LTE Security: Encryption Algorithm Enhancements

Mayur Solanki[1], Seyedmohammad Salehi[2], and Amir Esmailpour[3]

Abstract – Increasing desire for ubiquitous data made Long Term Evolution (LTE) one of the most popular Fourth Generation (4G) cellular networks worldwide. Formerly, low-speed of 3G cellular networks made WiFi a dominant technology for high-speed data when present but today LTE plays the important role of obtaining data on cellphones even where WiFi is present. Additionally, the rewards available to attackers, within the hacking subculture have shifted from bragging rights to monetary rewards from organized criminal networks in exchange for information theft. On one hand, the vulnerability of always-on-cellphones, combined with the fast speed of LTE, highlights the role of security more than ever. On the other, there is a trade-off between security algorithms and speed. Hence there is significant need for security measures that balance security with the speed of data acquisition. In this paper we propose an algorithm that advances efficiency within that balance. We show in MATLAB how our new algorithm works. We demonstrate that it does not add significant time to the encryption and decryption processes as the algorithm becomes more complex. Our algorithm and the method behind it can be employed in any system that takes advantage of LTE-advanced technology.

Keywords: Encryption, Cryptography, Key generation

INTRODUCTION

The purpose of LTE security is to provide a powerful defense mechanism against possible threats from the internet imposed by various types of attacks. Security measures taken by LTE include sophisticated mechanism for authentication, authorization and encryption to provide access, confidentiality and integrity respectively as illustrated in Figure 1.

Possible Threats: LTE like its predecessors is threatened by various types of attacks from hackers, imposters, eavesdroppers, viruses and other attackers.

Security measures: LTE takes several measures against these threats. Let's say two parties (A and B) are trying to establish communication and access data.

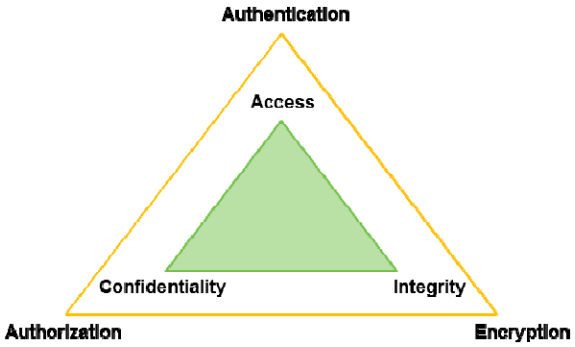

Figure 1: Security mechanism in LTE

[1,2]Master Student, ECE department, the University of New Haven, 300 Boston Post Rd. West Haven, CT, 06516, ([1]Msola1,[2]ssale3)@unh.newhaven.edu
[3]Assistant Professor, ECE department, the University of New Haven, 300 Boston Post Rd. West Haven, CT, 06516, [3]aesmailpour@newhaven.edu

Authentication and Access: In classical scenario where parties A and B are communicating over some channel, both typically want to begin with identifying each other. Authentication is the process of verifying that they can establish communication.

Authorization and Confidentiality: who can have access to what kind of data is called authorization which separates different users from having access to all data. Being sure that conversation between parties A and B are confidential as a result can be fulfilled.

Encryption and Integrity: If all messages sent by party A are identical to the ones received by party B, and vice versa, the message is not altered on the way, then integrity of the communication has been preserved and this can't be fulfilled without using Encryption Algorithms.

Design of Third Generation (3G) security is based on the practical experience with Global System for Mobile Communication (GSM) security and, to a lesser extent, experiences with the security of other second generation cellular systems. Design of the Evolved Packet System (EPS) security architecture follows the same principle of maximizing, from a system point of view, the synergies between security functions and other functions. EPS is introduced in 3GPP family with remarkable improvements compared to 3G and GSM security mechanism, such as a new radio interface and an evolved architecture for both the Access and the Core Network parts. EPS offers same security features as its prototypes UMTS (Universal Mobile Telecommunication System) and GSM. Besides the mutual authentication functionality of network, two other security functions are provided for making data more secure during its transmission over the air interface: ciphering of both user plane and control plane. Ciphering is used particularly for protecting data stream from being received by third party during transportation.

EPS security mechanism uses two ciphering algorithms: SNOW-3G which is a stream encryption method and Advance Encryption Standard (AES) which is a symmetric-key algorithm with different block and key sizes. This research will explain current EPS security mechanism with AES algorithm and what kind of improvements can make data more secure wile transmission. The entire EPS security mechanism will be implemented in MATLAB. Also new security architecture of EPS with possible improvements will be implemented in MATLAB. Basically, this development tool will show the results of EPS mechanism after making the changes.

The structure of this paper is as follows: Section II gives the necessary background information about LTE security including types of keys being used in it, the EPS authentication and key agreement etc. Section III will explain about literature reviews that have been done during this research and concept of each research. Section IV shows how EPS security mechanism work including algorithm and keys being used to choose algorithm method as well as keys being used for ciphering. The new possible improvements in EPS security mechanism and implement results are described in Section V; finally we conclude in Section VI.

BACKGROUND

This section aims to present a logical sequence of facts to justify the need for our research to be done. Many aspects of security are relevant for a communication system including physical security aspects and information security aspects. The former include issues such as locked rooms, safe and guards; all these are needed when operating large scale networks. In particular, this research study has been focused on communication security, yet physical security is also important for Evolve Packet System (EPS) security as well.

In LTE network architecture, UE, eNB and MME are the main components taking part in LTE security process including authentication and authorization. UE and MME are connected with Non Access Stratum (NAS) security protocol and NAS message communication between UE and MME are integrity protected and ciphered with extra NAS security header. UE and eNB are connected through Access Stratum (AS) protocol. AS security is carried out for Radio Resource Control (RRC) and user plane data and belongs to the scope of UE and eNB. Packet Data Control Plane (PDCP) layer in UE and eNB side is responsible for the ciphering and integrity protection. RRC messages are integrity protected and ciphered but U-Plane data is only ciphered.

The main emphasis of this research is on the first two features: authenticity and confidentiality. The main point of introducing LTE and EPS is to improve the availability of the cellular access channel. Non-repudiation feature is still of less importance in EPS networks; it is much more relevant for the application layer. There are many types of different keys used in LTE security. Key is the main element to encrypt data in a given algorithm. Several keys in LTE are being generated in different algorithms based on pre-shared keys.

The key agreement part of EPS AKA produces only a single intermediate key K_{ASME} instead of a set of keys that would be subsequently used in security mechanisms. All cryptographic keys that are needed for various security mechanisms are derived from the intermediate key K_{ASME} which can be viewed as a 'local master key' for the subscriber, in contrast to the permanent master key K. on the network side the intermediate local master key K_{ASME} is stored in the MME while the permanent master key K is stored in the AuC. The advantages of using an intermediate key are twofold.

After the idea of using the intermediate key K_{ASME} was introduced in the design of EPS, another intermediate key K_{eNB} was added that is stored in the base station eNB. Addition of K_{eNB} makes it possible to renew keys for protection of radio access without involving the MME. Furthermore, an appropriately modified K_{eNB} can be handed over between base stations in a so-called X2-handover without involving the MME. The keys used directly for protecting the RRC signaling and the user data on the radio interface would not be suited for this purpose as they are bound to particular cryptographic algorithms, which is not the case for K_{eNB}, and base stations may apply different cryptographic algorithms [1].

The EPS must also be able to interwork with legacy systems, so these adaptions have to be done in a backward-compatible manner. In addition to adaptions from security functionalities already existing in legacy systems, many new extensions and enhancements have been introduced in the EPS security architecture presented in reference [2]

LITERATURE REVIEW

In [3], 3GPP document lists the design criteria for 3G cryptographic algorithms. Two important decisions had to be made in the beginning; first, it had to be decided whether to aim for publicly available algorithm or secret algorithms. Second, it had to be decided for each algorithm whether it is obtained by:

- Selecting an already existing off-the-shelf algorithm (with adaptions to fit into the 3G security architecture)
- Inviting submissions from cryptography experts and/or the security community at large for a new algorithm
- Commission a specific group of experts to carry out the design work in a force project

3GPP chose the third option and delegated the ETSI body Security Algorithm Group of Experts (SAGE) to create a task force for the design and evaluation work for the 3G cryptographic algorithm. This study proposes an idea about how 3GPP security algorithm selection end up with and what kind of criteria effect for choosing algorithms.

Reference [4] explains that Confidentiality and Integrity protection for RRC and User Plane (UP) data is provided between the UE and the e-NB in the Access Stratum (AS). These security features are applied at the Packet Data Convergence Protocol (PDCP) layer, and no layers below PDCP are confidentiality protected. The PDCP layer manages data streams for the user plane, as well as for the control plane. The architecture of the PDCP layer differs for user plane data and control plane data.

With the references of 3GPP specifications and ETSI/SAGE specifications, the authors have mentioned as below for user and signaling data confidentiality. To ensure the data confidentiality, the following procedures are provided:

- Agreement for Cipher algorithm - EPS Encryption Algorithm (EEA): To ensure the confidentiality of user and signaling data in LTE, 3GPP has maintained the use of the UMTS algorithm UEA2 based on SNOW-3G algorithm, and has named it EEA1. In addition, a new algorithm EEA2, based on AES algorithm used in the CTR mode (Counter Mode), has been adopted. Besides, the UE and the EPS can securely negotiate the algorithm to use in their mutual communication
- Cipher key agreement: the agreement is done between the UE and the network during the Authentication and Key Agreement procedure
- Encryption/Decryption of user and signaling data

Moreover, the authors have provided a description for EEA algorithm identification including NULL algorithm, which may be used in certain special cases, such as for making an emergency call without a USIM (Universal Subscriber identity Module). LTE confidentiality algorithm EEA is a symmetric synchronous stream cipher. This type of ciphering has the advantage to generate the mask of data before even receiving the data to encrypt, which help to save time. Furthermore, it is based on bitwise operations which are carried out quickly.

Figure 2 shows EEA2 structure for encryption which has been adopted from [4]. This is the same structure to be used for decryption. A 128-bit key stream is used for encryption/decryption EEA algorithm. The most significant bit

consist of COUNT[0] ..COUNT[31] || BEARER[0] .. BEARER[4] || DIRECTION || 26 zero bits. These input values are written from 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 which are explained previously. A 128-bits plain text later will be XORed with AES output which will be a cipher text in result. This cipher text is going to be transmitted to the receiver. The same operation will be done on the receiver side to get the plain text. An implementation of EEA2 is done in C coding to prove the functionality of the EEA security algorithm in respect to the 3GPP requirements.

In [5], we see explanation about LTE-AKA and its process. The authors provide an explanation about the large changes made in the mobile network. One of the main issues by this change is discussion of security against various threats, which by progress and increases the growing complexity of networks and entry various services such as new multimedia services, Internet and e-commerce features, tried to improve the security mechanism. For instance, one of the most evolved security mechanisms is authentication and key agreement protocol in mobile networks which have been mutual. Furthermore, there is an explanation about how user and network authenticate each other and agree on the encryption and integrity keys, by the specific and complex mechanism and algorithms.

The authors provide an insight to reader about step by step process of authentication and key agreement. Also there is a note saying that during authentication process in the next generation mobile networks, key separation and key hierarchy has been added. The algorithms of key derivation and figures about EPS-AKA process give brief details about how EPA-AKA mechanism works between UE and MME. Reference [5] has details regarding the standard EPS-AKA authentication protocol in the LTE network. Also it has proposed improvement to perform terms of efficient use of bandwidth, and decrease wasted computation overhead, an improved protocol is recommended.

The main reason of using several keys are produced id to provide key separation and to protect the underlying shared secret key K. in UTRAN and GERAN, the same keys are used for control signaling and user traffic. EPS-AKA process between UE and MME as well as key generation algorithm is an essential part to for to complete this project. Hence, the authors provide details about EPS-AKA mechanism and key generation algorithm. They also proposed improved EPS-AKA algorithm with MATLAB simulation results.

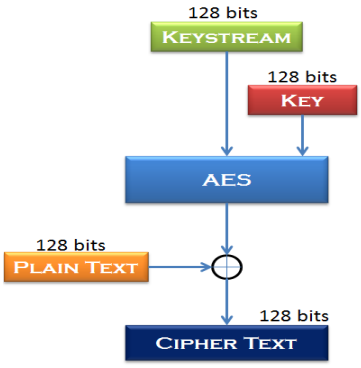

Figure 2: EEA2 Encryption Structure

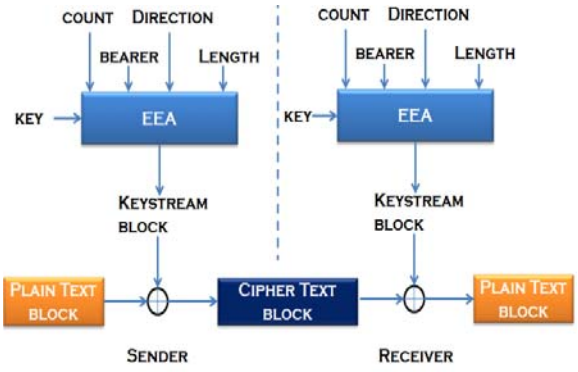

Figure 3: Encryption/Decryption of User/Signaling Data

Reference [6] has several sections starting from LTE security requirements, Key hierarchy, separation of AS and NAS security functions and handover security. LTE security requirements and key hierarchy system have been studied in previous studies. However, the key hierarchy and its generation steps are explained in more detail to provide in-depth explanation about generating keys pattern and their purposes. According to the authors, as soon as the UE enters the connected state and NAS security process is done, the eNB switched on the AS protection mode command, then the AS security is applied to all communication between the UE and the eNB. The algorithm used for AS is negotiated independently from the algorithm used for NAS.

This technology report has mentioned that in the LTE, encryption and integrity protection algorithm based on SNOW-3G and Advance Encryption Standard (AES) are standardized. While those two algorithms each provides full security, two standard algorithms that differ in basic structure are used in 3GPP so that even if one algorithm is broken, the other can be used for continued secure use of the LTE system.

Furthermore, reference [6] describes the key chain model for security handover which gives idea how K_{eNB} is derived and Next Hope (NH) is generated to determine K_{eNB*}. Because NH can be calculated by UE and MME, this use of NH provides a method that achieves across multiple eNBs. K_{eNB} is used as the base key for securing communication between UE and eNB.

EPS ENCRYPTION ALGORITHM (EEA) CIPHERING MECHANISM

The needs for a confidentiality protected mode of transmission are fulfilled by an LTE confidentiality cryptographic algorithm EEA which is symmetric synchronous stream cipher. Once the user and the network have authenticated each other they may begin secure communication. As described in 'types of key' section, a cipher key CK is shared between the core network and the terminal after a successful authentication event. Before encryption can begin, the communicating parties have to agree on the encryption algorithm also. To each EEA algorithm is assigned a 4-bit identifier. Currently, the following values have been defined for NAS, RRC and UP ciphering. This identifier is contained in each key named K_{NASenc}, K_{RRCenc} and K_{UPenc}. Below is the detail of each identifier has been used for algorithm selection.

•"0000": EEA0 null ciphering algorithm. The EEA0 algorithm is implemented in the way that it has the same effect as if it generates a key-stream of all zeroes. The length of the generated key-stream has to be equal to the LENGTH input parameter.it is important to note that the security functions are never deactivated, although it is possible to apply NULL ciphering algorithm. The NULL algorithm may be used in certain special cases, such as for making and emergency call without USIM.

•"0001": 128-EEA1, the EEA1 is a stream cipher based on another stream cipher named SNOW-3G. SNOW-3G has a classical stream cipher structure, producing a continuous key stream. It is built on Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM).

•"0010": 128-EEA2. The EEA2 is a stream cipher based on the block cipher AES algorithm used in its CTR (Counter mode) mode. In Cryptography, modes of operation are the procedure of enabling the repeated and secure use of a block cipher under a single key. The counter mode can do that operation as a stream cipher. Typically, the last block must also be extended to match the cipher's block length using a suitable padding scheme. The counter mode has significant efficiency advantages over the standard encryption modes without weakening the security.

The encryption/decryption takes place in the terminal and in the Radio Network Controller (RNC) on the network side. This means that the cipher key CK has to be transferred from the core network to the radio access network. This is done in a specific Radio Access Network Application Protocol (RANAP) message called Security Mode Command. After the RNC has obtained CK it can switch on the encryption by sending an RRC Security Mode Command to the terminal.

The EEA encryption/Decryption mechanism is based on a stream cipher as described in Figure 3 which is duplicated from [1]. Input parameters of EEA are the same as for the UMTS encryption function f8. They are as follow by combination of [4] and [7]:

•COUNT-C: The encryption occurs in either the Medium Access Control layer (MAC) or in the Radio Link Control layer (RLC). In both cases, there is a counter that changes for each Protocol Data Unit (PDU). In MAC this is Connection Frame Network (CFN) and in RLC a specific RLC Sequence Number (RLC-SN).if these counters were used as such as input for the mask generation, reply of message could still occur since these counters wrap around very quickly. This is why no longer counter called a Hyperframe Number (HFN) is introduced. It is incremented whenever the short counter (CFN in MAC case and RLC-SN in RLC case) wraps around. The combination of HFN and the shorter counter is called COUNT-C and is used as an ever-changing input to the mask generation inside the encryption mechanism [4] and [7].

In principle, the longer counter HFN could also eventually wrap around. Fortunately, it is reset to zero whenever a new key is generated during the authentication and key agreement procedure. The authentication events are in practice frequent enough to rule out the possibility of HFN wrap-around.

•BEARER: The radio bearer identity BEARER is also needed as an input to the encryption algorithm since the counters for different radio bearers are maintained independently of each other. If the input BEARER was not in use then this could again lead to a situation where the same set of input parameters would be fed into the algorithm, and

the same mask would be produced more than once. Consequently, reply of message could occur, and the messaged encrypted with the same mask would be exposed to the attacker.

•DIRECTION: the parameter DIRECTION indicates whether uplink or downlink traffic is encrypted. This is only one bit information in the key-stream. The parameter 0 indicates uplink while 1 indicates downlink.

•LENGTH: the parameter LENGTH indicates the length of the data to be encrypted. Note that the value of LENGTH affects only the number of bits in the mask bit stream; it does not have an effect on the bits themselves in the generated stream.

The combination of all these parameters and key make EEA algorithm operation succeed. The output is called Key-stream Block. Then after stream cipher will come in the operation sequence. A stream cipher will XOR Key-stream block and plain text and get the result as Cipher Text. A cipher text will be send to the receiver. On the receiver side, a Key-stream Block is or has already ready to get XORed with Cipher Text and get Plain Text back.

Encryption Algorithm EEA2 Operation

The EPS confidentiality algorithm EEA2 uses the block cipher AES as a kernel. Moreover, UEA1 based on K_{ASUMI} algorithm and EEA2 based on AES algorithm were apparent as proper choices as of fulfilling all security requirements for EEA and UEA individually. The reasons for selecting AES for the LTE confidentiality algorithm compared to UEA1 in UMTS which uses the block cipher K_{ASUMI} are given as below:

•eNB needs to support NDS/IP (Network Domain Security/ Internet Protocol) which uses AES. Hence, eNB has to support AES in any circumstance since it has to support NDS/IP.

•The licensing conditions on the core of UEA1/UIA1 (KASUMI) do not make it free for use for other purposes than 3GPP access protection.

•Similarity with other non-3GPP accesses.

The process of Key-stream generation and encryption/decryption will be described below

Key-stream Generation

The Key-stream is one of the inputs of EEA algorithm. For CTR mode stream ciphering it is required that Key-stream T has to be 128-bit long. Therefore, Key-stream T1, T2, T3…Ti… is constructed as follows:

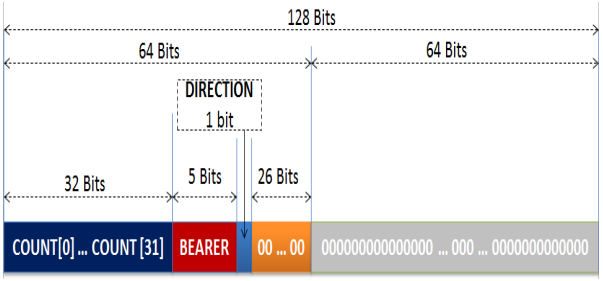

Figure 4: First 128-bits Key-stream T1

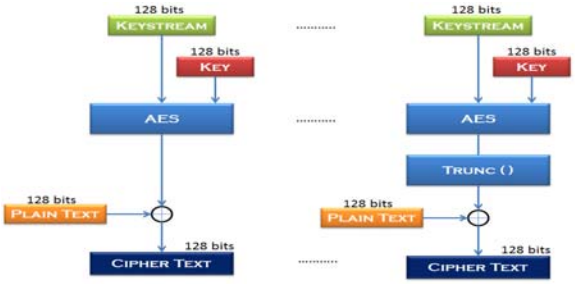

Figure 5: EEA2 Encryption Structure

Figure 4 shows the counter construction as duplicated from [4]. The details about COUNT, BEARER, and DIRECTION are explained before. The most significant bit starts from left to right in the figure as color of individual block goes from dark to light. The most significant 64 bits of T1 consist of COUNT [0] ... COUNT [31] || BEARER [32] … BEARER [36] || DIRECTION [37] || 026 (26 zero bits). Regarding most valuable bit, COUNT [0] is the most significant bit of T1. The least significant 64 bits of T1 are all 0 as shown in the figure. The main purpose of doing this is to make key stream 128-bits so it can be used as an input in 128-bits encryption algorithm. Subsequent counter blocks are then obtained by applying the standard integer incrementing function mod 264 to the least significant 64 bits of the previous counter block.

EEA2 Encryption/Decryption Operation

AES does process 128-bit input at a time and that should be the standard according to National Institute of Standard and Technology (NIST). Hence, the plain text has to be separated in 128-bits block by encryptor to encrypt payload with AES-CTR. The final block can be less than 128-bits. Encryption process occurs as shown in Algorithm 1.

Algorithm 1: Encryption process occurs

PT = PT [1] PT[2] … PT[n]
The key-stream T is 128-bits as explained above,
T: = COUNT || BEARER || DIRECTION || 026 || T0
Where T0 represents 64 bits zeroes.
FOR i := 1 to n-1
CT[i] := PT[i] XOR AES(T)
T0 := T0 + 1
END
CT[n]:= PT[n] XOR TRUNC (AES (T))

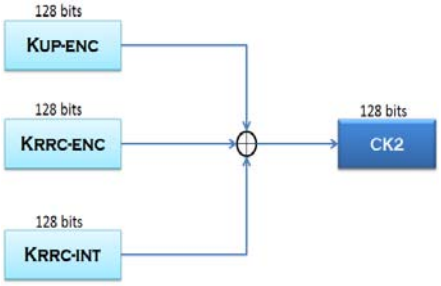

Figure 6: Generation of Cipher Key2 (CK2)

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].

Figure 5 illustrates EEA2 Encryption/Decryption structure as described in [4]. The decryption operation has the same process as encryption. At the receiver side the key-stream block has been already prepared to XOR with cipher text and gets the plain text. One thing has to be noted here that for both encryption and decryption operation, AES-CTR uses only AES encryption algorithm to make AES-CTR smaller than implementations of many other AES modes.

EPS IMPROVED SECURITY STRUCTURE

EPS Encryption algorithm has explained in last section, especially EEA2 algorithm mechanism. It has to be noticed that the plain text is only XORed with the key-stream block and get the cipher text by using CounTer Mode. The idea of stream cipher is based on simple but yet secured cipher called the one-time pad. Stream cipher is calculated:

"Cipher Text = Plain Text Key-stream Block"

The one-time pad is secure. On the other hand, the one-time pad has one major weakness: secure transport or storage of the key becomes as demanding a task as secure transport or storage of the plaintext itself. But still one main advantage of a stream cipher is the fact that the mask bit stream can be generated in advance, even before the plaintext is known. This helps avoiding delays in the communication.

Another advantage is that the number of erroneous bits in the ciphered message introduced by a noisy channel equals the number of erroneous bits in the recovered plaintext; whereas, for a block cipher, one bit error in a ciphered block typically renders the entire block of recovered plaintext unintelligible. This is the reason why stream ciphers are often used for channels with relatively high bit error rates, such as radio channels. This section will describe the proposed stream cipher improvement so it can make the security architecture more secure.

EPS algorithm selection is dependent on the contained information in each key K_{RRCenc}, K_{RRCint} and K_{UPenc}. These keys are derived from K_{eNB} [2]. A new Cipher Key CK2 can be derived by XOR operation of KRRCenc, KRRCint and KUPenc as shown in the Figure 6.

The 4-bits identifiers explained in the beginning of section 4. They are 0000, 0001 and 0010. The literature review demonstrates that 3GPP technology uses bit wise rotation operation for deriving different function such as f1,f2,f3,f4,f5 to generate several keys. Hence, the combination of identifier and bit wise rotation operation can be used to make EPS security mechanism more secure.

EEA Proposed Encryption/Decryption Operation

As it has shown in the previous section that EPS uses only XOR operation to get plain text ciphered. Now, another key which we propose is generated as shown in Figure 7, CK2 and dynamic bit wise rotation operation which is dependent on identifier we used in our new proposed algorithm mechanism. In algorithm, we do the encryption of n plaintext blocks as shown in Algorithm 2.

The block wise operational demonstration is shown in the Figure 7.

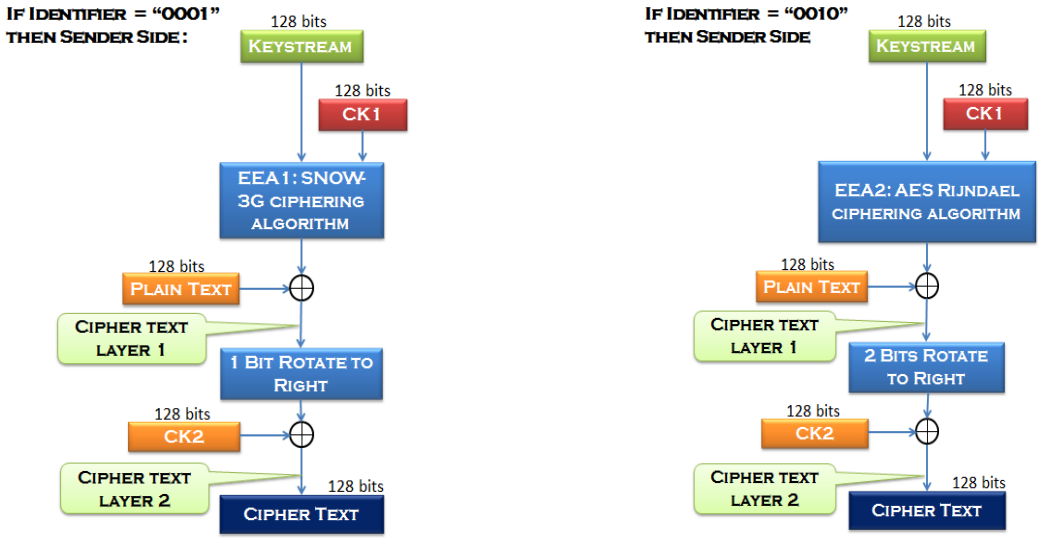

Figure 7: Ciphering Algorithm Mechanism on Sender Side (0001 and 0010)

The sender will transmit cipher text to the receiver. At the receiver side the plain text will get back by apposite operation of encryption. Here, it has to be noted that deciphering operation also uses AES encryption algorithm to decrypt the cipher text. The decryption of n cipher text blocks can be summarized below in Algorithm 3.

Algorithm 2: encryption of n plaintext blocks

1: IF identifier = "0001"
2: Then
3: Key-stream[i]:= PT[i] XOR AES ( )
4: Key-stream Block: = Rotate Key-stream[i] 1 bit to right
5: Cipher Text[n]:= CK2 XOR Key-stream Block
6: IF identifier = "0010"
7: Then
8: Key-stream[i]:= PT[i] XOR AES ( )
9: Key-stream Block[j]: = Rotate Key-stream[i] 2 bits to right
10: Cipher Text[n]:= CK2 XOR Key-stream Block[j]
11: END

Algorithm 3: decryption of n cipher text blocks

1: IF identifier = "0001"
2: Then
3: Key-stream[i]:= Cipher Text[i] XOR CK2
4: Key-stream Block[j]: = Rotate Key-stream[i] 1 bit to left
5: Plain Text[n] := AES ( ) XOR Key-stream Block[j]
6: IF identifier = "0010"
7: Then
8: Key-stream[i]:= PT[i] XOR CK2
9: Key-stream Block [j]: = Rotate Key-stream[i] 2 bits to right
10: Plain Text[n]:= AES ( ) XOR Key-stream Block [j]
11: END

The block wise decryption operational demonstration is shown in the Figure 8.

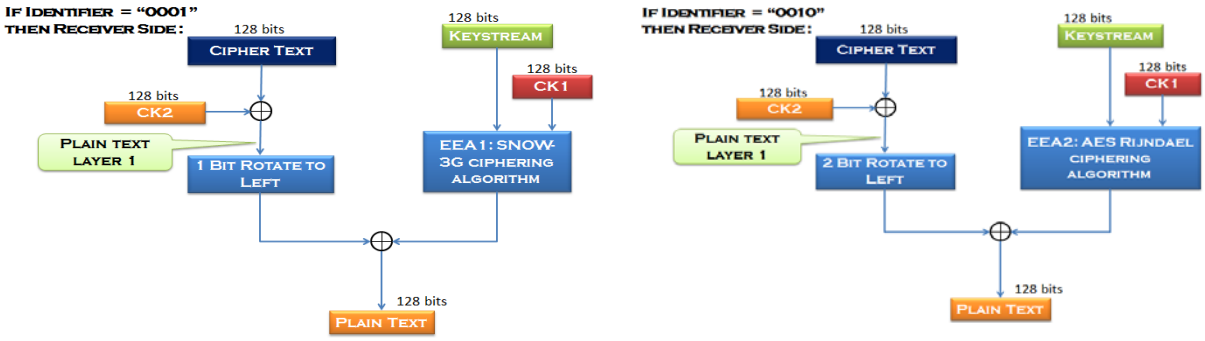

Figure 8: Deciphering Algorithm Mechanism on Sender Side (0001 and 0010)

The advantage or plus points of making improvements in EPS confidentiality algorithm (EEA) are as follow:

- The main advantage of AES encryption for key stream rather plaintext or cipher text is, a mask will get ready before the cipher text comes at the receiver side. Also the key CK2 will be ready even before the cipher text comes. This method does save time compare to using AES algorithm directly for plain text.
- The second Cipher key2 (CK2) is the result of XOR operation of three inputs. Therefore it is one way process and not possible to get any input component of CK2 key generation algorithm.
- If an attacker tries to get plaintext by breaking this algorithm, he has to go through XOR operation of CK2 and key-stream block which is rotated bitwise. It is kind of impossible to get Cipher Key2 since it will not be shared by UE and eNB.
- The XOR and bitwise operations do not take as much time as AES and also increase the complexity in the security mechanism.

EEA Proposed Algorithm Cipher/Decipher Implementations

The simulation experiment is done by using MATLAB version R2010a simulator. The MATLAB code for basic AES simulation was employed from [8]. The proposed algorithm was added to get the output such as input parameters, cipher key. The input parameters set in the simulator are illustrated in Table 1 below.

Table 1: The input Parameters used for Proposed EEA Security

INPUT PARAMETERS	PARAMETER VALUES
Keystream_Hex	54 4d 49 cd 20 00 00 00 00 00 00 00 00 00 00 00
CK1_Hex	0a 8b 6b d8 d9 b0 8b 08 d6 4e 32 d1 81 77 77 fb
KUPenc_hex	2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
KRRCint_hex	88 35 a9 2a 83 b1 bd c1 aa 8b a1 4b 26 91 36 7b
KRRCenc_Hex	73 7e ee 32 87 77 7c 9a 9c 4a d8 26 3a 44 db 65
Plain Text	LTE security is an essential part of latest communication system

Table 2: The Output Parameters from proposed EEA encryption algorithm

OUTPUT PARAMETERS	PARAMETER VALUES
AES Cipher_Hex	88 83 aa 26 35 b1 8b 91 a9 bd a1 362a c14b 7b
CK2_Hex	d0 35 52 0e 2c 68 13 fd 9d 36 6c e5 15 1a a2 22
Identifier	0010
Cipher Text	ámi]¤Ð«i$óô ªã0ÝØ%*\.bw` ïpãÄ$?D¥t§ ¯ãb\&V¬ÜØ i@cv§

Table 3: The Output Parameters from proposed EEA decryption algorithm

OUTPUT PARAMETERS	PARAMETER VALUES
AES Decipher_Hex	54 4d 49 cd 20 00 00 00 00 00 00 00 00 00 00 00
Plain Text	LTE security is an essential part of latest communication system

In Table 1, Key-stream_hex and CK1_hex are the input parameters used for AES algorithm. Key-stream_hex is the Key-stream parameters: COUNT= 544d49cd, BEARER=04 and DIRECTION=0. CK1_hex is the Cipher Key1 used to process AES encryption as well as decryption algorithm operation. K_{UPenc}_hex is K_{UPenc} key, K_{RRCint}_hex is the KRRC-int key, and K_{RRCenc}_hex is K_{RRCenc} key which will be used to get Cipher Key2 (CK2). Plain Text is the text which has to be encrypted and send it to the receiver. This is the main data that needs to send the other end of the network. In the MATLAB coding, CK2 is used as the Cipher Key2. Identifier indicates what algorithm will be used. Identifier will be either 0001 or 0010 in EEA. The final Cipher Text output of stream cipher is named as Cipher Text. The output is as followed in Table 2.

The AES Cipher_hex is the output of AES ciphering which is Rijndael ciphering algorithm. AES will occur with CK1_hex and Key-stream_hex which are described above. An Identifier is the selection of whether EEA1 or EEA2 algorithm. Here, identifier is 0010; therefore the system will select EEA2 security mechanism. Cipher text is the final output of algorithm therefore it can be anything in ASCII code such as numbers, symbols or alphabetic characters. Here, Cipher Text is the result of ciphering "LTE security is an essential part of latest communication system". Now cipher text will be sent over the other end of the network. The mask will be ready before the cipher text arrives to the receiver side. The decryption output is shown in Table 3.

The AES Decipher Hex is the output of AES decryption operation. Eventually, this decryption process is not in use in EEA structure. Plain Text (PT) is the output at receiver side after decryption operation of the AES-stream cipher, AES-CTR. These both output results can be compared with the input parameters.

CONCLUSION

In this study we proposed an algorithm that allows more complex algorithm for the encryption in the security process. We show in MATLAB how our new algorithm works in relation to the original algorithm. We demonstrate that it does not add significant time to the encryption and decryption processes as the algorithm becomes more complex. Our algorithm and the method behind it can be employed in any system that takes advantage of LTE-advanced technology. In future we are planning to investigate the efficiency of the proposed algorithm by performing more tests and comparing the results to those of other proposed solutions.

REFERENCES

[1]. 3GPP TS 33.401: "Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture; (Release 8)", V8.6.0 (2009-12).

[2]. 3GPP specifications: http://www.3gpp.org

[3]. 3GPP TR 33.901 V4.0.0 (2001-09): "3rd Generation Partnership Project Technical Specification Group Services and System Aspects 3G Security Criteria for cryptographic algorithm design process" release4.

[4]. Ghizlane ORHANOU, Said EL HAJJI, Youssef BENTALEB and Jalal LAASSIRI, "EPS Confidentiality and Integrity mechanisms Algorithmic Approach", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 4, July 2010

[5]. Masoumeh Purkhiabani and Ahmad Salahi, January 2012 "Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks"

[6]. Alf Zugenmaier, Hiroshi Aono Motorola "Special Article on Security Technology for SAE/LTE".

[7]. Dan Forsberg, Gunther horn, Wolf-Dietrich Moeller, Valtteri Niemi, "LTE Security" , John Wiley & Sons, Ltd, 2010

[8]. Jorg J. Bucholz, "MATLAB Implementation of the Advanced Encryption Standard", December, 2001. http://buchholz.hs-bremen.de