ISSN 2047-3338

Comparative Study on 4G/LTE Cryptographic Algorithms Based on Different Factors

Alyaa Ghanim Sulaiman[1] and Imad Fakhri Al Shaikhli[2]

[1]Department of Information System KICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Department of Computer Science KICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[1]aliaghanimm@gmail.com, [2]imadf@iium.edu.my

***Abstract*– Recently, (LTE) Long Term Evolution appeared as a robust technology to meet (4G) Fourth Generation cellular networks requirements. Apparently, there are three sets of cryptographic algorithms that work on LTE technology and each set based on core algorithm. Therefore, in this paper we are focusing on reviewing the three sets of the LTE cryptographic algorithms and their core algorithms and then comparing them based on different factors in order to understand their cons and pros and provide valuable information about LTE security.**

***Index Terms*– LTE, 4G, Cryptography and Algorithm**

I. INTRODUCTION

IN order to improve mobile communication services as well as security, LTE (Long Term Evolution) technology emerged to overcome many challenges that stand behind the previous network technology. This new technology has competitive advantages that make it one of the newest and most modern technologies in mobile Network technology.

Apparently, LTE is a long term evolution standard of Universal Mobile telecommunications system (UMTS) cellular technology. The first initiation of LTE in 2004 by 3GPP (Third Generation Partnership Project), but the commercial services of LTE launched in 2010.In fact, nowadays, LTE is considered to be the latest standard technology used in a mobile network whose the number of subscriber passed 85 percent of all subscriber worldwide. Based on GSA information in 2013, 244 operators were commercially launched LTE services in 92 countries. Furthermore, LTE (Long Term Evolution) is defined as a global standard for the fourth generation (4G) of mobile broadband where it introduced in 3GPP Release 8 as an essential step to the next generation in mobile radio communications. Particularly, based on Per Beming (2007), LTE supports users with a high experience and also offers a huge number of demanding applications such as interactive TV, video generator programs, and professional services and games [1].

Statistically, it is noticed that in 2010 LTE reached 612,000 users and then it grew to 13.2 million subscribers worldwide in 2011.By 2012, it rocketed to 100 million and it is estimated that by 2016, it is going to reach one billion users [15]. From these forecasts, it can be realized the importance of offering very powerful security for LTE technology which has been emerged to offer more capacity and speed over the mobile network to serve an enormous growth in mobile data and the number of users. Furthermore, LTE is a packet based system containing less network elements and recently LTE-A (LTE advance) appeared as an evolution of LTE system developed by 3GPP to meet the expectations of the next generation by supporting higher data usage, very low latency and enhanced the spectral efficiency. Both LTE & LTE-A technologies sustain a flat IP connectivity which works in heterogeneous wireless access network.

Therefore, LTE like its predecessors is threatened by different kinds of attacks such as imposters, eavesdroppers, viruses and other attackers. Searching on providing high security is continuous. Two standardized algorithms are provided to ensure data integrity and confidentiality protection via air interface named as EEA (EPS Encryption Algorithm) and EIA (EPS Integrity Algorithm). Those two algorithms have been developed for LTE technology. The first set appeared is 128-EEA1/128-EIA1 which is based on SNOW 3G algorithm, the second is 128-EEA2/128-EIA2 which is based on AES algorithm and the third is 128-EEA3/128-EIA3 which is based on ZUC algorithm. Therefore, this paper aims to make comparative study among all core LTE cryptographic algorithms such as ZUC, SNOW 3G and AES based on different factors toward providing higher security level and supply valuable information to support LTE security.

II. OVERVIEW ON THE THREE SETS OF LTE CRYPTOGRAPHIC ALGORITHMS

The (128-EEA1 and 128-EIA1) are announced by 3GPP (3rd Generation Partnership Project) to be the first set of cryptographic algorithms which are based on SNOW 3G in producing the keystream. The first one is, 128-EEA1 also called UEA2 which supports user confidentiality and signaling data in (LTE/SAE)-(Long Term Evolution- Service Architecture Evolution).The main usage of the first algorithm is to do encryption and decryption to a block of data ranged between 1 and 2^{32} bits in length under a confidentiality key CK. The second algorithm is the 128-EIA1 (EPS encryption algorithm) also known as UIA2 (UMTS Integrity Algorithm) used for integrity of data for LTE and used to account a 32-bit MAC-(Message Authentication Code) value of a plain text under using an integrity key IK. Apparently, the set 1 which includes (128-EIA1/128-EEA1), are stream cipher algorithms used SNOW 3G as its core also named UIA2& UEA2 in UMTS network. This set has been used since 2006 in the UMTS network and then elected to use as a first set of algorithms in the LTE-SAE network. [7][13]

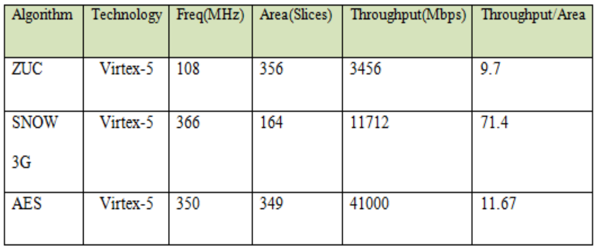
The second confidentiality and integrity algorithm set is denoted as (128-EEA2 /128-EIA2). The first portion is used for ensuring the confidentiality which is a stream cipher algorithm basing on the block cipher of 128-bit (AES) algorithm in CTR (Counter mode). The second portion is used for ensuring integrity and also based on AES but in the CMAC (Cipher-based MAC) mode. AES-CTR has many attractive advantages that encrypt with a high speed. Thereafter, the 3GPP SA3 was modified to the necessity to produce a new set of encryption and integrity algorithm which is known as (128-EEA3/128-EIA3). Furthermore, the new set is designed in China and based on ZUC algorithm, its name refers to the famous Chinese scientist in the history his name is Zu Chongzhi. The first algorithm is 128-EEA3, which is used in the encryption process in the LTE technology and the second algorithm is 128-EIA3 which used for integrity in the LTE technology destined as a universal Hash Function used ZUC as its kernel [14].

III. EVALUATING LTE’S CORE ALGORITHMS BASED ON DIFFERENT PERSPECTIVES

A) *Evaluating the performance of LTE’s core algorithms in hardware platform*

After implementing the LTE cryptographic algorithms in FPGA (Field Programmable Gate Array) hardware platform which is more suitable for 4G era to ensure security of wireless communication, according to Lingchen Zhang and et al. (2012), the results of implementing SNOW 3G and ZUC in Xilinx’s Virtex-5 FPGA as evaluation devices showed that the SNOW 3G performs higher throughput than ZUC and consumed less resources than ZUC as shown in Table (1) [20]. Additionally, both SNOW3G and ZUC are flexible in balancing different throughput with the consumed area.

Table 1: Comparison on the performance of LTE cryptographic core algorithms on FPGA hardware platform [5], [20]

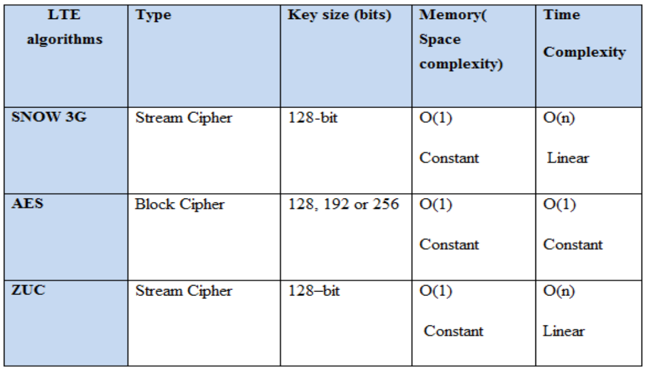


Algorithm	Technology	Freq(MHz)	Area(Slices)	Throughput(Mbps)	Throughput/Area
ZUC	Virtex-5	108	356	3456	9.7
SNOW 3G	Virtex-5	366	164	11712	71.4
AES	Virtex-5	350	349	41000	11.67

B) *Evaluating LTE’s core algorithms from security perspective*

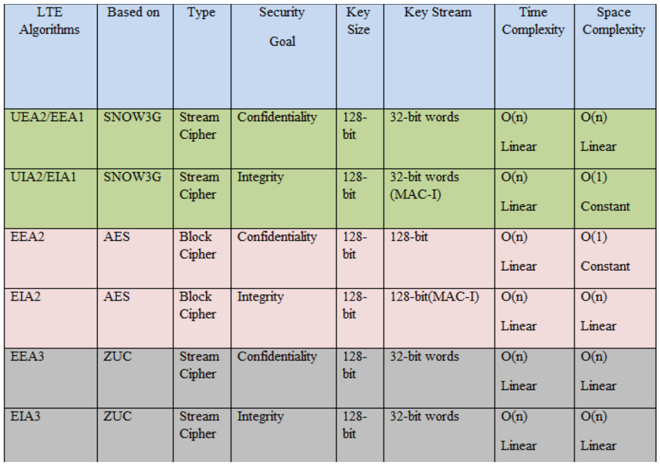
The main objectives of security are to ensure confidentiality and integrity of the algorithms. In addition, it is necessary to know the time, space and data complexity of an algorithm to perceive its efficiency during the execution. However, constant refers to the best case of running the algorithm while exponential refers to the worst case of running the algorithm. The time, space and data complexity are factors to measure the amount of security that is offered by the algorithm. Therefore, in this section first we will show the complexity values of the basis LTE algorithms and then we will explain the complexity of each set independently which are presented in Table 2 and Table 3 respectively.

Table 2: The space and time complexity of the core LTE algorithms [12]



LTE algorithms	Type	Key size (bits)	Memory(Space complexity)	Time Complexity
SNOW 3G	Stream Cipher	128-bit	O(1) Constant	O(n) Linear
AES	Block Cipher	128, 192 or 256	O(1) Constant	O(1) Constant
ZUC	Stream Cipher	128–bit	O(1) Constant	O(n) Linear

Table 3: Space and Time complexity of the three sets of LTE security algorithms



LTE Algorithms	Based on	Type	Security Goal	Key Size	Key Stream	Time Complexity	Space Complexity
UEA2/EEA1	SNOW3G	Stream Cipher	Confidentiality	128-bit	32-bit words	O(n) Linear	O(n) Linear
UIA2/EIA1	SNOW3G	Stream Cipher	Integrity	128-bit	32-bit words (MAC-I)	O(n) Linear	O(1) Constant
EEA2	AES	Block Cipher	Confidentiality	128-bit	128-bit	O(n) Linear	O(1) Constant
EIA2	AES	Block Cipher	Integrity	128-bit	128-bit(MAC-I)	O(n) Linear	O(n) Linear
EEA3	ZUC	Stream Cipher	Confidentiality	128-bit	32-bit words	O(n) Linear	O(n) Linear
EIA3	ZUC	Stream Cipher	Integrity	128-bit	32-bit words	O(n) Linear	O(n) Linear

It can be noticed from the Table 3, AES offers constant values for both time and space complexity which is the best case based on the standard security criteria, meaning that AES is very efficient during the execution in terms of time and space. Moreover, there is a similarity between ZUC and SNOW 3G where both of them offer constant space complexity and linear time complexity.

It can be seen that the comparison of the confidentiality and integrity algorithms of LTE network showed a good result in term of space complexity which provides either constant or linear value. Meaning that it provides high speed and efficiency during implementing the encryption and decryption operations and also this result of space complexity is suited to mobile equipments where the maximum message length that standardized by 3GPP is 20, 000 bits [14].

C) Complexity attacks on LTE's core algorithms

In this section, we made a literature survey of different types of common attacks of each LTE‘s core algorithm to show the resistance of each algorithm against specific attack such as guess and determine attack, differential attack , meet in the middle attack and others. Studying the time and space complexity of each attack on each LTE algorithm can give us a better image of the resistance of each algorithm against possible attack, the details of the complexity attacks with the reference can be found in Table 4.

The results in the Table 4 shows that ZUC has a better resistance than SNOW 3G against different attacks such as Guess and Determine attack with 2^{403} time complexity and Differential chosen IV Attack with $2^{99.4}$ time complexity. According to Tang Ming and et al. (2012), the ZUC algorithm can resist different cryptanalytic attacks such as weak key attacks, guess-and-determine attacks, algebraic attacks, timing attacks.

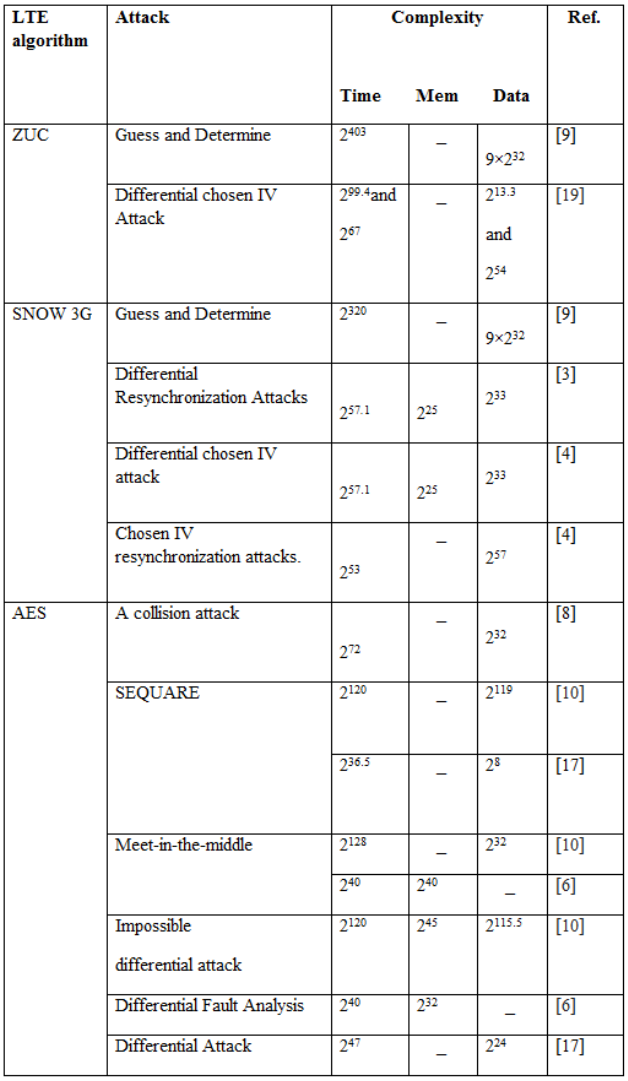
In addition, Tang stated that when Chunfang Zhou and et al. extended the differential properties of the initialization stage of ZUC from 20 rounds to 24 rounds, they discovered that ZUC can still resist against chosen-IV attacks. Experimentally, based on Tang Ming study the ZUC algorithm shows some weaknesses against DPA attack [11]. Eventually, from studying the attack complexity on AES algorithm, the values of the attack complexity that are presented in Table (4) cannot exceed the 7-rounds of 128-bit so the studies until now approved that AES has high effectiveness in resisting possible attacks because there is no attack until now can break AES algorithm of the full-rounds [16].

Going further, according to Shaaban Sahmoud (2013), AES shows very high resistance against multiple attacks such as brute-force attack, linear attack and differential attack. The high immunity of AES is due to its ability to use different lengths of keys to protect from different attacks [16]. Therefore, from studying the attack complexity of the three cryptographic algorithms where two of them are stream cipher and the other is block cipher, we can conclude that ZUC and AES offer very high immunity against multiple attacks while SNOW 3G offers less immunity against different attack than ZUC and AES.

IV. CONCLUSION

This paper compared LTE's core algorithms based on different factors in order to understand the strengths and weaknesses of each algorithm from different perspectives.

Table 4: Survey on LTE's complexity attacks algorithms



LTE algorithm	**Attack**	**Complexity**			**Ref.**
		Time	**Mem**	**Data**	
ZUC	Guess and Determine	2^{403}	–	9×2^{32}	[9]
	Differential chosen IV Attack	$2^{99.4}$and 2^{67}	–	$2^{13.3}$ and 2^{54}	[19]
SNOW 3G	Guess and Determine	2^{320}	–	9×2^{32}	[9]
	Differential Resynchronization Attacks	$2^{57.1}$	2^{25}	2^{33}	[3]
	Differential chosen IV attack	$2^{57.1}$	2^{25}	2^{33}	[4]
	Chosen IV resynchronization attacks.	2^{53}	–	2^{57}	[4]
AES	A collision attack	2^{72}	–	2^{32}	[8]
	SEQUARE	2^{120}	–	2^{119}	[10]
		$2^{36.5}$	–	2^{8}	[17]
	Meet-in-the-middle	2^{128}	–	2^{32}	[10]
		2^{40}	2^{40}	–	[6]
	Impossible differential attack	2^{120}	2^{45}	$2^{115.5}$	[10]
	Differential Fault Analysis	2^{40}	2^{32}	–	[6]
	Differential Attack	2^{47}	–	2^{24}	[17]

REFERENCES

[1]. Beming, Per, et al., "LTE-SAE architecture and performance", Ericsson Review3 (2007): 98-104.

[2]. Biryukov, Alex, Deike Priemuth-Schmid, and Bin Zhang. "Differential Resynchronization Attacks on Reduced Round SNOW 3G", e-Business and Telecommunications. Springer Berlin Heidelberg, 2012. 147-157.

[3]. Biryukov, Alex, Deike Priemuth-Schmid, and Bin Zhang, "Analysis of SNOW 3G resynchronization mechanism", Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on. IEEE, 2010.

[4]. Biryukov, Alex, Deike Priemuth-Schmid, and Bin Zhang, "Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G", Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2010.

[5]. Bulens, Philippe, et al. "Implementation of the AES-128 on Virtex-5 FPGAs", Progress in Cryptology–AFRICACRYPT 2008. Springer Berlin Heidelberg, 2008. 16-26.

[6]. Derbez, Patrick, Pierre-Alain Fouque, and Delphine Leresteux. "Meet-in-the-middle and impossible differential fault analysis on AES", Cryptographic Hardware and Embedded Systems–CHES 2011. Springer Berlin Heidelberg, 2011. 274-291.

[7]. ETSI/SAGE Specification: “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2.Document 1: UEA2 and UIA2 Specification”, Version: 2.1, March 2009.

[8]. Gilbert, Henri, and Marine Minier. "A collisions attack on the 7-rounds Rijndael." (2000).

[9]. Lin, Ding, et al. "Guess and determine attack on zuc based on solving nonlinear equations." First International Workshop on ZUC Algorithm. 2010.

[10]. Lu, Jiqiang, et al. "New impossible differential attacks on AES." Progress in Cryptology-INDOCRYPT 2008. Springer Berlin Heidelberg, 2008. 279-293.

[11]. Ming, T. A. N. G., C. H. E. N. G. PingPan, and Q. I. U. ZhenLong. "Differential Power Analysis on ZUC Algorithm."

[12]. Orhanou, Ghizlane, et al. "Analytical evaluation of the stream cipher ZUC."Multimedia Computing and Systems (ICMCS), 2012 International Conference on. IEEE, 2012.

[13]. Orhanou, Ghizlane, et al. "EPS Confidentiality and Integrity mechanisms Algorithmic Approach." International Journal of Computer Science Issues (IJCSI) 7.4 (2010).

[14]. Orhanou, Ghizlane, and Said El-Hajji. "The New LTE Cryptographic Algorithms EEA3 and EIA3." Applied Mathematics & Information Sciences 7.6 (2013).

[15]. Patrizio, A. “LTE Subscribers to Hit 200 Million Mark in 2013”. Retrived from, http://www.brighthand.com/default.asp?newsID=19753&news=LTE

[16]. Sahmoud, Shaaban, Wisam Elmasry, and Shadi Abudalfa. "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher."Int. Arab J. e-Technol. 3.1 (2013): 17-26.

[17]. Tunstall, Michael, “Practical complexity differential cryptanalysis and fault analysis of AES”, Journal of Cryptographic Engineering 1.3 (2011): 219-230.

[18]. Tunstall, M. “Low Complexity Differential Cryptanalysis and Fault Analysis of AES”. Retrieved from https://www.cosic.esat.kuleuven.be/ecrypt/courses/albena11/slides/michael_tunstall_dfaofaes.pdf. June 2011.

[19]. Wu, Hongjun, et al. "Differential attacks against stream cipher zuc." Advances in Cryptology–ASIACRYPT 2012. Springer Berlin Heidelberg, 2012. 262-277.

[20]. Zhang, Lingchen, et al., “Evaluating the Optimized Implementations of SNOW3G and ZUC on FPGA”, Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.