Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.1124 – 1132

RESEARCH ARTICLE

Implementation of Enhanced AKA in LTE Network

Noor Kareem Jumaa (Asst. Lecturer)

Al-Mansour University College, Iraq

Computer Technology Department

Abstract—4G LTE (Long Term Evolution) network is the latest deployed cellular network technology that provides high-speed data services for mobile devices. It seeks to take mobile technology to the next level through the realization of higher bandwidths, better spectrum efficiency, wider coverage, and full interworking with other access/backend systems. LTE new architecture is a flat IP architecture; it therefore comes with all security issues inherent in IP network; its' security cryptography, trips on the good features of AKA cryptographic algorithms. So, LTE security architecture evolution is the state of the art concerns in LTE network. AKA (Authentication and Key Agreement) which defines the protocol through which the User Equipment (UE), the Home Subscriber Server (HSS), Mobility Management Entity (MME) which are mutually authenticated and the mechanism through which the master encryption keys are generated with the LTE Certification Agency (CA). This paper reviews the security issues in LTE network, analyze the AKA protocol, enhance a proposed AKA by increase its security level, and analyze the implementation of AKA which is based on an enhanced version of SEAP AKA.

Keywords— 4G, LTE, Security, AKA, SEAP, MD5.

I. Introduction

Because of the lower latency and higher bandwidth than its predecessor 3G networks, the latest technological design for mobile telecommunications that appears to be the future communications architectural baseline is the 4G architecture, also called SAE (System Architecture Evolution). Long Term Evolution (LTE) is the latest buzzword on everyone's lips. [1, 2]

Fig. (1) below shows the most common design view of the LTE network which describe a non-roaming architecture with a 4G mobile device and only 4G access to the network. The entities that appear in this architecture are: [1]

I. UE (User Equipment)
II. eNodeB (the antenna)
III. MME (Mobility Management Entity)
IV. SGW (Serving Gateway)
V. PGW (PDN (Packet Data Network) Gateway)
VI. HSS (Home Subscriber Server)
VII. PCRF (Policy Charging Rules Function)

All the entities mentioned above are connected together in a 3G access network where the UE can roam to. [1]

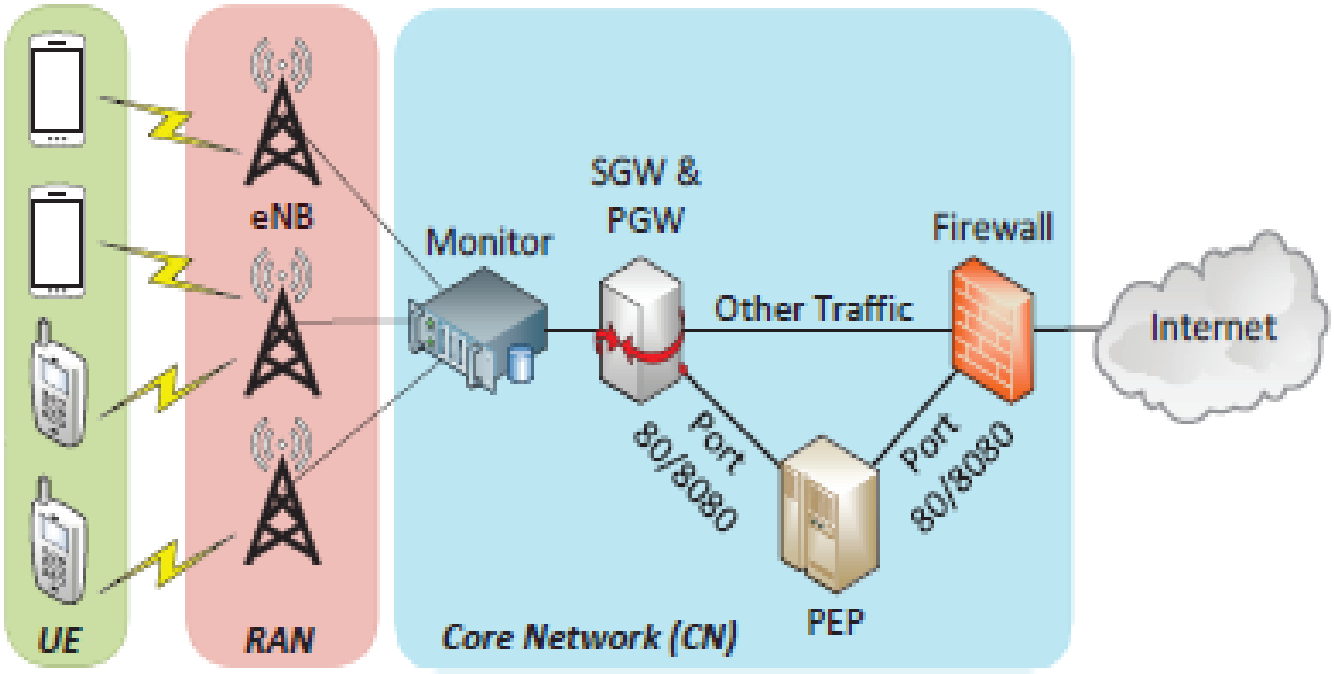


Fig. 1: LTE Reference Architecture. [2]

Two distinct components are performing the overall architecture: [3, 2]

1. The access network which Evolved Universal Terrestrial Radio Access Network (E-UTRAN) or some times just called RAN.
2. The core network or sometimes called the Evolved Packet Core (EPC) is perform all-IP core network and is fully Packet Switched (PS).

E-UTRAN and EPC together constitute the Evolved Packet System (EPS). EPC contains network control entities apart from the network entities handling data traffic, for keeping user subscription information represented by Home Subscriber Server (HSS), determining the identity and privileges of a user and tracking his/her activities. [3, 4]

Since LTE/SAE's new architecture is a flat IP architecture, it comes with all security issues inherent in IP network and its' security cryptography rides on the good features of AKA cryptographic algorithms in 4G LTE network [5]. Authentication of subscriber in EPS is depended on key agreement protocol since it provides mutual authentication between UE and core network ensuring robust charging and guaranteeing that no fraudulent entities can pose as valid network node. When a failure occurs in the home network, mobile station may not accept the authentication vector generated by the home network and this phenomenon causes the loss of synchronization. Each user in the network has two counter used to authenticate the user in the network; synchronization is needed to adjust the counter of the user in home network. Problems of the most designers comes from the task of 4G assessing the internet from a fixed location and mobility, coupled with the fact that cryptographic enhancement keeps evolving with new security threat and computation should not supersede performance. Exposed that, the security enhancement of AKA in GSM was with public review of encryption algorithm by the security community, encryption key with 128 bit length increased from 64 bits formerly used in GSM, mutual authentication and mandatory integrity between wireless terminals and the network unlike the unidirectional in GSM, and finally, encryption from terminal to a node beyond the base station. [5, 6, 7]

II. LTE Security Concerns

LTE security has five main concern areas: [1]

1. Network Access Security: This refers mostly to the radio attacks.
2. Network Domain Security: It defines the requirements and rules to prevent attacks over the wire, when exchanging control-plane and user-plane.
3. User Domain Security: It is dealing with securing the access to mobile terminals.
4. Application Domain Security: This standardizes the set of rules for secure message exchange between applications on clients and servers.
5. Visibility and Configurability of Security: It is a set of features that informs the user about a particular security feature and whether this feature is applicable or not to the services this user is trying to access.

AKA (Authentication and Key Agreement) Protocol is needed when the access medium is LTE.
AKA is a protocol contains a fixed steps related among the MME (Mobility Management Entity) which performs the authenticator, HSS (Home Subscriber Server) which is the authentication server, and the UE (User Equipment).
The communication between the MME and the HSS takes place over S6a and it uses Diameter as a protocol. The mobile terminal (UE) has a UICC (Universal Integrated Circuit Card) inside. UICC circuit stores the K, a located shared key between UE and HSS as well as on the AuC (Authentication Center) entity part of the HSS. The authentication in 4G is used a shared secret symmetric authentication key.
The purpose of the AKA mechanism is to create both ciphering and integrity keys for the RRC (Radio Resource Control) signaling, NAS (Non-Access Stratum) signaling and for the user plane. [1, 5, 7]

III. SEAP_AKA Protocol

SEAP_AKA protocol was first proposed in [5]. In the proposed protocol, all the transections among UE, MME, and HSS are encrypted in order to increase the security level of the authentication in the network. In LTE network, there are three security vectors should be fully protected against attackers:

1. IMSI (International Mobile Subscriber Identity): which is a 15 digit private number used as user authentication sequence. IMSI should be hidden and never sent in the clear, which results in a higher degree of privacy.
2. SNID (Serving Network Identity): MME_ID known as SNID, this vector should be encrypted and hidden from attackers.
3. AV (Authentication Vector): generated by HSS to authenticated n of users in the network, this vector should be encrypted too.

SEAP_AKA proposed the following steps:

1. UE, MME, HSS shall acquire the digital certification via CA, and acquire the public key PK
2. Subscriber initiates access request:
    a. UE uses HSS public key H PK which is stored in smart card to encrypt IMSI and get A
    b. UE sends {A, HSS ID} in access request to MME
    c. After MME receives the access request from subscriber, it adopts the public key H PK to encrypts its own network identity SNID, and derive the encryption information B
    d. A and B are regards as authentication data requests and delivered to HSS
    e. After receiving the authentication data request from MME, HSS uses its own private key H SK to decrypt A and B to get IMSI and SNID
3. HSS checks the validation of IMSI and SNID from registration subscriber list and authorization service network list maintained in the database.
4. If MME and SN identities have been verified, HSS will generates the random number array RAND{1,…….,n} and the group of authentication vector AV{1,……,n}

Proposed system in this paper based on SEAP_AKA but with more security features which resulting in the increasing of the AKA security level.

IV. Proposed AKA Protocol

The proposed AKA is based on SEAP_AKA. The enhanced SEAP Authentication protocol E_SEAP_AKA. The structure of E_SEAP_AKA is shown below in Fig. (2).

The E_SEAP_AKA protocol steps performed by the following steps:

1. UE, MME, and HSS asking the CA (Certification Agency) for the HSS Public Key (H PK). H PK is used to encrypt IMSI and SNID.
2. CA broadcast an acknowledgement message contains a code consists from one digit, this code should be sent over a secure communication.
3. After UE, MME, and HSS have receive the code from the CA, they run an internal secure algorithm –Message Digest5 MD5 random secure key generation is used- and a truly secure random secret key (SK) is generated using MD5 algorithm with 128 bit length.
4. UE use the SK and encrypt the IMSI using 128 AES cryptographic algorithm and a cipher message called A is generated.
5. UE transfer the cipher message A to MME.
6. MME save the received message A, after that MME encrypt the SNID using the SK and 128 AES cryptographic algorithm and the cipher message B is generated.
7. MME transfer A and B to HSS.
8. HSS used the SK generated by the MD5 algorithm and 128 AES cryptographic Algorithm to decrypt A and B. the decryption of message A resulting IMSI and from the decryption of B the SNID is obtained.
9. HSS checks if IMSI and SNID are valid for a valid user, if the so, HSS generate the AV and random vector RAND for users from 1 to n by using a random number generator algorithm –in this proposed system the golden code algorithm is used-.

Fig. (3) shows the encryption system and Fig. (4) shows the decryption system.

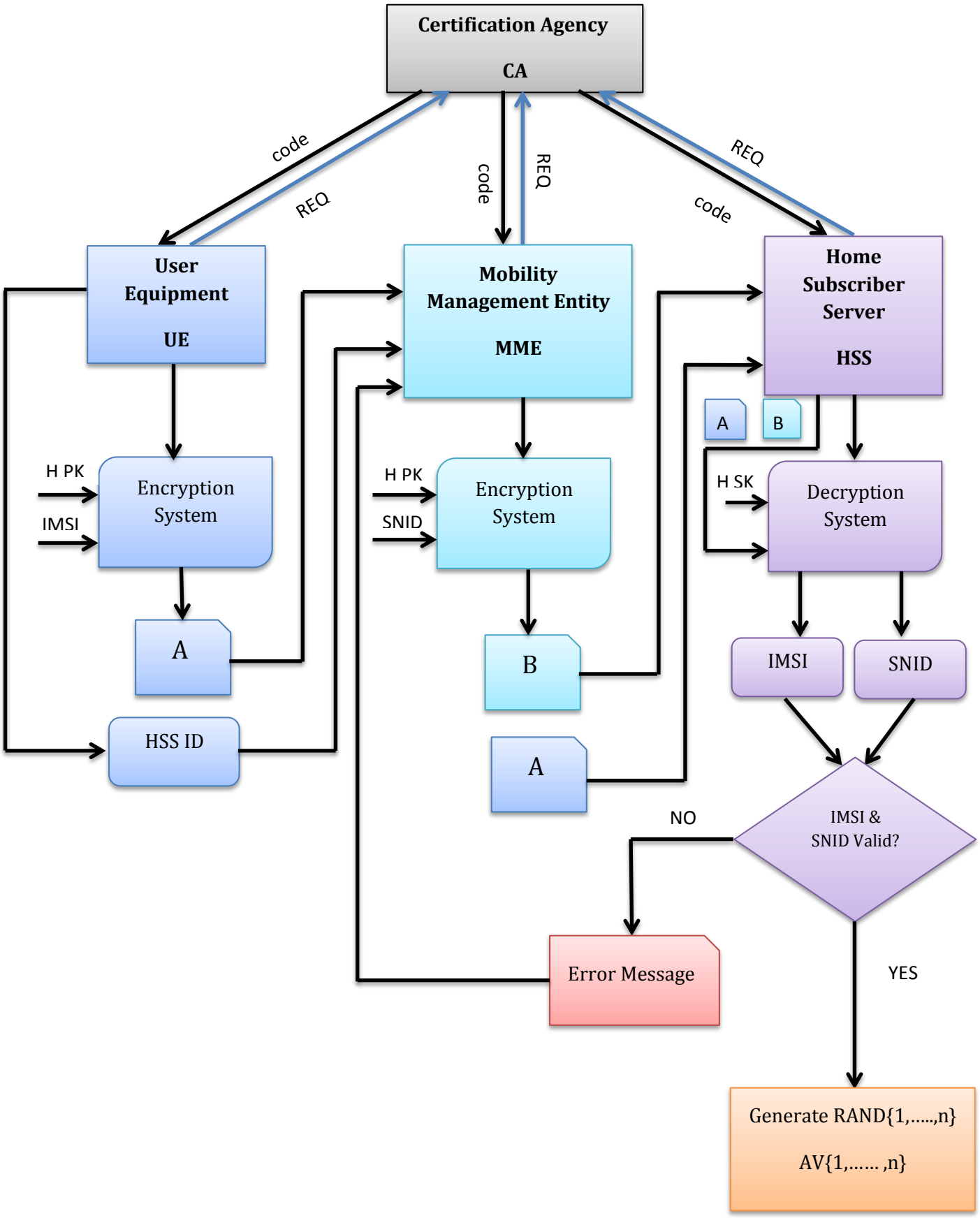


Fig. 2: Proposed AKA Structure.

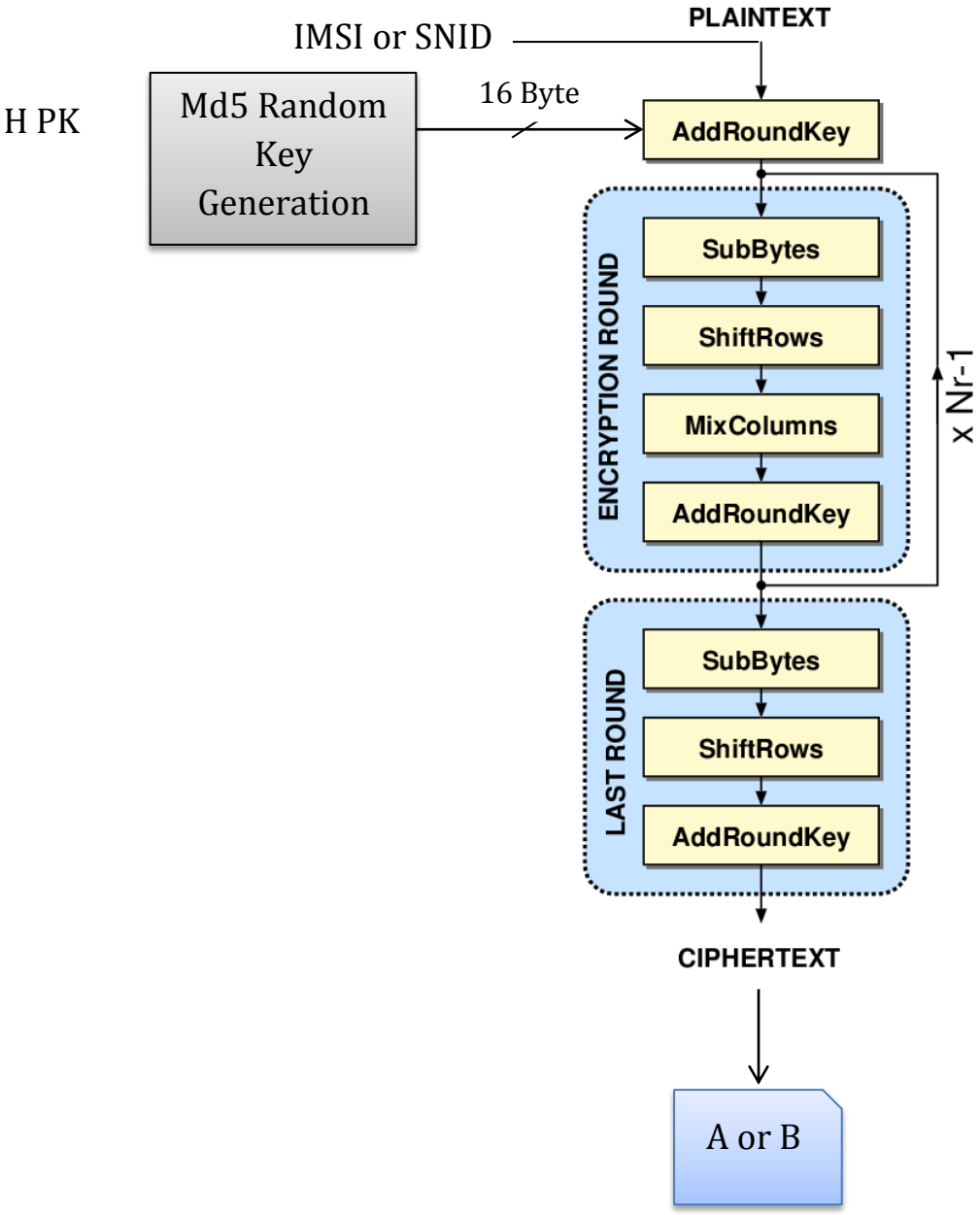


Fig. 3: Encryption System of the E_SEAP_AKA Protocol.

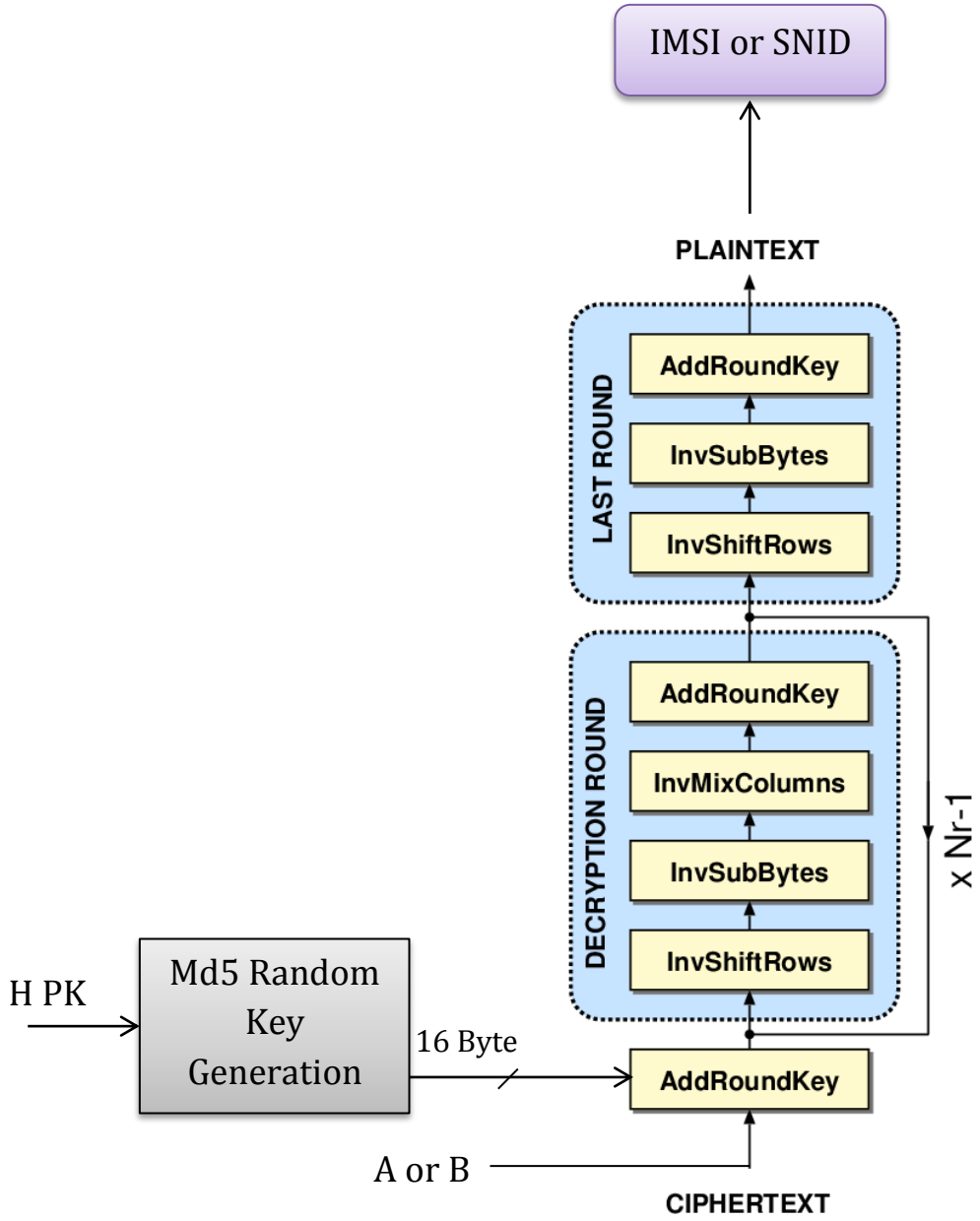


Fig. 4: System of the Protocol.

Decryption E_SEAP_AKA

V. Power Features and Security Measurements of the Enhanced System

The proposed system E_SEAP_AKA has many powerful features over the traditional SEAP_AKA. E_SEAP_AKA powerful features perform in the following points below:

1. Transfer a code on secure channel from the CA to UE, MEE, and HSS instead of the HSS PK prevent the attackers from ciphering faked data using the HSS PK.

2. Truly random secure key for encryption and decryption generated using MD5 random number generated prevent the attackers from knowing the original messages.
3. 128 bit AES cryptographic algorithm has 2^{128} possible keys for the attacker to try if they enabled from catching the ciphertexts. This is impossible to achieve.
4. Using Golden code to generate the AV and RAND generate a truly random secure vectors.

Table (1) shows the security featured of the proposed E_SEAP_AKA system.

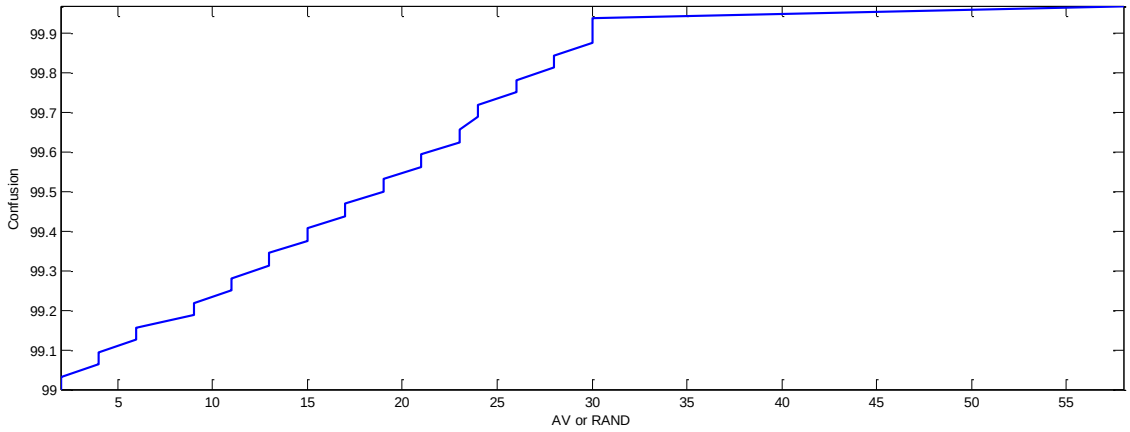
Table 1
E_SEAP_AKA Security Features.

Ciphertext confusion	100%
Ciphertext Diffusion	100%
Security against the brute force attack	100%
Repeated number inside the vector	0%

Fig. (5) below shows the relationship between the Random Vector length of AV and RAND with their confusion.

Fig. 5: Confusion of AV and RAND Vectors.

From Fig. (5) above, it could be consider that the security confusion of AV and RAND vectors ranged from 99 to 100 which perform a very high confusion level.



From the above security featured, the proposed system E_SEAP_AKA can considered as a powerful secure AKA protocol.

VI. Conclusions

An Enhanced SEAP_AKA was designed and implemented in this research. E_SEAP_AKA has a security level higher than the security level of the traditional SEAP_AKA; since E_SEAP_AKA contains a truly random secure algorithms such as the MD5 and the Golden code which provide a confusion and diffusion ranged between 99% to 100%. So, the proposed system considered as a flexible and lightweight AKA protocol suited for use in the mobile device environment. With the new enhancements and the SEAP_AKA features such as the elimination of the synchronization needing and decreasing the network corruption, the SEAP_AKA is efficient AKA protocol without compromising security.

REFERENCES

[1] Cristina-Elena Vintilă, Victor-Valeriu Patriciu, and Ion Bica, " **Security Analysis of LTE Access Network**", IARIA, The Tenth International Conference on Networks, ISBN:978-1-61208-113-7, 2011.

[2] Junxian Huang, Feng Qian, Yihua Guo, Yuanyuan Zhou, Qiang Xu, and Z. Morley Mao, " **An In-depth Study of LTE: Effect of Network Protocol and Application Behavior on Performance**", *SIGCOMM*, Hong Kong, China, 2013, Copyright © 2013 ACM 978-1-4503-2056-6/13/08.

[3] T. Ali-Yahiya, " **Understanding LTE and its Performance**", DOI 10.1007/978-1-4419-6457-1_2, Springer Science+Business Media, LLC 2011.

[4] 3GPP TS 24.301: Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS): Stage 3.

[5] Uwaya Fidelis and Madhavi Kumari, " **ENHANCED ADAPTIVE SECURITY PROTOCOL IN LTE AKA**", IJCSMC, Vol. 3, Issue 10, pg.584 – 594, 2014.

[6] Seddigh N., Nandy B. , Makkar R. , and Beaumont, J.F. , "**Security Advances and Challenges in 4G Wireless Networks**", IEEE Ottawa conference, Page(s): 62 – 71, E-ISBN : 978-1-4244-7549-0, Print ISBN: 978-1-4244-7551-3, 2010.

[7] Joe-Kai Tsay and Stig F. Mjølsnes, "**Computational Security Analysis of the UMTS and LTE Authentication and Key Agreement Protocols**", arXIVE: 1203.3866v2, cs.cr, 2012.

