Comparative Study of Vulnerabilities in LTE Cryptographic Algorithm

Fatma Nilofer
Dept. Information Technology
Illinois State University
Normal, IL, USA

Jihad Qaddour
Dept. Information Technology
Illinois State University
Normal, IL, USA

ABSTRACT

Long Term Evolution (LTE) is a standard for high-speed wireless communication for mobile and data terminals based on Global System for Mobile Communication (GSM) and Universal Mobile Telecommunications Service (UMTS) Technologies. The goal of LTE is to increase the capacity and speed of wireless data networks using new DSP (digital signal processing) techniques. LTE provides high spectral efficiency, high peak data rates, short round trip time as well as flexibility in frequency and bandwidth. One of the main purpose of LTE security is to perform user's authentication and to provide data integrity and confidentiality. Two standardized algorithms were provided by LTE technology to ensure data integrity and confidentiality protection via air interface named as EPS Encryption Algorithm and EPS Integrity Algorithm. Even LTE has complex and a vigorous set of security mechanisms, but there is still need for improvement.

This research paper investigates and discusses three sets of cryptographic algorithms that work on LTE technology. These three sets of the LTE cryptographic algorithms are SNOW-3G, ZUC and AES algorithm. This paper presents a comparative study of these cryptographic algorithms as well as related attacks and the contribution of various researchers in overcoming these attacks. A complete study has been done in comparing the three algorithms, their respective challenges and solutions proposed by various researchers. After complete analysis and investigation on the advantages and disadvantages of these algorithms, we concluded that AES is one of the strongest among the three cryptographic algorithms, whereas SNOW 3G is the weakest.

Keywords

Long Term Evolution (LTE); LTE Cryptographic Algorithm; Advanced Encryption Standard (AES); ZUC; SNOW 3G; Encryption Algorithm; Integrity Algorithm; Message Authentication Code (MAC).

1. INTRODUCTION

Long Term Evolution (LTE) is defined as a global standard for the fourth generation (4G) of mobile broadband; it overcomes many challenges of the previous technologies. The core purpose of LTE is to provide a powerful defense mechanism against many possible security attacks. It enhances many features of its predecessors. Such as UMTS (Universal Mobile Telecommunication System) and GSM. LTE provides two standardized algorithms to ensure data integrity and confidentiality protection via air interface named EPS Encryption Algorithm (EEA) and EPS Integrity Algorithm (EIA). The first set 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. In addition to the mutual authentication functionality of network, LTE provides two other security functions for making data more secure during its transmission over the air interface: ciphering both user plane and control plane. Ciphering is used particularly for protecting data stream from being received by a third party during transportation. To ensure data confidentiality, the following procedures are provided:

- Cipher key agreement: The key agreement is conducted between the User Equipment (UE) and the network during the Authentication and Key Agreement procedure.
- Encryption/Decryption: Encryption/Decryption of user and signaling data is done.
- Agreement for Cipher algorithm - EPS Encryption Algorithm (EEA): LTE uses confidentiality cryptographic algorithm EEA, which is a symmetric synchronous stream cipher, to ensure the confidentiality of user and signaling data. After successful authentication, the core network and the terminal share a Cipher Key (CK). Before beginning the encryption, the communicating parties agree on the encryption algorithm by using a 4-bit identifier.

    - **0000:** EEA0 is known as a null ciphering algorithm. It generates a key-stream of all zeroes and the length of the generated key-stream must be equal to the LENGTH input parameter.
    - **0001:** 128-EEA1, the EEA1 is a stream cipher based on another stream cipher named SNOW-3G, which produces continuous key stream.
    - **0010:** 128-EEA2. The EEA2 is a stream cipher based on the block cipher AES algorithm, it uses CTR (Counter) mode.
    - **0011:** 128-EIA3. A 128-bit key stream is used for encryption/decryption EEA algorithm. The most significant bit consists of **COUNT [0] ...COUNT [31] || BEARER [0] ... BEARER [4] || DIRECTION || 26 zero bits**. These input values are written from the most significant bit on the left to least significant bit on the right, so for example COUNT [0] is the most significant bit of key stream. The least significant 64 bits of key stream1 are all 0. The output of AES is based on 128 bits' key-stream and cipher key [1].

This paper is organized in four sections: Section I gives the general introduction of the LTE technology, Section II describes the overview of three set LTE cryptographic algorithms as well as related attacks and relevant conducted research. Section III shows discussion and solutions to the challenges of LTE cryptographic algorithm. Section IV describe the comparison of three algorithms based on attacks and their complexity. Section V gives the conclusion by reviewing the vulnerabilities of all three algorithms. Section VI presents future intended research.

2. OVERVIEW ON THE THREE SETS OF LTE CRYPTOGRAPHIC ALGORITHMS

2.1 SNOW 3G

SNOW 3G is a word-oriented stream having 128-bit initialization variable and 128-bit key, generating a sequence of 32-bit words as a cipher-text/plaintext as an output. First a *key initialization* is performed, and the cipher is clocked without producing output. Then the cipher operates in *key-generation* mode and it produces a 32-bit cipher-text / plaintext word output in every clock cycle. It takes 32-bit plaintext/cipher-text input and produces a 32-bit cipher-text/plaintext output. In addition,

SNOW 3G consists of a Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM). The LFSR is constructed from 16 stages, s0 to s15, each holding 32 bits and the feedback is defined by a primitive polynomial over the finite field GF (232). The FSM is based upon three 32-bit registers R1, R2, and R3. The operation of the FSM involves input from the LFSR and uses two substitution box ensembles S1 and S2. The mixing operations are exclusive OR and addition modulo 232 [1].

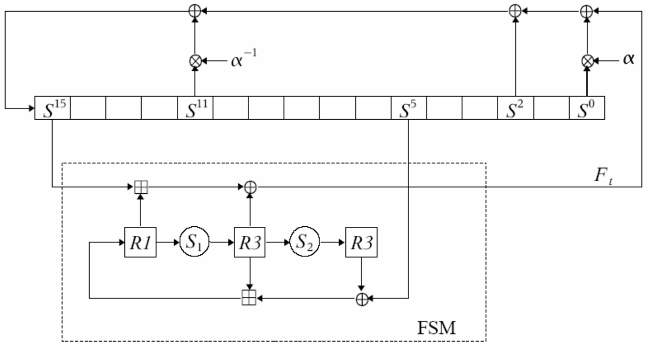

Figure 1. SNOW 3G algorithm during key-generation mode

The first SNOW algorithm SNOW 1.0 was vulnerable to guess-and-determine attack as described by Hawkes and Rose [4]. It was also vulnerable to linear cryptanalysis attack as described by Coppersmith, Halevi, and Jutla, ref. [5]. Because of the weakness of SNOW 1.0, a new algorithm is introduced in the SNOW family SNOW 2.0. The main changes from SNOW 1.0 to SNOW 2.0 is the modification of the feedback polynomial and two inputs is given two the FSM from the shift register. In SNOW 2.0 the finite field GF (232) is an extension field of degree four over the finite field GF (28) and the modified S-box in SNOW 2.0 also provides stronger diffusion since each output bit now depends on each input bit. As per the research done by Billet and Gilbert, SNOW 2.0 was not resistant to algebraic attacks [6].

Based on these results, the main goal for the design team is to come up with new algorithm that has resistance to algebraic attacks. This goal was achieved by the introduction of the SNOW 3G. In SNOW 3G, two new components were introduced into the earlier design of SNOW 2G: 32-bit register R3 and the second ensemble of S-boxes S2 in the FSM.

To increase the resistance of SNOW 2.0 against algebraic attacks, the designers used the 32-bit register R3 and S-Box S2 in FSM such that R3 gets as input the output of S2 [3]. The initial cryptanalyses of SNOW 3G show good resistant against algebraic attacks, guess and determine attack and linear distinguishing attack [3].

2.1.1 Attacks on SNOW 3G

The security assessment of the structure of SNOW 3G involved analysis of the cipher against the following class of attacks:

- Algebraic attacks
- Guess-and-determine attacks
- Distinguishing attacks based on linear approximations
- Initialization attacks based on differential cryptanalysis and collision attacks.

An Algebraic attack is a cryptanalytic method of finding and solving a system of multivariate polynomial equation over finite field. Guess and Determine (GD) attacks are general attacks on stream ciphers. GD attacks are divided in two classes:

- Ad-hoc GD attacks- They are relied on experience and creativity of cryptanalyst. However, there is no common method for designing ad-hoc GD attacks.
- Heuristic GD (HGD) attacks-In this, cryptanalysts use an algorithmic method on stream ciphers. The only condition in this method is that all variables of the underlying algorithm are to be the same size and each variable is (uniquely) determined if all other variables are known.

In ref. [8] Cryptanalytic attacks on SNOW 3G were described along following strategies:

1.) Structural attacks- These attacks based on the structure architecture of SNOW 3G that gave complexities that were well above the key size of the algorithm.

2.) Linear attacks- The report described general strategies for distinguishing attacks based on linear approximations and argued that they are most likely unsuccessful in building a distinguisher for SNOW3G.

3.) Algebraic attacks- The team discussed possible strategies for mounting algebraic attacks against SNOW 3G but concluded that the introduction of R3 succeeded very well against the problems identified by Gilbert and Billet, ref. [10].

4.) Resynchronization attacks- SNOW 3G was evaluated against chosen IV attacks. Researchers used the fact that the (then) S-box S2 was not a permutation and they argued that the diffusion rate of SNOW 3G with 32 clocks for the initialization of 19 registers does not have a huge security margin against resynchronization attacks.

2.2 ZUC

ZUC is a word-oriented stream cipher that forms the heart of the 3GPP, it uses confidentiality algorithm 128-EEA3 and the integrity algorithm 128-EIA3. It takes two inputs: a 128-bit initial key and a 128-bit initial vector (IV) and produces an outputs keystream of 32-bit word. This keystream can be used for encryption/decryption.

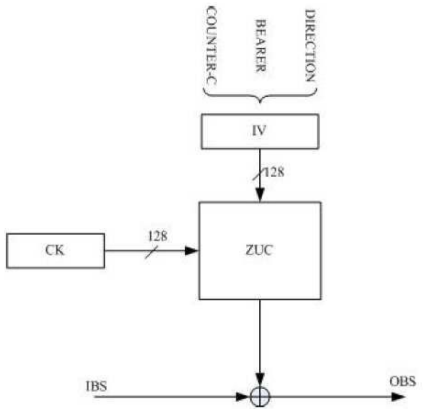

Figure. 2: Principles of the 128-EEA3 encryption operation

The operation of ZUC has two stages: initialization stage and working stage. In the first stage, a key/IV initialization is performed, i.e., the cipher is clocked without producing output. The second stage is a working stage, in this with every clock pulse, it produces a 32-bit word of output. During the working mode, the number of words to produce as output depends on the input parameter n. When an input parameter to ZUC, the algorithm produces exactly n 32-bit output words which will be added by an exclusive-OR operation to the n 32-bit words of the plaintext (or cipher-text) to obtain the cipher-text (or the plaintext). Therefore, based on this description and on the ZUC specifications [2], we can see that ZUC has a linear time complexity and constant space complexity.

ZUC consists of three logical layers:

1) The top layer is a **linear feedback shift register (LFSR)** which is of 16 stages (s0, s1, . . ., s15), each holding 31 bits. The feedback is a primitive polynomial over the finite field GF (2^{31}-1).
2) The middle layer is for **bit reorganization (BR)** extracts 128 bits from the registers of the LFSR and forms four 32-bit words. These four 32-bit words will be used by output of key stream nonlinear function F.
3) The bottom layer is a **nonlinear function F** which based upon two 32-bit memory cells R1 and R2. It uses two S-boxes: S 0 and S 1 and takes 3 of 32-bit words from the BR as its inputs. It also involves different operations such as addition modulo 2^{32}, the exclusive-OR and the cyclic shift [7].

2.2.1 Attacks on ZUC

In ref [1], 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 et al. (2012), the ZUC algorithm can resist different cryptanalytic attacks such as weak key attacks, guess-and-determine attacks, algebraic attacks, and timing attacks.

1. Differential attack:

In ref [9], researchers conducted a differential attack against ZUC 1.4. The vulnerability in ZUC 1.4 is due to the non-injective property in the initialization, which results in the difference in the initialization vector being cancelled. The identical keystreams pose a serious threat to the use of ZUC 1.4 in applications since it is similar to reusing a key in one-time pad. Once identical keystreams are detected, the key can be recovered with average complexity $2^{99.4}$. In the second attack, difference is injected into the second byte of the initialization vector, and every key can result in two identical keystreams with about 2^{54} IVs. The key can be recovered with complexity $2^{67,}$ once identical keystreams are detected. The researchers of this paper have presented a method to fix the flaw by updating the LFSR in an injective way in the initialization. This method is used in the later versions of ZUC which is ZUC 1.6 and is secure against differential attack.

2. Birthday forgery attack:

Researchers [11] have proved that 128-EIA3 is vulnerable to birthday forgery attack. The attack is based on the well-known problem of birthday paradox and it requires minimum 2^{16} known message-MAC pairs for finding collision in 128-EIA3. Birthday forgery attack aims to find internal and external collision in 128-EIA3 for distinct messages of same length. If 128 EIA3 is implemented in existing structure, it will have devastating effect on the integrity mechanisms of GSM as it has to be implemented in Subscriber Identity Module (SIM) cards and in GSM network authentication centers. They suggested that applicability of key/keystream recovery attacks based on collision should be considered for 128-EIA3.

2.3 AES

Advance Encryption Standard (AES) which is a symmetric-key algorithm with different block and key sizes. **AES** is a block-cipher used in LTE, it uses confidentiality algorithm ***128-EEA2*** and the integrity algorithm ***128-EIA2.*** The first portion 128-EEA2 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 128 EIA2 is used for ensuring integrity and is based on AES but in the CMAC (Cipher-based MAC) mode [1].

The AES algorithm uses a fixed block size of 128 bits and different key sizes of 128, 192 or 256 bits as input. It has four operations as follows:

1.) *AddRoundKey* - Each round key is derived from the cipher key using a key schedule which is XOR with 128 bits of state. In this stage, the 128 bits of state are bitwise XOR with the 128 bits of the round key.

2.) *SubBytes*- Non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).

3.) *ShiftRows*- A Shift Rows is a transposition step where each row of the state is shifted cyclically a certain number of times.

4.) *MixColumns*- A mixing operation operates on the columns of the state, it combines the four bytes in each column.

AES does encryption of key-stream with Cipher Key CK. AES (T) is TRUC () operation which will truncate the last plain text as of its size and return the most significant bits in truncate mode. Cipher text is the XOR result of plaintext and Key-stream Block of AES operation. The above algorithm process and truncated AES operation is explained in [4].

2.3.1 Attacks on AES algorithm

1. Fault attack

In ref [14], researchers conducted high-efficient fault attack against AES S-Box. They proposed that by changing the mapping relationship of the S-Box during the encryption process, faults can be introduced. Two models are introduced based on the round in which the fault was introduced. Results shows that the first model only needs 16 faulty cipher-text to recover 128-bit secret key. The second round is more efficient and in this model two rounds of attack are enough to find out 4-byte round key on the 9th round S-box based on DFA.

A novel Differential Fault Analysis on AES-128 is proposed to find the initial key, by inducing four bytes random faults into the nine-round key stored in static RAM. The relationship between faults in the last two round keys can be revealed. Faults induced can be determined fast by the difference between the correct and corrupted cipher-text. Finally, the initial key can be recovered with a brute force search of complexity 2^{32} [16]. As per the researchers of the article [17] carried a fault attack against AES algorithm. Their result shows that the fault can be gained by the attacker by either understanding the specific implementation under attack or by characterizing the injection technique in order to build a-priori a good fault model.

2. Algebraic Attack

Advanced Encryption Standard algorithm was designed to resist against many methods of cryptanalysis such as linear attack, differential attack etc. But, it has not sufficient immunity against algebraic attack. The complexity of algebraic attacks on block ciphers depends on the production of enough number of linearly independent equations. Aida Janadi and D. Anas Tarah [13], tried some methods to increase the immunity of AES algorithm against algebraic attack. A new enhancement on the immunity of new AES algorithm is being proposed by them. To achieve the required goal, they modified static AES S-Box. The modified S-Box is random and it depends on the concept proposed by L.Keliher and Y.H.Meijery [12] of Key-Dependent S-Boxes and also by Knuth proposed algorithm.

3. Side Channel Attack

AES is vulnerable to side channel attack (SCA). SCA is based on the knowledge of the algorithm implementation and measurements, for instance power consumptions or timing measurement. It is not an attack on the mathematical background for AES but an attack on the implementation of the cipher or the knowledge of the main algorithm. In ref [2], the researchers present a novel core implementation of the Advanced Encryption Standard (AES) with an integrated countermeasure against side channel attacks, which can theoretically increase the complexity of a DPA attack by a factor of 240 and hence turn the attack unfeasible or, at least, too expensive. This countermeasure is based on mathematical properties of the Rijndael algorithm and retains compatibility with the published Standard.

3. DISCUSSION AND SOLUTIONS TO CHALLENGES OF LTE CRYPTOGRAPHIC ALGORITM

This session discusses some of the challenges and solutions to all three-cryptographic algorithm. Researchers to overcome these vulnerabilities have done various research study and still some are under process. The various research study that has been done are as follows:

3.1 SNOW 3G

In ref [3], researchers conducted analysis of heuristic guess and determine (HGD) attack on SNOW 3G. Using auxiliary polynomials of relatively small degree, the HGD attack on SNOW 3G has been improved. By this method, the researchers have examined the resistance of SNOW 3G. The improved HGD attack reduces the complexity and the size of the guessed basis from *O* (2^{320}) to *O* (2^{160}) and 10 to 5, respectively, in comparison with the ad-hoc and HGD attacks. The complexity of the attack decreases as the guessed basis gets smaller. Hence, the result shows that the complexity of Heuristic guess and determine attack is greatly reduced by using auxiliary equations.

3.2 ZUC

Experimentally, based on Tang Ming study the ZUC algorithm shows some weaknesses against DPA attack [11]. The results show that ZUC algorithm is to some extent vulnerable to DPA. It exploits the weakness in the outputs of S-box in ZUC stream cipher. Differential Power Analysis (DPA) is one of the potential serious threat to ZUC algorithm, it is necessary for designers to add the effective countermeasures to the implementation of ZUC Algorithm to guarantee its security in real applications.

3.3 AES

Researchers Ali Mirzaeyan, Ahmad Patooghy & Mehdi Fazeli of the article [15], proposed a method to incorporate redundant substitution table to immune S-Box function of AES encryption algorithm against fault injection attacks. These substitution tables are constructed based on Chinese Reminder Theorem to distribute bits of a traditional S-Box cell into either 2,4, or 6 non-adjacent cells. In this way, at least 93% of injected attacks are detected i.e., attacker is prevented to reach his/her aim. Their results show that the proposed architecture imposes acceptable overheads i.e., 96% in critical path, 48% in occupied area. The proposed architecture for sub-byte function is developed and syntheses by Verilog code.

Table 1 mentions the three cryptographic algorithms and their respective challenges and solutions suggested by various researchers. Some attacks have been recovered successfully while some attacks are still a threat to these algorithms.

TABLE 1: CHALLENGES AND SOLUTIONS

Algori thms	***Challenges***	***Solutions***
SNO W 3G	Algebraic attack	With the introduction of register R3 SNOW 3G succeeded very well against the algebraic attack
	Heuristic and Guess attack	The HGD attack on SNOW 3G has been improved by using auxiliary polynomials of relatively small degree
	Resynchronization attack	SNOW 3G with 32 clocks for the initialization of 19 registers does not have a huge security margin against resynchronization attack. Research still need to be carried to make SNOW 3G

		resistant against Resynchronization attack
ZUC	Differential Attack	Differential Power Analysis (DPA) is one of the potential serious threat to ZUC algorithm, it is necessary for designers to add the effective counter-measures to the implementation of ZUC Algorithm to guarantee its security in real applications.
	Birthday Forge Attack	The applicability of key/keystream recovery attacks based on collision should be considered for 128-EIA3 to resist birthday forge attack.
AES	Algebraic attack	Static AES S-Box was modified to resist AES against Algebraic attack. The modified S-Box is random, and it depends on the Key-Dependent S-Boxes and by Knuth proposed algorithm.
	Side Channel Attack	A countermeasure has been implemented against side channel attacks, which can theoretically increase the complexity of a DPA attack by a factor of 240. This countermeasure is based on mathematical properties of the Rijndael algorithm, and retains compatibility with the published Standard
	Fault attack	Redundant substitution table was incorporated to immune S-Box function of AES encryption algorithm against fault injection attacks. These substitution tables are constructed based on Chinese Reminder Theorem and was succeeded against fault attacks

4. COMPARITIVE ANALYSIS OF THREE ALGORITHMS BASED ON ATTACKS AND COMPLEXITY

As per the research conducted by Alyaa Ghanim Sulaiman [1], Table 2 below summarizes various attack that has been tried on the three LTE cryptographic algorithm and the time complexity required by each attack to compromise the algorithm. It shows various attacks on LTE algorithms and the time complexity required to break that algorithms. The table shows that the time complexity to break AES is higher as compared to the other two. From studying the different attack complexity on 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 [1].

TABLE 2: ALGORITHMS AND COMPLEXITY

LTE Algorithms	***Attack***	***Complexity***		
		Time	***Data***	***Mem***
ZUC	Guess and Determine	2^{403}	-	$9x2^{32}$
	Differential chosen IV Attack	$2^{99.4}$ and 2^{67}	-	$2^{13.3}$ and 2^{54}
SNOW 3G	Guess and Determine	2^{320}	-	$9x2^{32}$
	Differential Resynchronization Attack	$2^{57.1}$	2^{25}	2^{33}
	Differential chosen IV Attack	$2^{57.1}$	2^{25}	2^{33}
	Chosen IV resynchronization attacks	2^{53}	-	2^{57}
AES	A collision attack	2^{72}	-	2^{32}
	Square	2^{120}	-	2^{119}
	Meet-in-the-middle	2^{128}	-	2^{32}
	Impossible differential attack	2^{120}	2^{45}	$2^{115.5}$
	Differential Fault Analysis	2^{40}	2^{32}	-
	Differential Attack	2^{47}	-	2^{24}

In ref [1], the literature surveys different types of common attacks on three LTE ‘s cryptographic algorithm to show the resistance of each algorithm against specific attacks such as guess and determine attack, differential attack, meet in the middle attack and others. The results show 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 $^{299.4}$ time complexity. Among the three set of cryptographic algorithm AES is resistance against most of the attack.

Table 3: Advantages, Disadvantages And Challenges to cryptographic Algorithms

Algorithms	*Advantages*	*Disadvantages*	*Challenges*
Snow 3G	Fits the requirements of the 3G security environment. Offers adequate protection against new forms of algebraic attacks Avoids similar design principles with Kasumi (like the atomic nonlinear functions)	Is more computationally complicated in terms of hardware area space regarding an application for integrity protection	Algebraic attack Guess-and Heuristic attack Resynchronization attack
AES	AES is more secure AES is faster in both hardware and software AES's 128-bit block size makes it less open to attacks via the birthday problem	Encryption of each block is sequential	Algebraic Attack Side-Channel Attack Fault attack
ZUC	Fits the requirements of the 3G security environment Offers strong encryption via 128-bit keys Appears to have a sound design with a large security spectrum Builds on design principles of well-known ciphering algorithms	Requires more analysis to gain further confidence	Differential attack Birthday forgery attack

Table 3 discusses the LTE cryptographic algorithm along with the advantages, disadvantages and challenges of them. Various researchers have overcome some of these challenges while research is still going on to make these algorithms more sustainable to these attack as well as other attacks. Although AES algorithm is one of the strongest algorithm among the three LTE cryptographic algorithm it is still possible to break this algorithm with some attacks. Though the time complexity to break AES is higher as compared to ZUC and SNOW 3G. SNOW 3G is the weakest algorithm among the three algorithms, it is vulnerable to various attack whereas ZUC is comparatively stronger than SNOW 3G, it offers strong encryption algorithm via 128 bits key. From studying the different attack complexity on 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.

5. CONCLUSION

We investigate and discuss the LTE cryptographic algorithm along with the advantages, disadvantages and challenges. Although AES algorithm is one of the strongest algorithm among the three LTE cryptographic algorithm, it is still possible to break this algorithm with some attacks. However, the time complexity to break AES is higher as compared to ZUC and SNOW 3G. SNOW 3G is the weakest algorithm among the three algorithms, it is vulnerable to various attack whereas ZUC is comparatively stronger than SNOW 3G, it offers strong encryption algorithm via 128 bits key.

We also, discussed challenges and solutions to all three-cryptographic algorithm and summarizes various attack that has been tried on the three LTE cryptographic algorithm and the time complexity required by each attack to compromise the algorithm. We showed various attacks on LTE algorithms and the time complexity required to break that algorithms. We conclude that the time complexity to break AES is higher as compared to the other two. In addition, 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. From studying the different attack complexity on 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. Finally, among the three set of cryptographic algorithm AES is resistance against most of the attacks.

6. FUTURE WORK

One can never prove that a cryptographic algorithm will be able to resist new attacks in the future; it is always prone to new types of attacks. So, research must be carried on in protecting these algorithms from evolving new attacks and to come up with a better version, in terms of security as well as space and time complexity. AES cryptographic algorithm involves protection against more advanced variations of the DPA attack. Since, the secret keys are now embedded into a number of devices means that the hardware becomes an attractive target for attackers to comprise the key. Therefore, future work involves defining suitable ways to secure the secret key of most embedded cryptographic devices against DPA attacks.

7. REFERENCES

[1] Ghanim, A., & Alshaikhli, I. F. T. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. International Journal of Computer Science and Telecommunications, 5(7), 7-10.

[2] Ghellar, F., & Lubaszewski, M. S. (2008, September). A novel AES cryptographic core highly resistant to differential power analysis attacks. In Proceedings of the 21st annual symposium on Integrated circuits and system design (pp. 140-145). ACM.

[3] Nia, M. S. N., & Eghlidos, T. (2014, September). Improved Heuristic guess and determine attack on SNOW 3G stream cipher. In Telecommunications (IST), 2014 7th International Symposium on (pp. 972-976). IEEE.

[4] P. Hawkes and G. G. Rose. Guess-and-determine attacks on SNOW. In K. Nyberg and H. M. Heys, editors, Selected Areas in Cryptography -- SAC 2002, Lecture Notes in Computer Science, pages 37--46. Springer -Verlag, 2002.

[5] D. Coppersmith, S. Halevi, and C. S. Jutla. Cryptanalysis of stream ciphers with linear masking. In M. Yung, editor, Advances in Cryptology -- CRYPTO 2002, Lecture Notes in Computer Science, pages 515--532. Springer -Verlag, 2002

[6] O. Billet and H. Gilbert. Resistance of SNOW 2.0 against Algebraic Attacks. In Alfred Menezes editor, Topics in Cryptology -- CT-RSA~2005, Lecture Notes in Computer Science, vol. 3376, Springer Verlag, 2005.

[7] ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3.Document 1:128-EEA3 and 128-EIA3 Specification; Version: 1.6, (2011).

[8] ETSI/SAGE Technical report: Speciation of the 3GPP Condentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report, Version 1.1, September 2006.

[9] X. Wang and K. Sako (Eds.): ASIACRYPT 2012, LNCS 7658, pp. 262–277, 2012.International Association for Cryptologic Research 2012.

[10] Haider, R. Z. (2011). Birthday Forgery Attack on 128-EIA3 Version 1.5. IACR Cryptology ePrint Archive, 2011, 268.

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

[12] L.Keliher and y.H.Meijery,"A New Substitution-Permutation Network Cipher Using Key-ependent S-Boxes', Proceedings of Fourth International Workshop on Selected Areas in Cryptography (SAC'97), Carleton University, Canada, pp. 13-26, 1997.

[13] Janadi, A., & Tarah, D. A. (2008, April). AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes. In Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on (pp. 1-6). IEEE.

[14] N. Liao, X. Cui, T. Wang, K. Liao, D. Yu and X. Cui, "A high-efficient fault attack on AES S-box," 2016 Sixth International Conference on Information Science and Technology (ICIST), Dalian, 2016, pp. 210-215.

[15] A. Mirzaeyan, A. Patooghy and M. F. Ali, "A novel countermeasure against fault injection attacks for AES-based cryptosystems," 2016 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, 2016, pp. 1148-1153.

[16] Pengjun Wang and Lipeng Hao, "A novel Differential fault analysis on AES-128," 2011 9th IEEE International Conference on ASIC, Xiamen, 2011, pp. 35-38.

[17] Ferretti, C., Mella, S., & Melzani, F. (2014, June). The role of the fault model in DFA against AES. In Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy (p. 4). ACM.