Authentication and Key Agreement Scheme for CDMA Cellular System

Mohammed Ramadan[1], Fagen Li[2], Chun Xiang Xu[3], Kwame Oteng[4], Hesham Ibrahim[5]
School of Computer Science and Engineering,
University of Electronic Science and Technology of China
Chengdu 610054, P.R. China
e-mail: [1]nopatia@gmail.com, [2]fagenli@uestc.edu.cn, [3]chxxu@uestc.edu.cn, [4]kermaabar@yahoo.com;
[5]hesham21060@hotmail.com

***Abstract* - The code division multiple access (CDMA) system is considered to be the most secured cellular standard because of its strong security techniques such as scrambling and interleaving. These security techniques have been improved from the GSM security system. However, the CDMA cellular standard still has some limitations particularly in term of authentication and key agreement process. In this paper, a new authentication and key agreement protocol is proposed to provide a security technique to ensure the mutual authentication of both the mobile station and the network provider, as well as provide a key agreement protocol for session keys by using short and efficenent signature with bilinear pairing method with some modifications to make the proposed scheme more compatible for the CDMA cellular system.**

Keywords-CDMA Security; CDMA-PKI; CDMA-AKA; CDMA-Signature.

I. INTRODUCTION

Wireless communication security entails the measures or techniques used to protect the communication between certain entities. Code Division Multiple Access (CDMA) is a form of spread spectrum whereby the signal is transmitted on a bandwidth much larger than the frequency of the original information. That is to say, the transmitted signal bandwidth is much greater than the information bandwidth. Spread spectrum uses wide-band, noise-like signals, hence making it hard to identify. The band spread is realized by a pseudo-random code, which is not depend on the data. Security has become a key topic in current mobile and wireless networks. The pseudo noise (PN) sequences are a sequence of 1's and 0's where the numbers look like they are statistically independent and uniformly distributed. They are also randomly arranged, implying that they can be mathematically generated. However, they statistically satisfy the necessities of a strictly random sequence in the limiting sense. For the Direct-Sequence (DS) CDMA system, the user signal is multiplied by a pseudo-noise code sequence of high bandwidth. This code sequence is also referred to as the chip sequence. The resulting coded signal is transmitted over the radio channel [1]. CDMA systems, both direct sequence and frequency hopping used for military purposes, where the need for signals displaying anti-jam and low probability of intercept characteristics was vital.

Thus, they were usually designed to be wideband, and those that used DS to realize multiple access capabilities were the original prototypes of what is now referred to as wideband CDMA. In the late 1980s, the utilization of DS-CDMA started to become more interesting to the commercial sector for use in cellular-type communications, and both narrowband CDMA and wideband CDMA systems were designed. This paper proposed a novel a scheme which provides authentication and key management agreement for CDMA system.

This paper proposes a novel a scheme which provides authentication and key management agreement for CDMA system, and it can take a good implementation in the field of mobile communication security which it needs lightweight algorithms to be able to implement on the mobile station and network operators components. Furthermore, the proposed scheme is consider to be more flexible and secure than the basic CDMA-AKA protocol as we presented in the following sections. The rest of the paper organized as follows: Section II Presents the CDMA security background, Section III presents the basic CDMA-AKA protocol, Section IV presents the limitations of the basic CDMA-AKA protocol, Section V and VI presents the proposed CDMA-AKA scheme and components, the performance evaluation and the security analysis of the proposed scheme is presented in Section VII. Finally, the conclusion and future scope is introduced in Section VII.

II. CDMA SECURITY BACKGROUND

As a digital communication system, security management is very straightforward to be achieved for CDMA. The security architecture for CDMA system defines security features intended to meet certain threats. It also sets up required security services for example network access security, to provide confidentiality of user identity and that of the user and signaling data. The integrity protection of important signaling data, authentication of user and network, and identification of Mobile Station (MS) is also done by this feature. The feature network domain security enables different nodes in the provider domain to securely exchange signaling data and also offers protection against attacks on the wire line network. The user domain security guarantees that only authorized access to Universal Subscriber Identity Module (USIM) is made. On the other hand, application domain security is used to enable applications in the user and provider domains to securely exchange messages [2, 3].

The figure 1 below illustrates the security parameters

and algorithms which are used in the fundamental CDMA security system:

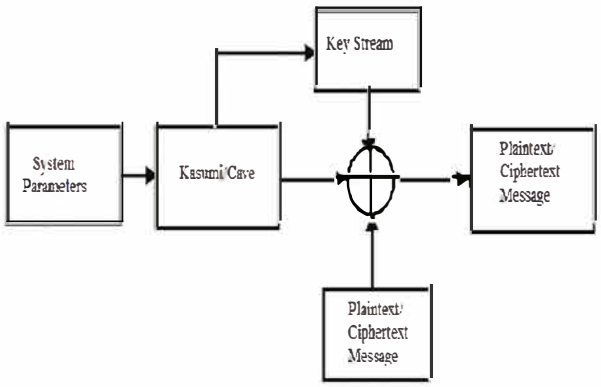

Figure 1. CDMA security procedures

The authentication algorithm in the fundamental CDMA system is enclosed within the smart card. The individual key for each IMSI must be chosen to be random, and must be safeguarded in order to prevent the user from being duplicated. Throughout the security process Ki should be protected [4].

III. THE BASIC CDMA-AKA PROTOCOL

In this section, the authentication and key agreement (AKA) protocols which are used in CDMA system are described. This protocol was designed within USECA and one of its design criteria, the compatibility with the security architecture of second generation systems. Furthermore, different methods for authentication and key agreement (AKA) are described. A vital characteristic of an AKA protocol is the goal the protocol achieves [5].

Entity authentication: for entity authentication of users to the network operator, a protocol employing random challenges as time variant parameters provides a guarantee to the network operator that the evidence was created during the current protocol run. A sequence number as time variant parameter only provides a guarantee to the network operator that the evidence was not employed in a prior protocol run.

Assurance of key freshness: to the network operator alludes to the fact that the network operator (HLR/AuC) can be sure that the keys obtained in the course of the AKA protocol were not employed before the current protocol run.

Key confirmation: for a user to the HLR/AuC provides an assurance to the HLR/AuC that the specific user holds the correct parameter(s) to derive the agreed keys. Key confirmation is the stronger aim and provides assurance to HLR/AuC that the specific user holds the derived key itself.

Goals of CDMA-AKA:

- Entity authentication of MS/USIM to HLR/AuC.
- Implicit key authentication of HLR/AuC to MS/USIM.
- Implicit key authentication of MS/USIM to the HLR/AuC.
- Assurance of key freshness to MS/USIM and HLR/AuC.
- Key confirmation from MS/USIM to HLR/AuC and vice -versa.
- Confidentiality of the user identity and other user related information from which the user identity may be obtained on the interface between MS/USIM and HLR/AuC. Also, if the transmission of the identity is not a component of the AKA and is instead provided by alternate means, the AKA must not prevent the provision of confidentiality of the user identity on the air interface. If the CDMA-AKA protocol does not offer key confirmation, then the usage of the agreed keys after a successful operation of the AKA, will (in case of a failure in one of the agreed keys) lead to problems in the messages protected by these keys and therefore to a break in the transmission of user/signaling data which otherwise could have been detected beforehand [6, 7].

The following figure 2 depicts the AKA protocol in the basic CDMA cellular standard:

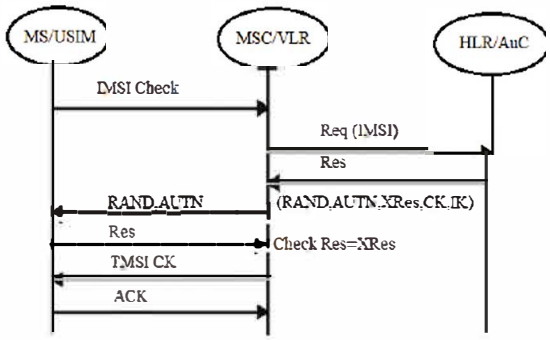

Figure 2. The basic AKA protocol in CDMA standard

IV. LIMITATIONS OF THE BASIC CDMA-AKA PROTOCOL

This section describes a threat model for the basic CDMA security on which the selection of security mechanisms is described. There are some important attacks on the CDMA-AKA and in this paper, emphasis is put on new attacks that were not possible when GSM was designed, but are now or are thought to be possible in the near future. Reasons for such added threats are e.g. that intruders have more computational abilities, new equipment have become accessible to attackers or the physical security of certain network elements is questioned.

A thorough analysis of the security threats and countermeasures cannot be presented here and as such, only some of the most important items are mentioned for brevity. Some of the most serious attacks discussed were based on the accessibility of supposed false base stations. A part of this problem is the so-called IMSI catching, which is a danger to the discretion of the user identity over the air interface. An additional type of attack analyzed was linked to an attacker taking control of the user's services. One vital result of the threat analysis was that some signaling elements were regarded as being sensitive and therefore having to be integrity protected. One of these signaling

elements is the secure mode command, which establishes whether or not ciphering is enabled and the ciphering and integrity algorithm to be used. Another example is the set of MS capabilities transmitted from the MS/USIM to the network operator, including authentication and key agreement mechanisms, ciphering algorithm and message authentication function capabilities. Corresponding contributions on threats and countermeasures were forwarded to 3GPP and formed a major input for the 3GPP technical report [3].

CDMA security system does not define a standard authentication algorithm; rather, it allows operators to pick their own versions, which conform to the published standards. However, in order to aid operators, guidelines are available as to how to develop an appropriate algorithm. Threats of medium significance include eavesdropping signaling or control data on the wireless or other interfaces; camouflaging as another user; manipulation of the terminal or USIM behavior by camouflaging as the creator of applications and/or data; camouflaging as a serving network; integrity of data on a terminal or USIM. As can be deduced from the above enumeration, the results of the threat analysis categorizes the main threats as coming from camouflaging as other users to get illegal access to services, eavesdropping which may result in the compromise of user data traffic privacy, or of call-related information like dialed numbers, location data, etc., and subscription fraud where subscribers take advantage of the services with heavy usage without any plan to pay.

What is new is the acknowledgment of threats which exploit more sophisticated, active attacks to achieve the eavesdropping or camouflaging [4].

These comprise of attacks which involve the manipulation of signaling traffic on the radio interface and where the intruder camouflages as a base station. Furthermore, attention is now not only focused on radio interface attacks, but also on other parts of the system [7, 8].

V. PROPOSED CDMA-AKA SCHEME

The proposed scheme achieves maximum compatibility with the current CDMA security architecture as much as possible. This proposed design provides mutual authentication and key agreement techniques for the CDMA cellular standard. This is achieved by using the hashed value of (IMSI\TMSI) with the pre-shared key (K) and the sequence code (PRN) to compute the session key which is changeable depending on the current parameters in case the mobile station is in its home area. Also, this paper uses the identifier IMEI as the message to be sent by the subscribers which is verified by the network operator and stored in both the MS and the HLR/EIR. The sequence code is derived for the spreading purpose in the scrambling process. The reasons to choose these parameters for this scheme will be explained in Section VII. The user and network operator can authenticate each other and compute the session key which is then stored in the MSC/VLR for encryption purposes and setup a secure network. The MSC\VLR in this case is only responsible to assign TMSI identifiers in case of visited users and storing the session key exchange for the encryption procedure. Therefore, the proposed scheme only needs two handshaking processes for both authentication and key agreement processes. However, the proposed scheme is based on short and efficient signature schemes to provide AKA scheme for the CDMA standard [9, 10]. As we presented in Section III, the basic existing CDMA-AKA scheme is challenge-response algorithm which it has many security weaknesses as false base station attack and IMSI catcher attack (See section VII). However, our proposed scheme solves such weaknesses with the same bandwidth consumption and handshaking process.

The following figure 3 explains the proposed CDMA-AKA architecture and the handshaking processes between the users and the network operator:

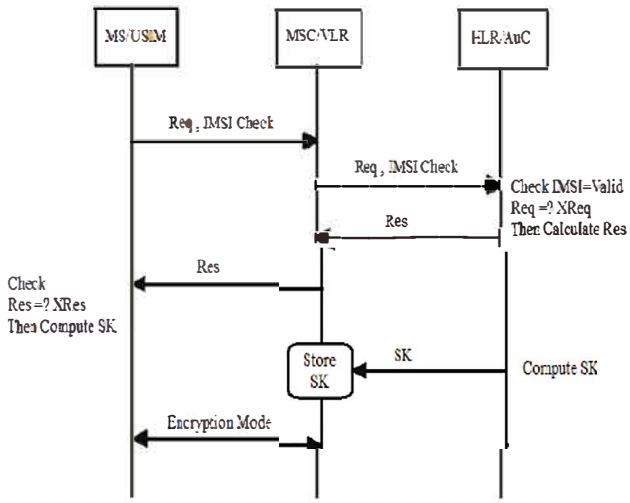

Figure 3.The proposed CDMA-AKA architecture

A. *Definitions:*

Below are some definitions which are essential to the proposed scheme [9].

B. *Mobile station (MS):*

The Mobile Station is made up of two parts, i.e. the Mobile Equipment (ME) and an electronic "smart card" namely, a Subscriber Identity Module (SIM) card.

C. *Mobile Switching Center (MSC):*

The key role of an MSC is call- switching in a GSM system. Its general function is basically the same as that of any telephone exchange.

D. *Home Location Register (HLR):*

Is the ultimate database of mobile subscriber information for a wireless carrier's network. It is the real-time list that links phones, phone numbers, user accounts and service plan information.

E. *Visitor Location Register (VLR):*

The VLR holds a copy of nearly all of the data stored at

the HLR. However, it is a temporary data that exists for only as long as the subscriber is "active" within the VLR coverage.

F. Authentication Center (AuC):

The AuC certifies any security information management (SIM) card attempting network connection when a phone has a live network signal, and it offers security to guarantee that third parties are unable to exploit network subscriber services.

G. International Mobile Station Equipment Identity (IMEI):

It is a kind of serial number that exclusively identifies a mobile station internationally. The IMEI is given by the equipment manufacturer and registered by the network operator, who stores it in the HLR/EIR.

H. International Mobile Subscriber Identity (IMSI):

Each registered user is exclusively recognized by its international mobile subscriber identity (IMSI). It is stored in the subscriber identity module (SIM). A mobile station can only be operated if a SIM with a valid IMSI is inserted into an equipment with a valid IMEI.

I. Temporary Mobile Subscriber Identity (TMSI):

Is the identity that is sent between the mobile and the network, and it is randomly assigned by the VLR to every mobile in the area, when it is switched on. The number is local to a specific area, and so it has to be updated each time the mobile moves to a new area, hence its name. The network can also change the TMSI of the mobile at any time in order to avoid the subscriber from being identified by third party attackers.

The following terms will be used in the proposed design:

K: the pre-shared key which is stored in both USIM and AuC by default.

ID_1: IMSI or TMSI depending on the current location of each user.

ID_2: The Sequence code (SQ) which is used in the scrambling process.

Q_1: The hashed value of ID_1

Q_2: The hashed value of ID_2

M: The IMEI identifier and we use it as the message to be signed.

SK: The session key.

Req: The authentication request.

XReq: The expected authentication request.

Res: The authentication response.

XRes: The expected authentication response.

The proposed scheme provide mutual authentication between the mobile station and the network operator with key agreement technique. The main description of this idea is to let the mobile station use the sequence code as a message and the subscriber's TMSI or use the specific IMSI, and SQ as identifiers; then hash them and use the hashed value for the modified short and efficient signature in the proposed scheme, and later for the session key. The AuC uses the same parameters for verification, and then sends another signature which we called RES to the MSC/USIM and computes the changeable session key depending on the current TMSI which is allocated in advance by MSC\VLR. It then sends it to a specific MS in the call setup process or in the paging process in case the MS is called from the network.

VI. Proposed CDMA-AKA components

The proposed scheme for both the MS/USIM and HLR/AuC requires a bilinear group and bilinear map to setup the scheme and compute the signature and the session key as follows [10, 11]:

* (G_1, G_2) multiplicative cyclic groups of prime order q
* g_1: generator of G_1 and g_2: generator of G_2
* $g_1=\Psi(g2)$: isomorphism from G_2 to G_1
* e: a bilinear map $e: G_1 \times G_2 \rightarrow G_T$ with the following properties:

1. Bilinear: $e(P + R, Q) = e(P, Q).\ e(R,Q)$
   For all $P, R \in G_1$,and $Q \in G_2$
2. Computable: There is an efficient algorithm to compute $e(P, Q)$ for any $P \in G_1$ and $Q \in G_2$
3. Non-degenerate: for all non-zero $P \in G_1$, there is a $Q \in G_2$, such that: $e(P,Q) \neq 1$
   There exists P and Q in G_1 such that $e(P,Q) \neq 1$

Let (G_1,G_2) be bilinear groups where $|G_1| = |G_2| = q$ for some prime q. and assume that the messages to be signed is $m \rightarrow$ IMEI $\in \{0, 1\}^*$, and by using a hash function

H: $\{0, 1\}^* \rightarrow Z^*q$. Then we can get all the hashed values as IMSI/TMSI, SQ in Z^*_q.

There are four algorithms achieved by the network operator (Setup, XReq, Res, and session key algorithms). On the mobile station side, there are also four algorithms achieved by the MS\SIM (Setup, Req, XRes, and session key). If the user receives a call (MTC) or wants to make a call (MOC), the first step is an authentication process to its own network operator. This is achieved by sending Req to the network using its own parameters depending on the IMSI\TMSI which is based on the current location. Later on, the user computes the session key for the encryption mode process. In the proposed design, firstly when an MS requests access to the network, the MSC/VLR will normally require the MS to authenticate it. The MSC will forward the IMSI to the HLR or check the specific TMSI in its database VLR. Then, when the HLR receives the IMSI and Req, it first checks its database to make sure the IMSI is valid and it is a part of the network. Once it has accomplished this, it will forward the IMSI and authentication request to the Authentication Center (AuC). The MSC\VLR can then only take a place in the encryption mode process after computing the session key. After that, the user will get Res which is generated by the network operator using the specific user's parameters TMSI\IMSI, MEI, and SQN. The MS runs the next algorithm's XRes key immediately to verify the network and generate the specific session's private key and stores it for a specific time period to encrypt/decrypt the message (M). The process (set session key) depends on the previous algorithms (Req, XReq, Res, and XRes).

The proposed scheme consists of six algorithms

distributed between the mobile station and the network operator as follows:

A. Setup algorithm in both MS/USIM and HLR/AuC:

The mobile station that needs to get access to the network resources (Voice, Data, Internet, SMS, MMS, etc.) starts computing the setup parameters in the synchronization process. The same algorithm will be computed by the network operator when getting the authentication request from the specific user. The setup algorithm is as follows:

Pick a random generator:

Set $g_1 = \Psi(g_2)$ and $g_2 \epsilon G_2$

Compute:

$Q_1 = H(ID_1)$ and $Q_2 = H(ID_2)$

The setup parameters: (g_1, g_2, Q_1, Q_2)

B. Req and XRes algorithms MS/USIM:

To get access to the network resources in the call setup process, the mobile station will start to compute the Req; to be able to compute this algorithm, the MS/USIM has to compute a secret value in advance as follows:

Given the setup parameters and the pre-shared key (K) which is from the basic CDMA-AKA protocol and it pre-shared and stored in both USIM and AuC in advance.

The MS/USIM sets secret value: $S = (g_2)^K$

Then computes the Req using the IMEI identifier as a message and the secret value:

$Req = g_1 \hat{} 1/(m+Q_1+Q_2.S)$

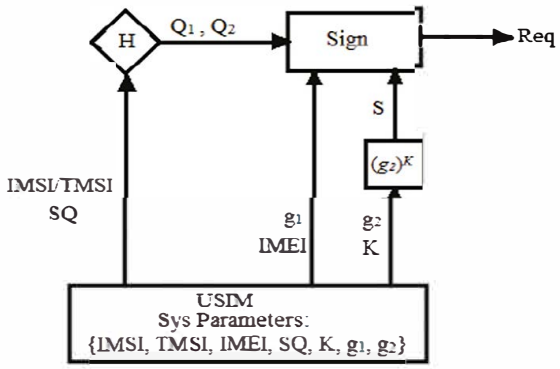

Figure 4. Req algorithm in MS/USIM

The MS/USIM sends Req to the HLR/AuC as authentication request [see figure 4].

Note that the term $1/(m+Q_1+Q_2.S)$ is computed using modulus p.

When the mobile station receives Res from the network operator, the MS/USIM computes XRes using the setup parameters as follows:

$$XRes = e(Q_1, Q_2)$$

if $Res = XRes$ holds then the result is valid, otherwise the result is invalid and the call setup process is aborted.

C. XReq and Res algorithms in HLR/AuC:

After the HLR/AuC receives the user's authentication request *Req*, it first checks Q_1 from its database, then it can compute the secret value, and use it to verify the request i.e. compute *XReq* using the setup parameters, message (IMEI), and Req.

Using the pre-shared key (K) compute the secret value:

$S = (g_2)^k$

Given $XReq = e(g_1, g_2)$

Compute:

$X = (g_2)^{Q1} \epsilon G_2$

$Y = (g_2)^{Q2} \epsilon G_2$

Then compute:

$Req^* = e(Req\ ,\ x.g_2^m.v^S)$

$XReq = e(g_1, g_2)$

Check if $Req^* = XReq$, if not output invalid and abort the authentication process, if yes then output:

$XReq = Req$ (valid).

After verifying the *XReq*, the HLR/AuC starts to compute the *Res* as follows:

Pick random $r \epsilon Z^*_q$

Let $U = r \cdot Q_1$

Compute:

$V = (1/H(m)+r)Q_2)$

Then compute:

$Res = e(H(m)\ Q_1 + U\ ,\ V)$

And send the *Res* to MS/USIM, which can be verified in the previous XRes algorithm. (figure 5)

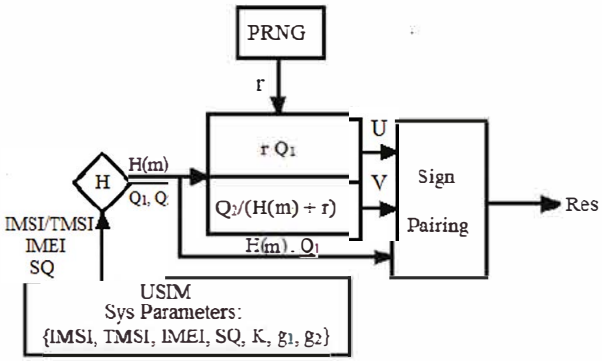

Figure 5. Res algorithm in HLR/AuC

D. SK algorithm in both MS/USIM and HLR/AuC:

The session key can be computed as follows:

First we define e: $G_1 \times G_1 \rightarrow G_2$

Set $U = (g_1)^{Q1} \epsilon G_1$

$V = (g_1)^{Q2} \epsilon G_1$

In the MS/USIM:

Pick random $a \epsilon Z^*_q$

Set: $A = a\ X$

Then compute:

$K_{MS/USIM} = e(U\ ,\ B + aV)^k$

In the HLR/AuC:

Pick random $b \epsilon Z^*_q$

Set: $B = b\,Y$
Then compute:
$K_{HLR/AuC} = e(V, A + bU)^k$
The shared session key:
$SK = e(U, V)^{k(a+b)}$

The session key will be used in the next step (encryption mode process), and it will be changed in the next session when the parameters are changed i.e. when the user moves to a new location area.

E. Req and XReq correctness:

When HLR/AuC receives the Req:
$Req = g_1 \wedge 1/(m + Q_1 + Q_2.S)$
it can compute the secret value:
$S = e(Q_1, Q_2)^k$
First it starts to compute:
$Req^* = e(Req, x.g_2^m.v^S)$
Where,
$X = (g_2)^{Q1}$ *and* $Y = (g_2)^{Q2}$
Then,
$Req^* = e(g_1 \wedge 1/(m+Q1+Q2.S), g_2^{Q1}.g_2^m.g_2^{Q2.S})$
$= e(g_1, g_2)^{(m+Q1+Q2.S)/(m+Q1+Q2.S)}$
$= e(g_1, g_2) = XReq$

F. Res and XRes correctness:

When the MS/USIM receives the $Res = e(H(m)Q_1 + U, V)$, it starts to compute:
$XRes = e(Q_1, Q_2)$
Where,
$U = r\,Q_1$
$V = Q_2/(H(m) + r)$
Then,
$Res = e(H(m)\,Q_1 + U, V)$
$= e((H(m) + r)\,Q_1, (H(m) + r)^{-1}\,Q_2)$
$= e(Q_1, Q_2)^{\wedge(H(m)+r).(H(m)+r)-1} = e(Q_1, Q_2) = XRes$

G. SK correctness:

$U = (g_1)^{Q1}$, $V = (g_1)^{Q2}$, $A = aX$, $B = bY$
For MS/USIM:
$K_{MS/USIM} = e(U, B + aV)^k$
$= e(U, b\,g_1^{Q2} + a\,g_1^{Q2})^k = e(U, (a+b)\,g_1^{Q2})^k$
$= e(U, g_1^{Q2})^{k(a+b)}$
So The shared session key:
$SK = e(U, V)^{k(a+b)}$
For HLR/AuC:
$K_{HLR/AuC} = e(V, A + bU)^k$
$= e(V, a\,g_1^{Q1} + b\,g_1^{Q1})^k = e(V, (a+b)\,g_1^{Q1})^k$
$= e(V, g_1^{Q1})^{k(a+b)}$
The shared session key:
$SK = e(U, V)^{k(a+b)}$

VII. Performance Evaluation and Security Analysis of Proposed Scheme

This performance is evaluated based on experimental outcomes [12, 13], for a variety of cryptographic operations using MIRACLE [14] in PIV 3 GHZ platform processor with Windows XP operating system and 512 MB memory. From [12, 13], the relative running time for the pairing operation is 20.04 (ms); for the pairing-based scalar multiplication is 6.38 (ms); for the one-way hash function is (3.04) ms; and for the other operations the time will not be presented. Here we define some terms for the running time calculation:
T_p= Pairing operation time complexity.
T_m= Pairing-based scalar multiplication time complexity.
T_h= Hash function time complexity.

For the proposed CDMA-AKA scheme we need three pairing operations and one exponential operation on the user side, and four pairing operations and one exponential operation on the network side. As shown in Table 1, the computational costs of the proposed scheme can be implemented in the CDMA cellular standard comparing with the basic standard for the synchronization and call setup process which it takes 2.4 sec approximately in the CDMA2000 cellular standard [2].

The following table illustrates the performance efficiency of the proposed scheme based on running time for each operation:

TABLE 1: THE PERFORMANCE EFFICIENCY TIME

Algorithms	Computational Cost	Running Time (ms)	Running Time MS/USIM	Running Time HLR/VLR
Setup	$2T_h$	6.08	6.08	6.08
Req	$2T_m$	12.76	12.76	0
XReq	$T_p + 1T_m$	45.56	0	45.56
Res	$T_p + T_m$	26.42	26.42	0
XRes	T_p	20.04	0	20.04
SK	$T_p + 2T_m$	32.8	32.8	32.8
		143.66	78.06	104.48

There are many weaknesses in the basic CDMA-AKA security system (CAVE, KASUMI algorithms). The existing CDMA-AKA is a challenge-response based mechanism that uses symmetric cryptography. The CDMA security system requires a lot of work to calibrate the communication parameters with high security schemes in order to prevent such vulnerability. Also, the users always want to be in secure hand and they don't trust the service providers. As such, by this proposed scheme we provide a mutual authentication with key agreement techniques. The proposed scheme can not be forged and this is confirmable factual under a chosen message attack without the random oracle model [9]. Hence, it makes the system more robust against numerous kinds of attacks such as false base station attack, core system attack, and Man-in-the-middle attack [15]. Therefore, there is no way the intruder puts itself in between the network components for eavesdropping. This is a very significant problem in the field of mobile communication

security i.e. in the CDMA authentication process, two related parameters, RAND and Req, and the corresponding Res are transmitted clearly on the air interface. Therefore, any introdure between MS and BTS or between BTS/BSC and MSC can execute a known plaintext attack on the challenge-response pair to eavesdrop and then to acquire the encryption key.

Using the parameters (IMSI/TMSI, IMEI, SQ) in the proposed scheme provides the system with more security and flexibility. The identifier IMSI/TMSI is used for making the session key changeable depending on the current subscriber's location. Then all the subscribers have a unique session key (SK) for a specific period of time. The identifier IMEI is used because it is internationally unique. Hence, if the authentication process fails, the network operator can know this is a non-functional equipment or the equipment is stolen. The sequence code SQ is used as an identifier ID_2 which can be simply generated by a shift register with feedback. The PN sequences decide the user capacity (limited by the number of different codes), and give a good synchronization for the CDMA system. Thus, it is more secure if we can synchronize our scheme. Also, with the spreading and modulation processes, if the SQ code is invalid (Low capacity or Unsynchronized device), the scheme aborts the authentication process. The proposed approach is more efficient than other competing topologies. In comparison to other schemes, such as KASUMI algorithm in a basic CDMA system, the proposed scheme is a flexible and secure cryptosystem. The only practical problem might be a relatively higher computational cost than the existing schemes, but it will be improved as new mathematical propositions are implemented.

VIII. Conclusion and Future Scope

In this paper, the essential security features of CDMA systems and the limitations of the existing CDMA-AKA protocols were presented and extensively discussed. Moreover, a technique to provide authentication and key agreement for the CDMA system with handshaking procedures was proposed and comprehensively analyzed. As CDMA system is recently being used as a basis for the GSM systems, the proposed scheme can be the most suitable one for CDMA cellular standard owing to its lightweight infrastructure and high security outcomes. The proposed scheme is a promising solution for improving several weaknesses of the basic CDMA-AKA. In the future work the USIM card is a most important component for the security in the whole mobile communication security system, beside the authentication center in the core system, so improvement for the USIM and AuC database is required i.e. that gives the system a good security e.g. using a new techniques of Integrated Circuits (IC) and Smart Cards technologies to be compatible with the public key cryptography. There is also a suggestion to make separation for the security architecture and the CDMA architecture, i.e. make a full design of PKI in the standalone equipment, and let the authentication center be standalone center and then make a interfaces between them, that gives the system a high reliability for the security issues, possibility of development in the future.

REFERENCES

[1]. A. K. Parthasarathy, "Improved Content Based Watermarking for Images," M. S. Thesis, Louisiana State University and Agricultural and Mechanical College, Kanchipuram, India, August 2006.

[2]. 3GPP TS 21.133 (4.1.0), "3G Security; Security threats and requirements," *Release 4*, December, 2001.

[3]. 3GPP TS 33.102 (5.2.0), "3G Security; Security Architecture," Release 5, June, 2003.

[4]. 3GPP TR 33.900 (1.2.0), "A Guide to 3G Security" January, 2000.

[5]. ISO, SD 6, SC 27 N1954: Glossary of IT security terminology, March 1998, "Review of third generation mobile security architecture,"

[6]. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.

[7]. K. Shim, and Y. R Lee, "Security flaws in authentication and key establishment protocols for mobile communications," Applied mathematics and computation, vol. 169(1), 2005, pp. 62-74. Toorani, Mohsen, and A. Beheshti. "Solutions to the GSM security weaknesses." Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on. IEEE, 2008.

[8]. Document reference AC336/VOD/WP12/DS/P/11-1/1D11 – USECA Final technical report Part 1: Technical Rsults.

[9]. T. S. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Singapore: Pearson Education, Inc., 2002.

[10]. D. Boneh and X. Boyen, "Short Signatures Without Random Oracles," in Advances in Cryptology—EUROCRYPT 2004, LNCS, vol. 3027, pp. 56–73, 2004) appears in Eurocrypt 2004.

[11]. Fangguo Zhang, Reihaneh Safavi-Naini and Willy Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," PKC 2004, Singapore. LNCS 2947, pp.277-290, Springer-Verlag, 2004.

[12]. Debiao, J. Chen and R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," Comput. Electr. Eng. 37, 4, pp. 444-450, July 2011.

[13]. Debiao and C. Jianhua, "An effcient certificate-less designated verifier signature scheme," Int. Arab J. Inf. Technol. 10 no. 4, pp.389-396, 2013.

[14]. MIRACLE, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/ Mscott.

[15]. Whitehouse, Ollie, and Graham Murphy, "Attacks and counter measures in 2.5 G and 3G cellular IP networks," Atstake Inc. (March 2004).