Analysis of Encryption Algorithms Proposed for Data Security in 4G and 5G Generations

Khalid Fadhil Jasim [1*], *Kayhan Zrar* Ghafoor[2,3], *and Halgurd S.* Maghdid [4]

[1] Department of Computer Science, Cihan University-Erbil, Kurdistan Region, Iraq
E-mail: khalid.jassim@cihanuniversity.edu.iq
[2] Department of Computer Science, Knowledge University, Erbil 44001, Iraq, 3 Department of Software Engineering & Informatics, Salahaddin University, Erbil, Iraq
[3] Department of Computer Science, Knowledge University, Erbil 44001, Iraq, Department of Software Engineering & Informatics, Salahaddin University, Erbil, Iraq
[4] Department of Software Engineering, Faculty of Engineering, Koya University, Kurdistan Region-F. R. Iraq

Abstract. This paper intended to investigate and analyze encryption algorithms that can be proposed to perform data security in 4G and 5G networks. The research explores different standards, services, and features presented via 4G and 5G networks. Also, the basic components of encryption algorithms (e.g., ZUC, SNOW 3G, and AES) are investigated. For instance, initialization keys have been identified and analyzed due to their vital roles in determining the security of the encryption algorithms. Moreover, the researchers analyzed the effective elements of these algorithms (i.e., LFSR registers, substitution boxes, NLF functions like finite state machines, Math transformations, secret encryption keys, and non-secret IV keys). Cryptanalysis methods play important roles in determining the security of these algorithms. Thus, some cryptanalysis methods have been explored and investigated. Various weak points have been identified in initialization process of these algorithms. Therefore, different recommendations are presented that enhance the security of these ciphers, and can be reflected in data security in 4G and 5G networks.

1 Introduction

In the previous years, Mobile Communication Networks had various positive impacts on our life and society. Today, most people rely on Mobile devices to perform many activities such as mobile tickets, phone calls, bank transactions, internet access, and parking payment. The new generation of 5G networks supports critical communications, enhanced mobile broadband (eMBB), and used in Internet of Things (IoT) applications [1]. Also, 5G networks offer various services (e.g., Unmanned Aerial Vehicles, communication between cars, data networks using blockchain, and smart networks) [2]. More features are supported by these

* Corresponding author: khalid.jassim@cihanuniversity.edu.iq

networks like audio and video with high clarity, Artificial Intelligence abilities, and high-speed data transmissions. Furthermore, the frequency bandwidth (between 1.8 and 2.6 GHz) and support transmission speeds between (10 and 50 Gbps) [3].

The 4G networks supported mobile broadband internet accessibility. Smart devices and laptops can easily access the Internet networks. 4G networks adopted various standards such as Long-Term Evolution (LTE, as standard technology) and Worldwide Interoperability for Microwave Access (WiMAX) [4]. The 4G-LTE networks supported frequency bandwidth between (1.4 & 20 MHz). In uplink data transmissions, the bit rate (50 Mbps) and the bit rate between (100 & 326.4 Mbps) in downlink data transmissions. The 4G networks with WiMAX standards offered suitable bandwidth (1.25 … 20 MHz), and the bit rate was (40 Mbps, via the fixed stations) [5]. In terms of data security of 4G and 5G networks, various encryption algorithms are proposed to secure data transmissions via smart devices and mobile network base stations. For instance, the proposed encryption algorithms included ZUC cipher, AES cipher, and SNOW 3G cipher [6].

The research is organized as follows. Some standards and features offered in 4G and 5G networks introduced in Section 1. Section 2 provides analysis the components of AES cipher algorithm. Section 3 investigates the elements of SNOW 3G cipher. Section 4 is devoted to analyze the cryptographic elements of ZUC cipher. Section 5 covers the discussion of 4G networks, 5G networks, and the analysis results of the ciphers algorithms (i.e., ZUC, AES, and SNOW 3G). Finally, the conclusions are presented via section 6.

2 Analysis of AES Cipher Algorithm

Advanced Encryption Standard (AES) proposed according to the National Institute of Standards and Technology [7]. The AES-128 cipher contains ten rounds functions, AES-192 with 12 rounds functions, and AES-256 with 14 rounds functions. Each round consists of four mathematical transformations (SubBytes operation, ShiftRows operation, MixColumns, and AddRoundKey operation). The AES-128 cipher algorithm, which operates with counter mode technique (AES-CTR) was proposed as a secure cipher algorithm. This version used in confidentiality and integrity algorithms (EEA2 and EIA2) in 4G and 5G networks [8].In light of cryptanalysis of AES cipher algorithm, the Impossible Differential technique used to analyze the AES-128 and was conducted in [9, 10]. Boura et al. [11] introduced the Improved Impossible Differential technique, and implemented on AES cipher algorithm. This method used to analyze the AES-128 cipher (with 7 from 10 total rounds). The data complexity equal to (2^{105}), time complexity equal to ($2^{106.88}$), and memory complexity equal to (2^{74}).

The initialization phase of AES-CTR cipher algorithm depends on secret encryption key (K, K=128 bits) and counter block (T, T=128 bits) [12]. AES-CTR includes 10 rounds and 4 math transformations (SubBytes, ShiftRows, MixColumns, and AddRoundKey) [13]. In light of the Brute force attack, this cipher algorithm depends on a secret encryption key (K = 128 bits). Thus, Brute force attack requires (2^{128}). It is recommended to increase the lengths of secret key and counter block T, and it is more secure to use encrypted counter block.

3 Analysis of SNOW 3G Cipher Algorithm

The first version of SNOW 3G cipher adopted for data security in (3G-UMTS) [14]. This cipher used in some data security algorithms (e.g., 128-EEA1 and 128-EIA1) as part of 4G-LTE [15]. Moreover, the SNOW 3G cipher algorithm proposed for data security in 5G network [6]. In this context, SNOW 3G requires secret key (K=128 bits), and IV key (IV=128 bits). The first part of SNOW 3G contains LFSR (S0, S1, … S15). The second part is the

finite state machine (FSM). FSM contains Registers (R#1, R#2, and R#3), 2 Substitution Boxes (Sbox(S#1) & Sbox(S#2)) (Figure 1) [16].

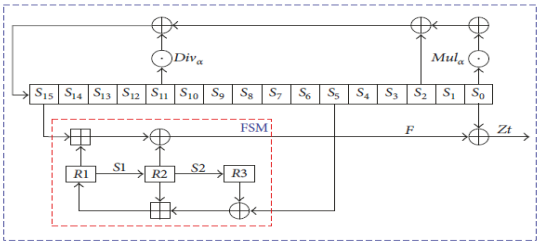

Fig. 1. Design of SNOW 3G Cipher Algorithm

In the cryptanalysis field, the Chosen IV analysis method was conducted to analyze the algorithm of SNOW 3G cipher. The distinguishing attack method applied on (13) steps of SNOW 3G, it requires data complexity (2^8) and time complexity (2^8). In case of applying choosing IV method on (14) steps of SNOW 3G, it needs data complexity (2^{32}) and time complexity (2^{37}) [17]. Also, the vectorized linear approximations used to attack the SNOW 3G. It requires (24 bits) approximation and complexity (2^{172}) [18]. Furthermore, in the initialization phase of SNOW 3G, register (LFSR) loaded with IV key and secret key (K). The key (K= K#0, K#1, K#2, and K#3), IV key (IV=IV#0, IV#1, IV#2, and IV#3). For example, LFSR_S1 = K#1 **XOR** 0xffffffff; … LFSR_S15 = K#3 **XOR** IV#0. After analyzing the initialization steps of SNOW 3G cipher, we identified some weak points. For instance, the length of secret key (128 bits) is less than the length of LFSR (512 bits). The IV key includes (128 bits), the length of IV key is less than LFSR. Also, the IV key is transmitted without protection. It is more secure to use 512 bits for each of secret key and IV key, and encrypt IV key. The complexity of brute force equal to (2^{128}), if we use (512 bits for each of IV and secret key) then brute force increased to (2^{512}).

4 Analysis of ZUC Cipher Algorithm

The 4G-LTE systems used secure data transmissions via some algorithms (128-EEA3 & 128-EIA3 algorithms) [19, 20]. These algorithms designed based on ZUC cipher algorithm [21]. The ZUC needs two keys, which include 128 bits of the secret encryption key (K) and 128 bits of the Initialization Vector key (IV key). The first component of ZUC is register LFSR (S#0, S#1, … S#15). The second is Bit Reorganization (BR) (Words: X#0, X#1, X#2, and X#3). The third is nonlinear function (NLF). The NLF contains Registers R#1 & R#2, substitution boxes S-box S#0 & S-box S#1 [22].

In terms of cryptanalysis, the differential cryptanalysis method was adopted to analyze the components of ZUC algorithm. For instance, the attack focuses on the difference in values of the first byte of IV key (IV#0). To recover the secret key, the attacker explores keyspace with complexity ($2^{30.4}$) [23]. A spectral analysis method developed to attack the ZUC cipher algorithm (i.e., Version of ZUC with 256 bits). This method relied on distinguishing attacks with complexity value equal to (2^{23}) [24]. Iinitialization process of ZUC algorithm (Fig. 2) [25], includes loading register LFSR with bytes from (Secret Key: K#0, K#1, …, K#15), constant bytes (d[16]: d#0, d#1, …, d#15), and bytes from (IV key:IV#0, IV#1,…, IV#15). For example initialization process includes, LFSR_S0 = (K#0 ‖ d#0 ‖ IV#0); … LFSR_S15 = (K#15 ‖ d#15 ‖ IV#15); Where (‖: denotes concatenation).

Analysis of initialization process revealed some weak points. For instance, IV keys are transferred without protection. It is recommended to transfer encrypted bytes of IV keys. The

constant values of (d[16], e.g. do= 0x44D7) used in this algorithm. It is recommended to use variable values of (d[16]). ZUC algorithm relies on secret key (128 bits), and LFSR requires 496 bits, which means secret key bits cannot cover LFSR. Complexity of brute force attack decreased from (2^{496}) to (2^{128}).

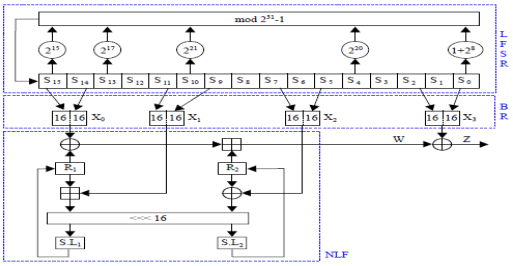

Fig. 2. ZUC Cipher Algorithm

5 Discussion

The encryption algorithms offer suitable level of data security in many applications. For instance, some encryption algorithms (e.g. RSA Enc., DES, Triple DES, and SHA256) have been used for data security in Software-Defined Network (SDN) [26]. Also, some encryption algorithms (e.g. AES, RC6, Twofish, SPECK, and chacha20) have been used for data security in Internet of Things devices (IoT devices) [27]. In this paper we focused on the encryption algorithms used in data security of 4G and 5G networks. The 4G systems (Table 1) supported Internet Accessing with Mobile Broadband networks, facilitated the connection of smart devices with Internet resources, and designed with two rigid standards (WiMAX and LTE). The 5G systems (Table 1) offered more features and relied on advanced standards. In this context, research groups focused on Dynamic Adhoc Net (DAWN), support Voice calls through IP connections (VOIP), and enhance the worldwide wireless web (wwww).

Table 1. Some Features of 4G and 5G Generations.

Mobile Technology	Features of Mobile Generations
Mobile(4G)	- Presented faster mobile broadband - Increased data capacity -Supported wider channel bandwidths (up to 20 MHz with OFDMA technique) - Offered data rates (200 Mbps, 1 Gbps in future) - Adopted multiple antenna technologies - Mobile WiMAX and LTE standards have been adopted as 4G Technology.
Mobile(5G)	- Focused on improving worldwide wireless web (wwww) - Provide voice services via IP (VOIP) - Dynamic Adhoc Net (DAWN) - Data rates (10 Gbps) - Core network (Internet), switching (All packet).

AES-CTR, this cipher depends on input and output with 128 bits. The algorithm relies on secret key K (128 bits) and IV key (128 bits). The complexity of exhaustive search of secret key is (2^{128}) (Table 2). SNOW 3G, this algorithm requires secret key (K= 128 bits) and IV key(128 bits). An exhaustive search for secret key (2^{128}) (Table 2). ZUC, the ZUC algorithm requires two types of keys (i.e., secret key K = 128 bits and non-secret IV key = 128 bits). The hacking operation of these keys requires complexity equal (2^{128}) for each of the mentioned keys. The design includes register LFSR [496 bits], BR [128 bits], and function NLF which including two registers and 2 S-boxes (Table 2). The three ciphers (i.e., AES-CTR block

cipher, SNOW 3G, and ZUC stream ciphers) can be used to perform the data security in 4G-LTE and 5G generations systems.

Table 2. Symmetric Ciphers AES-CTR, SNOW 3G, and ZUC.

	Symmetric Ciphers		
	AES-CTR	SNOW 3G	ZUC
Cipher System	128-bit Block Cipher work in Stream mode	32-bit Word Oriented Stream Cipher	32-bit Word Oriented Stream Cipher
Secret Key	K=128-bit	K=128-bit	K=128-bit
IV Key	IV=128-bit	IV=128-bit	IV=128-bit
Complexity Of Initial Keys	Complexity(K)=2^{128} Complexity(IV)= 2^{128}	Complexity(K)=2^{128} Complexity(IV)= 2^{128}	Complexity(K)=2^{128} Complexity(IV)= 2^{128}
Keystream	128-bit Block	32-bit Word stream	32-bit Word stream
Period of Keystream	2^{64} - 1 Where T0=64-bit	2^{512} - 1 Where LFSR=512-bit	2^{496} - 1, LFSR=496-bit
Structure of Cipher Algorithm	-Bytes Substitution (8-bit S-boxes), -Shift Rows(Byte Permutation.), -Mix Columns (Linear Transform) -Add Round Key	-LFSR (S0,…, S15), -FSM(32-bit registers R1, R2, R3), and -Substitution Boxes (S1,S2)	-LFSR (16 cells), -Bit-Reorganization (128 bits), -Nonlinear Function F(32-bit memory cells R1 and R2), -S-boxes S0 and S1
No. of Rounds	10 rounds	33-steps to produce keystream	33-steps to produce keystream
Cryptanalysis Method	Improved Impossible Differential Cryptanalysis	Chosen IV Cryptanalysis	Differential Cryptanalysis
Mobile Generations	Proposed for security of: 4G-LTE and 5G	Proposed for security of: 4G-LTE and 5G	Proposed for security of: 4G-LTE and 5G

6 Conclusion

This research investigated some features presented in 4G and 5G systems. The 4G networks introduced Access to Internet resources based on Mobile Broadband, employed LTE and WiMAX standards. The design of 5G networks focused on Dynamic Adhoc Net (DAWN), Voice calls based on IP (VOIP) and worldwide wireless web (wwww). Some cipher algorithms like ZUC, AES-CTR, and SNOW 3G were presented to perform the data security in 4G and 5G networks. These ciphers possessed some characteristics. For instance, AES-CTR depends on ten rounds, 128 bits input block, and 4 math transformations. This cipher adopting secret key (128 bits). SNOW 3G algorithm employing IV and K keys. The design including LFSR register and FSM part. Brute force attack in SNOW 3G requires complexity (2^{128}). ZUC algorithm requiring IV key and secret K key. ZUC involving LFSR, BR, and function NLF. Brute force attack minimized to (2^{128}) instead of (2^{496}). For the three cipher algorithms, It is recommended to maximize the bits of initialization keys, employing encrypted forms of IV keys, and adopting dynamic variable elements of (d []) in ZUC cipher. These improvements can enhance the security of these ciphers.

References

1. Yang, J., Johansson, T., An overview of cryptographic primitives for possible use in 5G and beyond. Sci. China Inf. Sci. 63, 220301 (2020). https://doi.org/10.1007/s11432-019-2907-4
2. M. Amine, L. Maglaras, A. Argyriou, and D. Kosmanos, Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes, *J. Netw. Comput. Appl.*, vol. 101, no. November, pp. 55–82, 2018.
3. M. I. Baba, N. Nafees, I. Manzoor, K. A. Naik, and S. Ahmed, Evolution of Mobile Wireless Communication Systems from 1G to 5G: A Comparative Analysis, IJSRCSEIT,vol. 4, no. 1, pp. 1–8, 2018.
4. E. Ezhilarasan and M.Dinakaran, A Review on mobile technologies: 3G , 4G and 5G, Second International Conference on Recent Trends and Challenges in Computational Models, 2017. DOI 10.1109/ICRTCCM.2017.90
5. G. S. Nitesh and A. Kakkar, Generations of Mobile Communication, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 3, pp. 320–324, 2016.

6. S. Atapoor, Security for 4G and 5G Cellular Networks , Report for the Course Research Seminar in Cryptography (MTAT.07.022), Institute of Computer Science, University of Tartu, 2018.
7. NIST. , ADVANCED ENCRYPTION STANDARD (AES), 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
8. M. Khan and V. Niemi, AES and SNOW 3G are Feasible Choices for a 5G Phone From Energy Perspective, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 211. Springer, Cham, 2018.
9. J. Lu, O. Dunkelman, N. Keller, and J. Kim, New Impossible Differential Attacks on AES, In: INDOCRYPT'08. LNCS, vol. 5365, pp. 279-293. Springer (2008).
10. H. Mala, M. Dakhilalian, V. Rijmen, and M. Modarres-hashemi, Improved Impossible Differential Cryptanalysis of 7-Round AES-128, In: INDOCRYPT'10. LNCS, vol. 6498, pp. 282-291. Springer (2010).
11. C. Boura, V. Lallemand, M. Naya-Plasencia, and V. Suder, Making the Impossible Possible. Journal of Cryptology, Volume 31, Issue 1, pp. 101-133, January 2018.
12. J. Park and D. Lee, FACE: Fast AES CTR mode Encryption Techniques based on the Reuse of Repetitive Data, *TCHES*, vol. 2018, no. 3, pp. 469-499, Aug. 2018.
13. G. Orhanou, S. E. L. Hajji, Y. Bentaleb, and J. Laassiri, EPS Confidentiality and Integrity mechanisms Algorithmic Approach, International Journal of Computer Science Issues, vol. 7, no. 4, 2010.
14. Specification of 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Doc.2: SNOW 3G specification, Tech. Specification TS 35.216 V12.0.0, 3GPP, 2014.
15. Specification of 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Doc.1: UEA2 and UIA2 specifications, Technical Specification TS 35.215 V12.0.0, 3GPP, 2014.
16. 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, Hindawi Security and Communication Networks, vol. 2017, 2017.
17. A. Biryukov, Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G, LNCS 6123, pp. 139–153, 2010.
18. Yang J, Thomas J, Alexander M., Vectorized linear approximations for attacks on SNOW 3G, In: Proceedings of the 27th Annual Fast Software Encryption Conference, 2020.
19. ETSI / SAGE, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3 . Document 1: 128-EEA3 and 128-EIA3 Specification, pp. 1–16, 2011.
20. ETSI/SAGE, Specification. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification, Version: 1.6, pp. 1–18, 2011.
21. S. Lawange and M. Narnaware, Review on LTE Cryptography Algorithm ZUC and its Attacks, International Journal of Emerging Research in Management &Technology, vol. 6, Issue 7, 2017.
22. F. Nilofer and J. Qaddour, Comparative Study of Vulnerabilities in LTE Cryptographic Algorithm, International Journal of Computer Applications, vol. 180, no. 25, pp. 19–25, 2018.
23. H. Wu, T. Huang, P. H. Nguyen, H. Wang, and S. Ling, Differential Attacks Against Stream Cipher ZUC, in *Advances in Cryptology -- ASIACRYPT 2012*, pp. 262–277, 2012.
24. Yang J, Thomas J, Alexander M., Spectral analysis of ZUC-256, In: Proceedings of the 27th Annual Fast Software Encryption Conference, 2020.
25. M. Madani and C. Tanougast, Combined and Robust SNOW-ZUC Algorithm Based on Chaotic System, *2018 Int. Conf. Cyber Secur. Prot. Digit. Serv. (Cyber Secur.)*, pp. 1–7, 2018.
26. I. Aziz and I. Abdulqadder, An Overview on SDN and NFV Security Orchestration in Cloud Network Environment, *cuesj*, vol. 5, no. 1, pp. 20-27, Jun. 2021.
27. K. Jasim, R. Ismail, A. Nahi Al-Rabeeah, and S. Solaimanzadeh, Analysis the Structures of Some Symmetric Cipher Algorithms Suitable for the Security of IoT Devices, *cuesj*, vol. 5, no. 2, pp. 13-19, Sep. 2021.