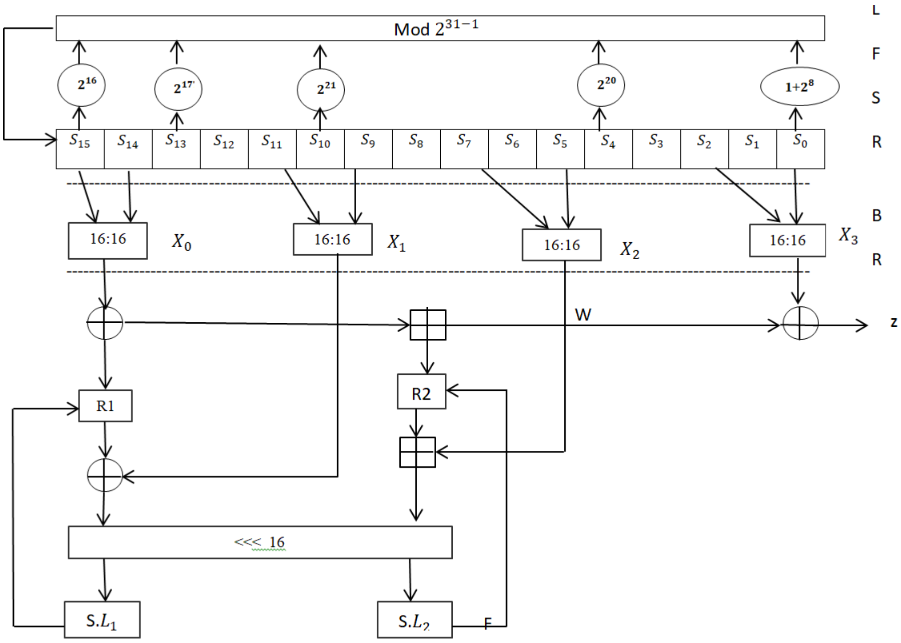

Fig. 8. Architecture by ZUC algorithm [34]

The ZUC specification According [34, 35], There are three logic layers in ZUC. The top layer is a 16-stage linear shift register (LFSR), the middle layer is a bit reorganization procedure (BR), and the bottom layer is a nonlinear function's Faction.

Shri Ramtej Kondamuri, Nitish Kumar Gupta, and Rakesh Sharma, the proposal "Modified EEA3 Algorithm with Improved Throughput Performance" (2014) [35]. In this work in a thorough investigation of the LTE EEA3 confidentiality algorithm based on ZUC flow coding was carried out. The time and space complexity of the EEA3 algorithm are both linear, according to analytical evaluation [36]. Then, a modified coding algorithm is proposed that uses a simple change in the EEA3 algorithm to reduce the space complexity from linear to static. Furthermore, the adjustment encryption algorithm takes less time to encrypt and has better throughput efficiency than the EEA3 algorithm; there is no need to generate L blocks of z. Furthermore, the modified encryption algorithm's defense. Zongbin Liu, Qinglong Zhang, Cunqing Ma, Changting Li, and Jiwu Jing, proposed a High-throughput Pipeline Architecture of ZUC in Hardware (2016) [37]. This work is included in the security file of 3GPP LTE Advanced. The scheme with the highest productivity single carries out the stage of work of the ZUC [38–40]. Schemes realization ZUC fully ability single realize a lot of lower throughput, ago the self-feedback loop in the high path significantly reduces the operating frequency. The design is a two-phase pipeline mixed structure that not only completely implements ZUC, but also greatly increases productivity. FPGAs platform, when compared to newer businesses, the new architecture boosts productivity by 45 percent, particularly since it also saves about 12 percent on hardware resources. The latest design's throughput in 65 nm ASIC technology will hit 80 Gbps, which is 2.7 times faster than the fastest in the literature, and it saves no less than 40% of hardware resources [41–43]. "Dr. R. Latha, Dr. C. Thiripura Sundari, V. Agalya, D. Sandhiya, P. Sankari, proposal Efficient VLSI architecture for 4G cryptoprocessor using MILENAGE and ZUC Algorithm is proposed based on two main cryptographic algorithms: MILENAGE algorithm and ZUC algorithm"(2019) [44]. This work shows that the 4G LTE security architecture encryption processors consist of an on-demand cryptographic algorithm that is set up new design basics. The cipher processor reduces wrapped area and increases speed best other encryption processors. The new design techniques and reviews imposed in building wizard security have proven to be very beneficial. Not only does this proposal obtain higher execution and perfection in the throughput/lag area, but it is also one of the most advanced designs in terms of uniting the S-BOX of a "4G" encryption processor at just one as well as being able to simulate complex operations Left shift bitstream in-circuit ready.

3.3 AES algorithm

NIST recommended standard for encryptions is AES. "4G LTE wireless network uses 128-bit Advanced Encryption Standard (AES) and SNOW3G algorithms" to protect safety [45–48]. Since it has been subjected to closed surveillance In a 4G LTE wireless network, the 128-bit AES algorithm is the preferred choice [49]. In LTE-SAE safe, EEA2 (or EIA2) is used. Many researchers are forced been concerned about combining AES with encryption algorithms [50]. Its ability to be considered a catalyst moreover improvement of AES. "Prerana Choudhari, Vikas Kaul, S K Narayankhedkar, proposal An Enhanced Encryption Algorithm for 4G Networks" (2014) [51], This paper discusses the improved encryption algorithm for 4G networks, as well as its styling and valuation. The S-box modification of the AES algorithm improves the performance, and the complication is increased by using AES in a Round structure. The cipher key transforms a static S-box into a dynamic one. As shown in the diagram, the reverse S-box is also updated (Figure 9). The AWGN channel was used to create a 4G simulation model.

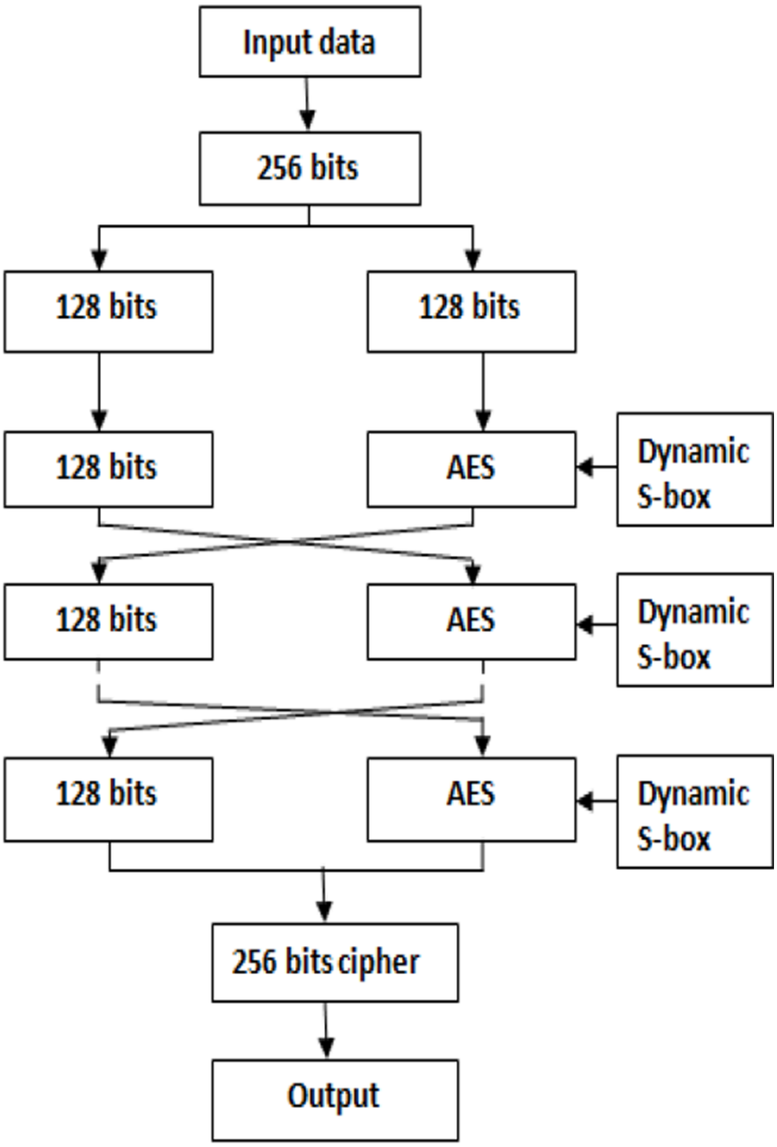

Fig. 9. Dynamic S-box with Round AES [51]

"Vikas Kaula, Bhushan Nemadeb, Dr. Vinayak Bharadic, Dr. S. K. Narayan khedkard, proposal Next Generation Encryption using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks" (2016) [52], This work presents an evaluation of the performance of choice symmetric cipher algorithms. The time spent for optimized AES with clutter and dynamic box in Performance evaluation appears that is roughly the selfsame classic, the AES created is a good alternative to traditional AES, but it adds to the mystery. Although incorporating AES into the round architecture increases uptime for several rounds, it also increases coding complexity. Increased complexity makes the machine less likely to attack [53], and the number of rounds in the hull can be restricting in applications where time is a factor. As result, the encryption key must be highly sensitive for a good encryption scheme to work, and even minor changes in the key cause significant changes in the performance. Change key results in huge blocks of ciphertext or a single bit change in plain text in an improved framework. When the two technologies are compared, the result obtained for AES with dynamic S-BOX is better, and the circuit structure with Dynamic is better.

4 Comparison on the 4G security algorithms

After reviewing the 4G (LTE) cryptographic algorithms which included three algorithms (SNOW3G, AES, and ZUC). These algorithms achieved confidentiality and integrity despite their different implementation of time complexity, space complexity, and data complexity. The constant denotes the best running condition for the algorithm, while the exponential denotes the worst running condition [38]. The values will first show the complexity of LTE-based algorithms, and then slice the complexity of each category provided in Table 3 and Table 4 separately.

Table 3. LTE algorithms to space and time complexity [38]

LTE algorithm	Type	Key Size	Memory Complexity	Time Complexity
SNOW3G	Stream Cipher	128 bits	O(1) Constant	O(n) Linear
AES	Block Cipher	128,192,256	O(1) Constant	O(1) Constant
ZUC	Stream Cipher	128 bits	O(1) Constant	O(n) Linear

Table 4. Comparison of LTE security algorithms

LTE Alg.	Based on	Security Goal	Type	Key Size	Initial Vector	Key Stream	Space Complexity	Time Complexity
EIA1	SNOW3G	Integrity	Stream Cipher	128 bits	128 bits	32 bits	O(n) Linear	O(1) Constant
EEA1	SNOW3G	Confidentiality	Stream Cipher	128 bits	128 bits	32 bits	O(n) Linear	O(n) Linear
EIA2	AES	Integrity	Block Cipher	128 bits	128 bits	128 bits	O(n) Linear	O(n) Linear
EEA2	AES	Confidentiality	Block Cipher	128 bits	128 bits	128 bits	O(n) Linear	O(1) Constant
EIA3	ZUC	Integrity	Stream Cipher	128 bits	128 bits	32 bits	O(n) Linear	O(n) Linear
EEA3	ZUC	Confidentiality	Stream Cipher	128 bits	128 bits	32 bits	O(n) Linear	O(1) constant

5 Conclusion

The most important algorithms that depend on it for the fourth generation (SNOW3G, AES, and ZUC) have been presented, where work has been made on a comparison between them in terms of cipher key length and initial vector length to generate keystream of the time and space complexity, and developments were proposed to them in order to increase security and prevent the attack and provide fast and safe service to users. Work is still in place to develop these algorithms and there are many ideas to provide a fast and safe service in Mobile networks.

6 References

[1] K. E. Mayes and K. Markantonakis, "Mobile communication security controllers an evaluation paper," Information Security Technical Report, vol. 13, no. 3, pp. 173–192, 2008. https://doi.org/10.1016/j.istr.2008.09.004

[2] C. Blanchard, "Security for the third generation (3G) mobile system," Information Security Technical Report, vol. 3, no. 5, pp. 55–65, 2000. https://doi.org/10.1016/S1363-4127(00)03007-7

[3] M. Solanki, S. Salehi, and A. Esmailpour, "LTE security: encryption algorithm enhancements," in 2013 ASEE Northeast Section Conference, 2013.

[4] H. B. A. Wahab and S. F. Amir, "Efficient Digital Watermark key Generation Using Hexagonal Structure and parametric Lagrange Curve," Eng. & Tech. Journal, vol. 33, no. 2, pp. 192–203, 2015.

[5] H. B. A. Wahab and T. A. Jaber, "Using Chebyshev Polynomial and Quadratic Bezier Curve for Secure Information Exchange," Engineering and Technology Journal, vol. 34, no. 5 Part (B) Scientific, 2016.

[6] H. B. A. Wahab, S. M. Kadhem, and E. A. R. Kadhim, "Proposed Approach for Key Generation Based on Elliptic Curve (EC) Algebra and Metaheuristic Algorithms," Engineering and Technology Journal, vol. 32, no. 2 Part (B) Scientific, 2014.

[7] H. Bahjat and M. Ali, "Improvement Majority Function in A5/1 stream cipher Algorithm," Engineering and Technology Journal, vol. 34, no. 1 Part (B) Scientific, 2016.

[8] H. B. A. Wahab and M. A. Mohammed, "Improvement A5/1 encryption algorithm based on sponge techniques," in 2015 World Congress on Information Technology and Computer Applications (WCITCA), 2015: IEEE, pp. 1–5.

[9] H. M. Al-Mashhadi, H. B. Abdul-Wahab, and R. F. Hassan, "Data security protocol for wireless sensor network using chaotic map," International Journal of Computer Science and Information Security, vol. 13, no. 8, p. 80, 2015.

[10] O. A. Dawood, A. M. S. Rahma, and A. M. J. A. Hossen, "The new block cipher design (Tigris Cipher)," International Journal of Computer Network and Information Security, vol. 7, no. 12, p. 10, 2015. https://doi.org/10.5815/ijcnis.2015.12.02

[11] L. Ding, S. Liu, Z. Zhang, and J. Guan, "Guess and determine attack on zuc based on solving nonlinear equations," in Proceedings of the 1st International Workshop on ZUC Algorithm, 2010.

[12] G. Orhanou, S. E. Hajji, Y. Bentaleb, and J. Laassiri, "EPS confidentiality and integrity mechanisms algorithmic approach," arXiv preprint arXiv:1102.5191, 2011.

[13] A.G. Sulaiman and I. F. Al Shaikhli, "Comparative study on 4G/LTE cryptographic algorithms based on different factors," International Journal of Computer Science and Telecommunications, vol. 5, no. 7, pp. 7–10, 2014.

[14] S. Sahmoud, W. Elmasry, and S. Abudalfa, "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher," Int. Arab. J. e Technol., vol. 3, no. 1, pp. 17–26, 2013.

[15] P. Kitsos, G. Selimis, and O. Koufopavlou, "High performance ASIC implementation of the SNOW 3G stream cipher," IFIP/IEEE VLSI-SOC, pp. 13–15, 2008.

[16] S. E. Hajji and G. Orhanou, "Confidentiality in the UMTS radio access network simulation approach under OPNET," in Third International Workshop on Verification and Evaluation of Computer and Communication Systems (VECoS 2009) 3, 2009, pp. 1–11. https://doi.org/10.14236/ewic/VECOS2009.2

[17] P. Ekdahl and T. Johansson, "A new version of the stream cipher SNOW," in International Workshop on Selected Areas in Cryptography, 2002: Springer, pp. 47–61. https://doi.org/10.1007/3-540-36492-7_5

[18] S. Traboulsi, M. Sbeiti, F. Bruns, S. Hessel, and A. Bilgic, "An optimized parallel and energy-efficient implementation of SNOW 3G for LTE mobile devices," in 2010 IEEE 12th International Conference on Communication Technology, 2010: IEEE, pp. 535–538. https://doi.org/10.1109/ICCT.2010.5688900

[19] D. Watanabe, A. Biryukov, and C. De Canniere, "A distinguishing attack of SNOW 2.0 with linear masking method," in International Workshop on Selected Areas in Cryptography, 2003: Springer, pp. 222–233. https://doi.org/10.1007/978-3-540-24654-1_16

[20] K. Nyberg and J. Wallén, "Improved linear distinguishers for SNOW 2.0," in International Workshop on Fast Software Encryption, 2006: Springer, pp. 144–162. https://doi.org/10.1007/11799313_10

[21] A. Biryukov, D. Priemuth-Schmid, and B. Zhang, "Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G$^{\oplus}$," in International Conference on Applied Cryptography and Network Security, 2010: Springer, pp. 139–153. https://doi.org/10.1007/978-3-642-13708-2_9

[22] J. Molina-Gil, P. Caballero-Gil, C. Caballero-Gil, and A. Fúster-Sabater, "Analysis and implementation of the SNOW 3G generator used in 4G/LTE systems," in International Joint Conference SOCO'13-CISIS'13-ICEUTE'13, 2014: Springer, pp. 499–508. https://doi.org/10.1007/978-3-319-01854-6_51

[23] O. Delgado-Mohatar and A. Fúster-Sabater, "Software implementation of linear feedback shift registers over extended fields," in International Joint Conference CISIS'12-ICEUTE' 12-SOCO' 12 Special Sessions, 2013: Springer, pp. 117–126. https://doi.org/10.1007/978-3-642-33018-6_12

[24] M. A. A. Wasi and S. Windarta, "Modified SNOW 3G: Stream cipher algorithm using piecewise linear chaotic map," in AIP Conference Proceedings, 2016, vol. 1707, no. 1: AIP Publishing LLC, p. 050018. https://doi.org/10.1063/1.4940850

[25] M. Madani, I. Benkhaddra, C. Tanougast, S. Chitroub, and L. Sieler, "Digital implementation of an improved LTE stream cipher snow-3G based on hyperchaotic PRNG," Security and Communication Networks, vol. 2017, 2017. https://doi.org/10.1109/CoDIT.2017.8102758

[26] T. Iwata and T. Kohno, "New security proofs for the 3GPP confidentiality and integrity algorithms," in International Workshop on Fast Software Encryption, 2004: Springer, pp. 427–445. https://doi.org/10.1007/978-3-540-25937-4_27

[27] S. Sadoudi, C. Tanougast, M. S. Azzaz, and A. Dandache, "Design and FPGA implementation of a wireless hyperchaotic communication system for secure real-time image transmission," EURASIP Journal on Image and Video Processing, vol. 2013, no. 1, pp. 1–18, 2013. https://doi.org/10.1186/1687-5281-2013-43

[28] D. Talay, "Résolution trajectorielle et analyse numérique des équations différentielles stochastiques," Stochastics: An International Journal of Probability and Stochastic Processes, vol. 9, no. 4, pp. 275–306, 1983. https://doi.org/10.1080/17442508308833257

[29] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, 2001. https://doi.org/10.6028/NIST.SP.800-22

[30] N. Hulle, B. Prathiba, S. R. Khope, K. Anuradha, Y. Borole, and D. Kotambkar, "Optimized architecture for SNOW 3G," International Journal of Electrical and Computer Engineering, vol. 11, no. 1, p. 545, 2021. https://doi.org/10.11591/ijece.v11i1.pp545-557

[31] N. Hulle, R. Kharadkar, and S. Dorle, "High Performance Architecture for LILI-II Stream Cipher," International Journal of Computer Applications, vol. 107, no. 13, pp. 10–13, 2014. https://doi.org/10.5120/18810-0378

[32] M. Madani and C. Tanougast, "Combined and robust SNOW-ZUC algorithm based on chaotic system," in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2018: IEEE, pp. 1–7. https://doi.org/10.1109/CyberSecPODS.2018.8560677

[33] A.N. Bikos and N. Sklavos, "Architecture design of an area efficient high speed crypto processor for 4G LTE," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 729–741, 2016. https://doi.org/10.1109/TDSC.2016.2620437

[34] G. Sulaiman, "Overview of ZUC Algorithm and its Contributions on the Security Success and Vulnerabilities of 4G Mobile Communication," International Journal of Computer Applications, vol. 975, p. 8887, 2017.

[35] S. R. Kondamuri, N. K. Gupta, and R. Sharma, "Modified EEA3 algorithm with improved throughput performance," in 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014: IEEE, pp. 890–894. https://doi.org/10.1109/ICCICCT.2014.6993084

[36] G. Orhanou and S. El-Hajji, "The new lte cryptographic algorithms eea3 and eia3," Appl. Math, vol. 7, no. 6, pp. 2385–2390, 2013. https://doi.org/10.12785/amis/070631

[37] Z. Liu, Q. Zhang, C. Ma, C. Li, and J. Jing, "HPAZ: A high-throughput pipeline architecture of ZUC in hardware," in 2016 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016: IEEE, pp. 269–272. https://doi.org/10.3850/9783981537079_0557

[38] G. Orhanou, S. El Hajji, A. Lakbabi, and Y. Bentaleb, "Analytical evaluation of the stream cipher ZUC," in 2012 International Conference on Multimedia Computing and Systems, 2012: IEEE, pp. 927–930. https://doi.org/10.1109/ICMCS.2012.6320128

[39] S. S. Gupta, A. Chattopadhyay, and A. Khalid, "Designing integrated accelerator for stream ciphers with structural similarities," Cryptography and Communications, vol. 5, no. 1, pp. 19–47, 2013. https://doi.org/10.1007/s12095-012-0074-6

[40] Z. Liu, L. Zhang, J. Jing, and W. Pan, "Efficient pipelined stream cipher ZUC algorithm in FPGA," in First Int'l Workshop on ZUC Algorithm, China, 2010.

[41] M. Al-dabag, H. S. ALRikabi, and R. Al-Nima, "Anticipating Atrial Fibrillation Signal Using Efficient Algorithm," International Journal of Online and Biomedical Engineering (iJOE), vol. 17, no. 2, 2021. https://doi.org/10.3991/ijoe.v17i02.19183

[42] A. S. Hussein, R. S. Khairy, S. M. M. Najeeb, and H. T. ALRikabi, "Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression," International Journal of Interactive Mobile Technologies, vol. 15, no. 5, 2021. https://doi.org/10.3991/ijim.v15i05.17173

[43] H. Naman, N. Hussien, M. Al-dabag, and H. Alrikabi, "Encryption System for Hiding Information Based on Internet of Things," International Journal of Interactive Mobile Technologies, vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[44] R. Latha, E. Suruthi, K. Divya, R. Nithisha, R. Sangeetha, and B. Subalakshmi, "An Efficient 2-Bit Error Compensation with Side Channel Security," International Research Journal in Global Engineering and Sciences, vol. 3, no. 4, pp. 43–51, 2019. http://www.irjges.com/Volume3Issue4/paper7.pdf

[45] A. M. S. Rahma and A. M. Abbas, "A modified Matrices Approach in Advanced Encryption Standard Algorithm," Engineering and Technology Journal, vol. 37, no. 3B, pp. 86–91, 2019.

[46] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, "Designing Substitution Box Based on the 1D Logistic Map Chaotic System," in IOP Conference Series: Materials Science and Engineering, 2021, vol. 1076, no. 1: IOP Publishing, p. 012041. https://doi.org/10.1088/1757-899X/1076/1/012041

[47] J. R. Naif, G. H. Abdul-Majeed, and A. K. Farhan, "Secure IOT system based on chaos-modified lightweight AES," in 2019 International Conference on Advanced Science and Engineering (ICOASE), 2019: IEEE, pp. 1–6. https://doi.org/10.1109/ICOASE.2019.8723807

[48] M. Vishnu, S. K. Tiong, M. Zaini, and S. Koh, "Security enhancement of digital motion image transmission using hybrid AES-DES algorithm," in 2008 14th Asia-Pacific Conference on Communications, 2008: IEEE, pp. 1–5.

[49] N. H. M. A. Al-khafaji, A. M. S. Rahma, A. M. Jaber, and S. Yousef, "Random Key Permutation Stream Algorithm Based on Modified Functions in AES Algorithm," 2014.

[50] A. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," International Journal of Interactive Mobile Technologies, vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[51] V. Kaul and S. Narayankhedkar, "An Enhanced Encryption Algorithm for 4G Networks," International Journal of Engineering Research, vol. 3, no. 6, 2014.

[52] V. Kaul, B. Nemade, and V. Bharadi, "Next Generation Encryption using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks," Procedia Computer Science, vol. 79, pp. 1051–1059, 2016. https://doi.org/10.1016/j.procs.2016.03.133

[53] H. T. AlRikabi, A. H. M. Alaidi, A. S. Abdalrada, and F. T. Abed, "Analysis of the Efficient Energy Prediction for 5G Wireless Communication Technologies," International Journal of Emerging Technologies in Learning, vol. 14, no. 8, 2019. https://doi.org/10.3991/ijet.v14i08.10485

7 Authors

Rana M. Zaki received the BSc and MSc degrees in Computer Sciences in 2003 and 2016, respectively from the University of technology. In 2007 she worked at the Department of Computer Sciences/University of Technology, Baghdad, Iraq, and completed her as an assistant lecturer in 2016. She published five articles in image processing, multimedia, and data encryption. Her research interests are Mobile networks, Encryption algorithms, and cloud computing. (Department Computer Sciences, University of Technology, Baghdad, Iraq). 110074@uotechnology.edu.iq.

Hala Bahjat Abdul Wahab She author became a Reviewer (R) of IEEE in 2010. Was born in Basra, Iraq in 1969. She received the B.S. degree in 1990 in computer science, Basra University, M.S. degree in 2001 in computer science, Technology University, and finally the Ph.D. degree in 2006 in computer science security from the department of computer science, University of Technology, Baghdad, Iraq. She received a professor degree in 2018 from the technical university. From 1991 to 1995, Dr. Hala was a lecturer assistant in the computer science department at the Basra University, Iraq. From 1995 to 2020, Dr. Hala was a lecturer in the computer science department at the Technology University, Iraq. She received the Assistant professor's degree in 2006 and the professor's degree in 2018 from the Technology University. Prof. Hala is the author of more than 65 articles. Prof. Hala research interests include Information and network Security. Prof. Hala is a co-author in the "PGP Protocols and its Applications" book in IN TECH 2012. (Department Computer Sciences, University of Technology, Baghdad, Iraq). 110005@uotechnology.edu.iq

Article submitted 2021-05-03. Resubmitted 2021-06-04. Final acceptance 2021-06-04. Final version published as submitted by the authors