On the Security of Wireless Network Access with Enhancements

Lein Harn and Wen-Jung Hsin

Computer Networking
School of Interdisciplinary Computing & Engineering
University of Missouri–Kansas City
Kansas City, MO 64110, USA
Phone: (816)235-2358
Email: {HarnL,HsinW}@umkc.edu

Abstract

The security of the current 3G wireless protocols addresses the problems faced by the 2G systems, in addition to fulfilling the higher 3G security requirements mandated from operating in IP networks as well as voice networks. However, the approach adopted by the two most popular 3G mobile system forerunners, UMTS and cdma2000, leaves many areas for improvement. In this paper, we improve the security of the 3G protocols in network access by providing a stronger periodically mutual authentication and a non-repudiation service in an elegant way. The simplicity of our enhancements is achieved by using hash chaining and keyed-Hash Message Authentication Code in the directions both to and from a mobile handset, thereby making re-synchronization a trivial task. Furthermore, by utilizing the recently proposed $O(log(n))$ storage and time hash chaining technique, our enhancement is very desired for mobile environment where mobile handsets have limited storage.

Index Terms

3G Mobile Network Security and Authentication

I. Acronyms

2G,3G,4G	The Second, Third, Fourth Generation
3GPP	3G Partnership Project
3GPP2	3G Partnership Project 2
A3	An authentication algorithm used in GSM
A5	An encryption algorithm used in GSM
A8	a key generation algorithm used in GSM
AES	Advanced Encryption System
AK	Anonymity Key
AKA	Authentication and Key Agreement
AV	Authentication Vector
CK	Cipher Key
CDMA	Code Division Multiple Access
cdmaOne	IS-95 based CDMA
cdma2000	IS-2000 based CDMA
COUNT	Call History Counter used in cdma2000
CS	Circuit Switching
ESA	Enhanced Subscriber Authentication
ESP	Enhanced Subscriber Privacy
FIPS	Federal Information Processing Standards
GSM	Global System for Mobile communications
HLR	Home Location Register
HMAC	keyed-Hash Message Authentication Code
IC	Integrated Circuit

IK	Integrity Key
IMT-2000	International Mobile Telecommunications 2000
Key K	A common secret key between MS and HLR
MS	Mobile Station
NIST	National Institute of Standards and Technology
PS	Packet Switching
RAND	A random number
SAKA	Subscriber Authentication and Key Agreement
SEQ	Sequence Number used in UMTS AKA
SIM	Subscriber Identity Module
SSD	Shared Secret Data
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register

II. Introduction

In recent years, due to technology advances, we have seen a phenomenal increase in the number of cellular users. As the demand increases, so does the importance of security in the cellular systems. This can be seen from many highly publicized incidents, e.g., the plain text communication among allied pilots during Kosovo war as reported by Washington Post, and the interception of House Speaker Newt Gingrich's cellular conference conversation. To provide protection, many different security areas are addressed, e.g., network access security provides users with secure access to the mobile services, network domain security provides secure exchanges of signaling data in the core network, application domain security provides users and providers with secure exchanges of application data, etc. [6]. Our emphasis in this paper is in the area of network access security.

For network access security, 2G mobile systems such as GSM and cdmaOne were designed to protect against external attacks. However, these designs have led to numerous interception attacks [5], [14], [23], [26], [32], [33], [34]. Mouly [24] stated that the design of GSM security was not aimed to be any higher than that of a fixed trunk network. Thus, it is not surprising that there have been many GSM security problems reported over the years. The 3G wireless protocols must not only address the problems faced by the 2G systems but also provide strong security functionality to fulfill the 3G cellular requirements as defined in IMT-2000 [7], especially the required support over IP networks. Unfortunately, the proposed security protocols for network access provided by the two most popular 3G cellular system forerunners, UMTS and cdma2000 (the descendants of GSM and cdmaOne, respectively), still leave many areas for improvement. In this paper, we address some of these areas and provide protocol enhancements on top of these two systems.

For clarity, here we specify the security standards to which we will be referring in this paper. The security architecture standard for UMTS is defined in [6]. For cdma2000, the latest published documentation on network access security can be found in [8], [9], [10].

One of the areas for improvement is the way in which a subscriber authenticates a network. 3G systems provide mutual authentication between a subscriber and a network, whereas 2G provides only subscriber authentication. To allow network authentication, UMTS uses a sequence number approach with which a subscriber can verify the freshness of an authentication request and thus prevent an attacker's replay. However, the generation, verification, and management of sequence numbers are complicated especially with regard to frequently occurred situations such as re-synchronization failure recovery, simultaneous registration in circuit-switching (CS) and packet-switching (PS) domains, and authentication record transfer between VLRs. Recently, cdma2000 has also been approved to adopt the UMTS authentication approach. Instead of sequence numbers, we propose to use Lamport's one-time password/hash chaining technique [21] to establish periodically mutual authentication. Hash chaining provides strong periodical authentication and is used in many applications [3], [17], [18], [19], [22]. The management and record keeping of hash chaining is also much simpler as compared to the sequence number approach, especially in regard to the common situations mentioned above. Thus, by using this technique, our enhancement is both efficient and elegant, and our authentication is stronger than that in UMTS and cdma2000.

An extra benefit resulting from using hash chaining is its ability to solve a billing dispute problem. Neither UMTS nor cdma2000 address the issue of billing disputes, and thus there is no recourse to settle disputes when they arise. This issue is implicitly dealt with by trusted assumptions. Specifically, the UMTS Security Architecture standard [6]

assumes that a mobile station (MS) trusts its home register location (HLR). This is most evident by the fact that an MS and its HLR share a common secret key K. The standard further assumes that the MS's HLR trusts a visitor register location (VLR) to securely handle the authentication information. UMTS does not have an explicitly trusted assumption about the relationship between an MS and a VLR. However, this relationship can be inferred from the condition that a transitive rule applies. That is, if an MS trusts an HLR, and an HLR trusts a VLR in handling authentication information, then an MS trusts the VLR for authentication matters. Our enhancement removes this implicit assumption, and thus if there is a billing dispute between an MS and a VLR, both sides can prove their claims. Specifically, we use keyed-Hash Message Authentication Code (HMAC) recently drafted by FIPS [15] on top of hash chaining to provide a non-repudiation service to explicitly address the billing issue without complicating the existing protocols.

Aside from the benefits mentioned above, we provide an authentication style that offers both security and convenience. Currently, there are two basic authentication styles differing in the way as to which entity gets the control. In UMTS, it is the HLR that gets the control whereas in cdma2000 the VLR does. Specifically, in UMTS, an HLR prepares and sends a list of challenge and response vectors to a VLR so that the VLR can authenticate an MS, whereas in cdma2000, from a common secret key K established between an MS and its HLR, a shared secret data (SSD) is derived and can be shared with a VLR so that the VLR itself can authenticate the MS locally. (Note that although cdma2000 is recently approved to use UMTS AKA, the latest published security documents [8], [9], [10] do not describe how cdma2000 will simultaneously adopt the UMTS authentication style and maintain its backward compatibility with cdmaOne.) The HLR control method is more secure than the VLR control method in that the HLR is the one that an MS trusts. However, the VLR control method is more convenient for a VLR to authenticate an MS locally. Here, our authentication enhancement gives a VLR local control yet an HLR still has the total control, therefore it is both secure and convenient, allowing the best features of both styles.

Previous work in this area includes a comparative study between UMTS and cdma2000 for the entire systems, but with little emphasis in the area of security [2], [13]. Rose [30] offered a high level general overview of wireless security between UMTS and cdma2000. Our detailed comparative study here emphasizes the subscriber authentication and key agreement procedures, as this becomes the basis for building our protocol enhancements. Al-Muhtadi et al. [1] proposed a lightweight component in mobile devices and a security server for authentication and call setup for 3G/4G systems. Their work can benefit from our enhanced protocol mentioned here to provide stronger authentication and simplify the implementation.

The remainder of this paper is organized as follows. Section III provides an overview of network access security from 2G to 3G. Sections IV and V describe detailed AKA procedure in UMTS and cdma2000, respectively. Section VI describes our enhancements, and hash chaining and HMAC techniques that we adopt to achieve the improvements. Finally, section VII provides conclusion and summary.

III. Overview of Network Access Security from 2G to 3G

Network access security provides legitimate users access to wireless network services securely and protects them against attacks on the access link [6]. The primary mechanisms for achieving network access security are entity authentication and data confidentiality. The subscriber authentication and key agreement protocol in the cellular network is used to facilitate these mechanisms. Specifically, in order for a subscriber to access the network, the network must confirm the identity of the legitimate user. This is called *subscriber authentication*. In 2G and 3G systems, the subscriber authentication is based on a common secret key K shared between the subscriber and subscriber's HLR. Using GSM as an example, the steps for achieving subscriber authentication and data confidentiality are

1) An MS requests services at a visiting network.
2) The corresponding VLR requests and obtains a list of <challenge, response, session key> triplets from the MS' HLR, where challenge is a 128-bit long random number $RAND$.
3) The VLR challenges the MS with $RAND$ from a selected triplet.
4) The MS generates a response by using algorithm A3 with inputs $RAND$ and key K, and sends the response to the VLR.
5) The VLR verifies that the MS' response matches the response in the selected triplet. If so, the MS is authenticated.

6) After the MS is authenticated, the MS generates a session key by using algorithm $A8$ with $RAND$ and key K. Note, VLR's session key is in the selected triplet that is used to authenticate MS.
7) The MS and the VLR can now encrypt user and signaling data using algorithm $A5$ with the shared session key to obtain data confidentiality.

Note that the security standards [6], [8], [9], [10] that we are referring to in this paper assume the communication links between a VLR and an HLR are adequately secure. Furthermore, these standards do not address the authentication issues between a VLR and an HLR. In this paper, we also maintain the same assumption and do not address these issues between a VLR and an HLR.

As can be seen from the above steps, an HLR in GSM has the control in terms of generating authentication triplets, and a VLR merely uses the authentication triplets prepared by an HLR to authenticate an MS and encrypt data. This is quite different from cdmaOne where a VLR local control mechanism is adopted. Since the security mechanism in cdma2000 described in the current standards [8] and [9] still shows the same procedures as in cdmaOne, we will discuss these procedures for cdmaOne in details in section V where cdma2000 is introduced.

In an effort to provide stronger network access security than the 2G counterparts, both UMTS and cdma2000 provide enhanced subscriber authentication (ESA) and enhanced subscriber privacy (ESP). In particular, in UMTS, an additional authentication is provided so that subscribers can authenticate the network, and an additional integrity key is used to protect the integrity of signaling messages after the subscriber and the network are mutually authenticated. AKA is the name given by 3GPP to refer to the subscriber authentication and key agreement protocol in UMTS, where 3GPP is a collaboration agreement by telecommunication standards bodies for developing a global UMTS standard. As for cdma2000, the standard effort for AKA by 3GPP2, the sister project of 3GPP placed in charge of developing the global cdma2000 standard, is on-going and has not yet been finalized. In the next two sections, we will describe UMTS AKA procedure in detail and the on-going progress in cdma2000.

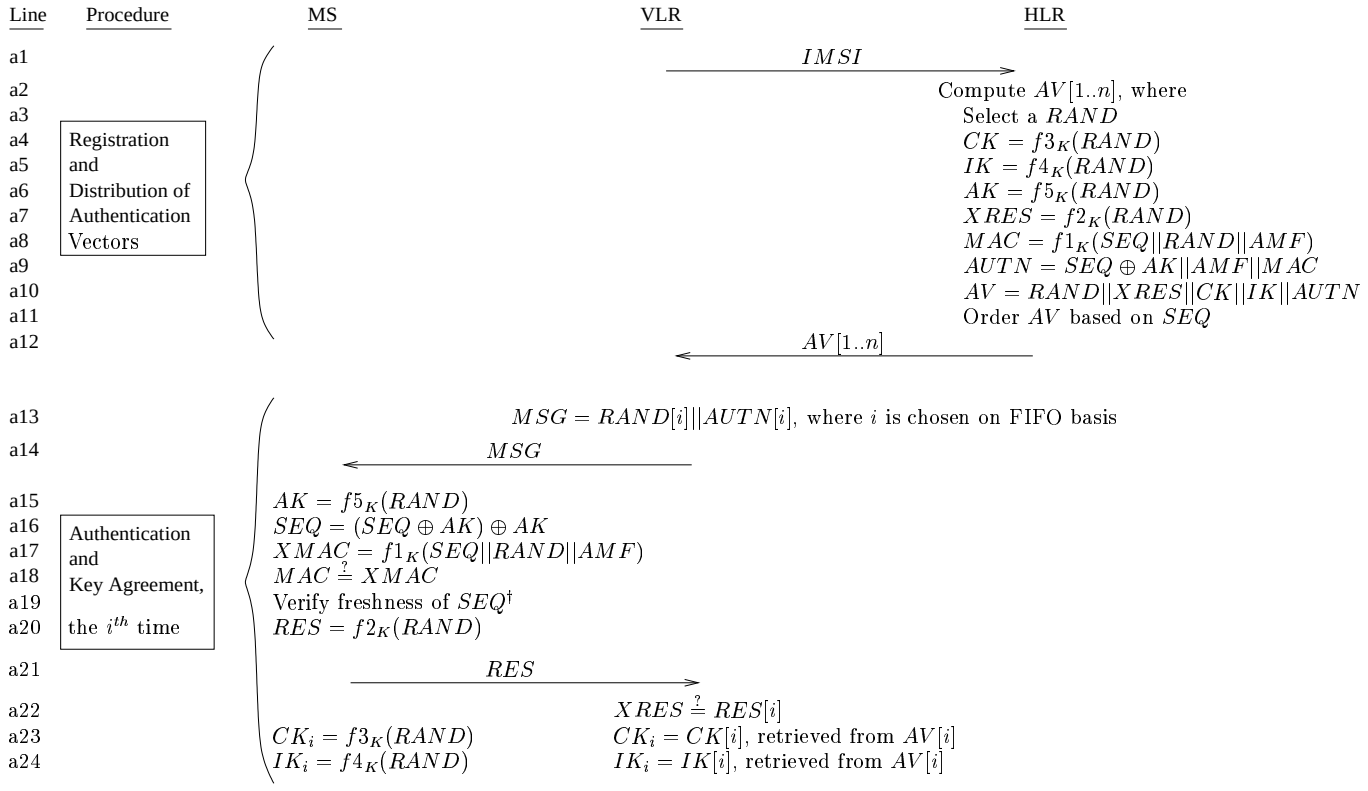
IV. UMTS Authentication and Key Agreement

This section describes the registration and AKA procedures in UMTS [6], shown in Figure 1. For ease of reference, each line in the figure is provided with a line identification number. UMTS maintains the same challenge and response method as its 2G predecessor, GSM, to facilitate generation migration. In particular, during registration, an HLR prepares and sends a list of authentication vectors (AV) to a VLR (see lines $a2$ to $a12$ in Figure 1.) During AKA, a VLR uses an AV (lines $a13$ and $a14$) to authenticate an MS. Each AV is used once for each AKA invocation. If a VLR runs out of AVs, it can request more from the HLR. When an MS roams out of a VLR, the old VLR should transfer the leftover AVs to the new VLR. The standard [6] assumes that the communication links between VLRs are adequately secure.

The major differences in registration and AKA procedures between UMTS and GSM are (1) GSM allows only subscriber authentication, while UMTS provides both subscriber (line $a22$) and network (line $a19$) mutual authentications, and (2) UMTS can protect the integrity of signaling data (via IK_i in line $a24$), while GSM can not. For the network authentication, UMTS employs a complicated sequence number (SEQ) technique. With the considerations of simultaneous registration in CS and PS domains, re-synchronization failure recovery, and leftover authentication vector transferring between VLRs, SEQ complicates both protocol and implementation tremendously. In fact, in the UMTS Security Architecture [6], a 6-page appendix is necessary to describe the generation, allocation, verification, and management of SEQ.

More specifically, UMTS achieves these two extra functionalities by adding two extra fields in the AV, namely an authentication token (line $a9$) and an integrity key (IK) (line $a5$) on top of the triplet provided in GSM. The authentication token allows an MS to authenticate a VLR. The fields within the token include SEQ, anonymity key (AK), authentication management field (AMF), and message authentication code (MAC). Each authentication token is assigned a unique SEQ. When an MS receives an authentication token, it verifies that the corresponding SEQ has not been accepted before (line $a19$), thereby precluding replay by an attacker. To allow for out-of-order SEQs due to simultaneous registration in both CS and PS domains, MS maintains a list of SEQs that it has accepted. To prevent exposition of MS's identity and location, key AK can be used to conceal the SEQ. AMF is an authentication management field which can be used for purposes such as specifying a particular authentication algorithm used, etc. MAC is used to ensure the authenticity and integrity of the authentication token and the random challenge. The IK

is used to protect the integrity of the control data. Readers are referred to the UMTS Security Architecture [6] for a detailed description of the AKA procedure.



† : The generation, allocation, verification, and management of SEQ (sequence number) are described in a 6-page appendix in UMTS security architecture standard [6].

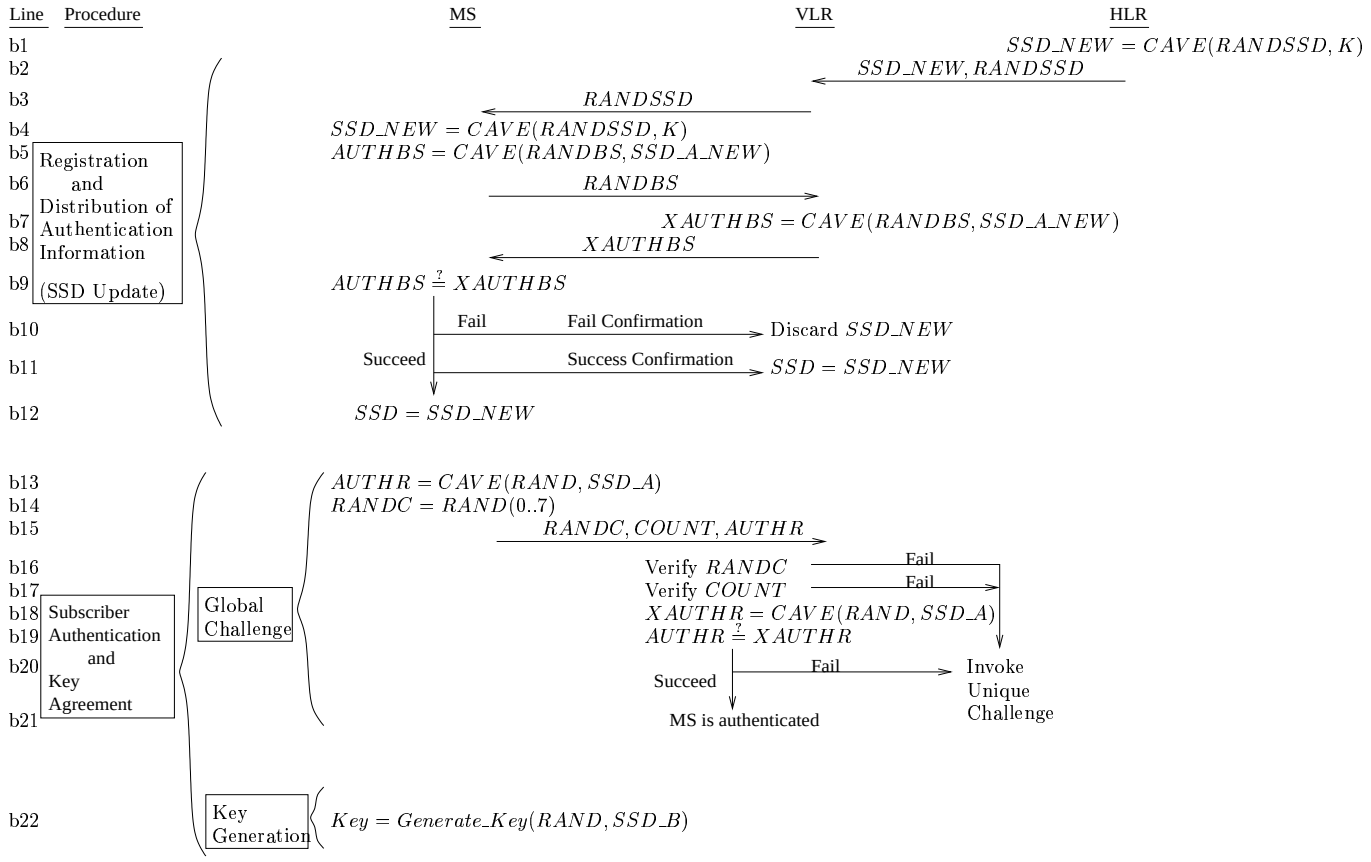
Fig. 1. Authentication and Key Agreement in UMTS

V. CDMA2000 Subscriber Authentication and Key Agreement

Cdma2000 is designed to be backward compatible with its predecessor cdmOne, therefore it inherits most of the cdmaOne security features. Specifically, for cdma2000, Figure 2 depicts the general registration and the subscriber authentication and key agreement procedures in the latest published documents on security [8], [9]. These standards show the same procedures as in cdmaOne.

In particular, during registration (invoked by the SSD update procedure, lines $b1$ to $b12$), the HLR selects a $RANDSSD$ and calculates a new SSD which can be shared with a VLR (lines $b1$ and $b2$.) The VLR then sends the $RANDSSD$ to an MS for it to derive the new SSD (lines $b3$ and $b4$.) To authenticate the VLR, an MS sends a base station challenge order (line $b6$) to the VLR. It is only when the VLR passes the challenge does the MS update to the new SSD (line $b12$).

During the subscriber authentication phase (lines $b13$ to $b21$), the MS invokes the global challenge procedure by first calculating a response $AUTHR$ using a globally broadcast challenge $RAND$ and SSD_A, the first portion of SSD. In line $b15$, the MS sends $RANDC$ (the first 8 bits of $RAND$), $COUNT$ (Call History counter used for clone prevention by keeping track the number of calls made by the MS), and $AUTHR$ to the VLR who will then verify the received values to authenticate the MS, (in lines $b16$ to $b21$). In case that the MS fails the global challenge, the VLR will invoke a unique challenge procedure with a unique random number specifically generated to challenge the MS (readers are referred to [8] for the details of the unique challenge procedure). Note that the subscriber authentication here is only one-way (i.e., the VLR authenticates the MS, but not vice versa). Only when the MS is successfully authenticated can the encryption key be generated. In line $b22$, the encryption key is calculated based on the $RAND$ and SSD_B, the second portion of SSD.



Note: In this figure, we only show the essential inputs to the CAVE algorithm. The detailed inputs can be found in [8] and [9].

Fig. 2. Cdma2000 Subscriber Authentication and Key Agreement in documents C.S0004-A_v6.0 [8] and C.S0005-A_v6.0 [9]

The predominant difference in the network access security between GSM and cdmaOne, and thus their descendants UMTS and cdma2000, is how the authentication data is prepared. In UMTS, an HLR prepares and sends a list of challenge and response vectors to the VLR to authenticate an MS; while in cdma2000, a derived shared secret data (SSD) from a common secret key K can be shared with a VLR so that the VLR itself can authenticate an MS locally. The HLR total control method adopted by UMTS is secure in that the HLR is the one that an MS trusts, however it is not convenient for a VLR as the VLR has to rely on the HLR to generate challenges and responses. On the other hand, cdma2000's VLR local method is convenient for a VLR but not as secure as UMTS, since an HLR does not have the total control in the communication between a VLR and an MS. This is most evident when there is a dispute between an MS and a VLR; an HLR has no easy way to settle the dispute as it has given the VLR the control. To lesson the degree of the problem, in cdma2000, an HLR can periodically change the value of the SSD (using the SSD Update procedure) to make the sharing with a VLR less problematic.

To meet the 3G security challenges, cdma2000 will provide ESA and ESP enhancements [11]. However, the detailed steps in achieving these enhancements are still being worked out, although 3GPP2 has approved the following: (1) the adoption of openly reviewed algorithms such as Rijndael Encryption algorithm [9], the AES chosen by NIST, and (2) the adoption of 3GPP AKA with SHA-1 and Message Authentication Code as the hash and integrity functions for AKA operations [10]. SHA-1 is a hash function defined in FIPS "Secured Hash Standard" [16]. A message authentication code is generated by means of a hash function to ensure the authenticity and integrity of the transmitted messages. With the adoption of 3GPP AKA, it remains to be seen as to how cdma2000 handles both authentication styles (i.e., UMTS' HLR total control and cdma2000's VLR local control) smoothly. As of the writing of this paper, 3GPP2 has not published the details of this transaction.

VI. ENHANCEMENTS

As can be seen from section IV, the approach adopted by UMTS to provide strong 3G AKA complicates the already complex wireless protocol. Here, we provide an elegant approach to achieve stronger AKA on top of UMTS as well as cdma2000.

In the following, section VI-A introduces a list of notations that we use in our enhanced protocol. Section VI-B describes HMAC and hash chaining techniques. Section VI-C describes our enhanced protocol, the advantages, and the time and space analysis.

A. Notation

- $t(x, y)$: HMAC with key x, and message y
- $p(x, y)$: Cipher key generation function with key x, and random data y
- $q(x, y)$: Integrity key generation function with key x, and random data y
- $r(x, y)$: Anonymity key generation function with key x, and random data y
- AK: Anonymity Key
- $RAND_H$: A random number selected by an HLR
- CK_H: The Cipher Key generated by an HLR, using HLR-selected $RAND_H$. An MS can also generate this when given a $RAND_H$.
- IK_H: The Integrity Key generated by an HLR, using HLR-selected $RAND_H$. An MS can also generate this when given a $RAND_H$.
- $CK_{i,m}$: The Cipher Key with id (i, m) generated by an MS and a VLR and for use between the MS and the VLR
- $IK_{i,m}$: The Integrity Key with id (i, m) generated by an MS and a VLR and for use between the MS and the VLR
- $f^m(b_i)$: One-way hash function with i^{th} random seed b_i and m^{th} composition, where $i \leq I$ and $m \leq M$, for use in authenticating an MS
- M: The maximum number of f hash chaining composition
- I: The maximum number of random seeds for f hash chaining
- $g^n(a_j)$: One-way hash function with j^{th} random seed a_j and n^{th} composition, where $j \leq J$ and $n \leq N$, for use in authenticating a VLR.
- N: The maximum number of g hash chaining composition
- J: The maximum number of random seeds for g hash chaining
- $\stackrel{?}{=}$: An equality comparison operator

B. Techniques

To enhance the 3G AKA protocol, we adopt two major techniques: keyed-Hash Message Authentication Code (HMAC) and hash chaining.

HMAC is very popular in the Internet community [27], and has been recently drafted by FIPS [15]. It is used for message authentication by means of a cryptographic hash function and a shared secret key. In a public-key system, a digital signature can be used to replace HMAC. The main components in HMAC are a hash algorithm and a key, and the most common form of HMAC is $hash(key, hash(key, message))$. Two of the most popular HMAC's are HMAC-MD5 [28] and HMAC-SHA [29].

Lamport's one-time password/hash-chaining was proposed in 1981, and has been used in many applications [3], [17], [18], [19], [22]. Let $f(x)$ be a one-way function and $f^M(x) = f(f(\cdots(f(x)\cdots)))$ be the composition of M fs. During registration, the claimant (i.e., the one wishes to be authenticated) randomly selects an integer b, computes $f^M(b)$ and $HMAC$ of $f^M(b)$, and sends $f^M(b)$ and the $HMAC$ of $f^M(b)$ to the verifier (i.e., the one decides whether the claimant is who it is). Once registered, each hash chain can be used by the claimant to prove itself to the verifier M times. In the first visit, the claimant submits $f^{M-1}(b)$ to prove itself. The verifier checks the equality $f(f^{M-1}(b)) \stackrel{?}{=} f^M(b)$. If passed, the verifier updates $f^M(b)$ and stores $f^{M-1}(b)$ for the next visit; otherwise, the claimant is not authenticated. The claimant reveals $f^{M-1}(b), f^{M-2}(b), \cdots, f(b)$, and $b = f^0(b)$ in sequence to prove itself M times. The one-way hash chaining algorithm prevents all users, except the legitimate one, from computing backward values using the published one-way value.

Straight forward implementations of a hash chain such as storing all chain elements or iteratively hashing from a seed have $O(M)$ of combined memory and computational complexity for an M element chain. Recently, Jakobsson [20], and Coppersmith and Jakobsson [12] proposed a $log_2(M)$ space and access time mechanism, especially desired for low-cost applications such as mobile handsets, micro-payments, smart dust, authentications, and signatures (see [20], [12] for references therein.)

For the purpose of non-repudiation, the combination of $f^{M-m}(b)$ and the $HMAC$ of $f^M(b)$ (that is provided by the claimant during registration) can be used as a non-repudiation proof by the verifier as an evidence for all m visits made by the claimant. Specifically, for all m visits, the verifier only needs to store the most recently released f value (i.e., $f^{M-m}(b)$), and does not need to keep all other values that it has received (i.e., $f^M(b)$, $f^{M-1}(b)$, $\cdots$, $f^{M-m+1}(b)$) before the m^{th} visit. The verifier can produce a proof of the claimant's j^{th} visit, where $1 \leq j \leq m-1$, by simply computing $f^{m-j}(f^{M-m}(b))$. This desired feature is especially good for the applications (such as mobile handsets) with limited storage space.

To prolong the life time of a hash chain, an additional dimension can be added to the above scheme as follows. The claimant (1) randomly selects I seeds, $b_1, b_2, \cdots$, and b_I, (2) computes $f^M(b_1), f^M(b_2), \cdots$, and $f^M(b_I)$, and an HMAC on the concatenated message $f^M(b_1)||f^M(b_2)||\cdots||f^M(b_I)$, (3) sends the computed values in (2) to the verifier. Note that by using the concatenation of I hash chaining values as one single message, one message authentication code between an MS and an HLR is all that is needed for establishing the initial registration (see lines $c1$ and $c2$ in Figure 3).

A general discussion on one-way functions and one-way hash functions can be found in [31] and the implementation of these functions can be found in [4].

C. Protocol Enhancement

Figure 3 provides our registration and AKA enhancements on top of the two 3G forerunners, UMTS and cdma2000. For clarity, a set of protocol steps composed to achieve a unique functionality are grouped into a procedure. These procedures mirror those in Figures 1 and 2. The significance of this grouping indicates that our procedures can be used to replace with ease the corresponding UMTS and cdma2000 procedures.

1) Enhancement Details: In the following, we explain each procedure and the corresponding steps in detail.

- Procedure: Registration and Distribution of Authentication Information

  This procedure is used when an MS first roams into a new visitor domain. The MS must send its HLR a set of data which is subsequently used by the VLR.

  – Lines $c1$ to $c3$: Both MSG_1 and $HMAC_1$ are sent from the MS via the VLR to the HLR. These messages serve as a legal evidence of the MS' intention to use the service within the VLR's domain. The I hash chains fs, each with different seed b_i where $i \leq I$, will be used by the VLR to authenticate the MS at most $I \times M$ AKA invocations. The use of a timestamp guarantees the freshness of the message. $HMAC_1$ is used by the HLR to authenticate MSG_1 sent from the MS. One stronger form of authentication by means of a public-key system with a signature on MSG_1 such as $Sign(MS_{private\_key}, h(MSG_1))$ where $h(x)$ is a one-way hash function, can be used. Note that a common secret key K has already been established and shared between the MS and the HLR when the MS first signs up with the HLR.

  – Lines $c4$ to $c12$: After verifying the authenticity of MSG_1 sent from the MS, the HLR selects a random number $RAND_H$. The HLR then generates a set of master keys, i.e., CK_H, IK_H, and AK, based on the chosen random number, $RAND_H$. This set of master keys and the selected random number along with MS' hash chains are then sent to the VLR. Note that just like in UMTS Security Architecture [6], we also assume that the communication link between the HLR and the VLR is adequately secure.

  – Lines $c13$ to $c15$: In order for the MS to verify the authenticity of the VLR later on in the AKA phase, a set of hash chains $g^N(a_j)$, where $j \leq J$, and an $HMAC$ are composed and sent to the MS along with the random number selected by the HLR.

  – Lines $c16$ to $c18$: These lines are used by the MS to authenticate MSG_3 sent from the VLR. This is obtained via the key AK that is shared among MS, VLR, and HLR.

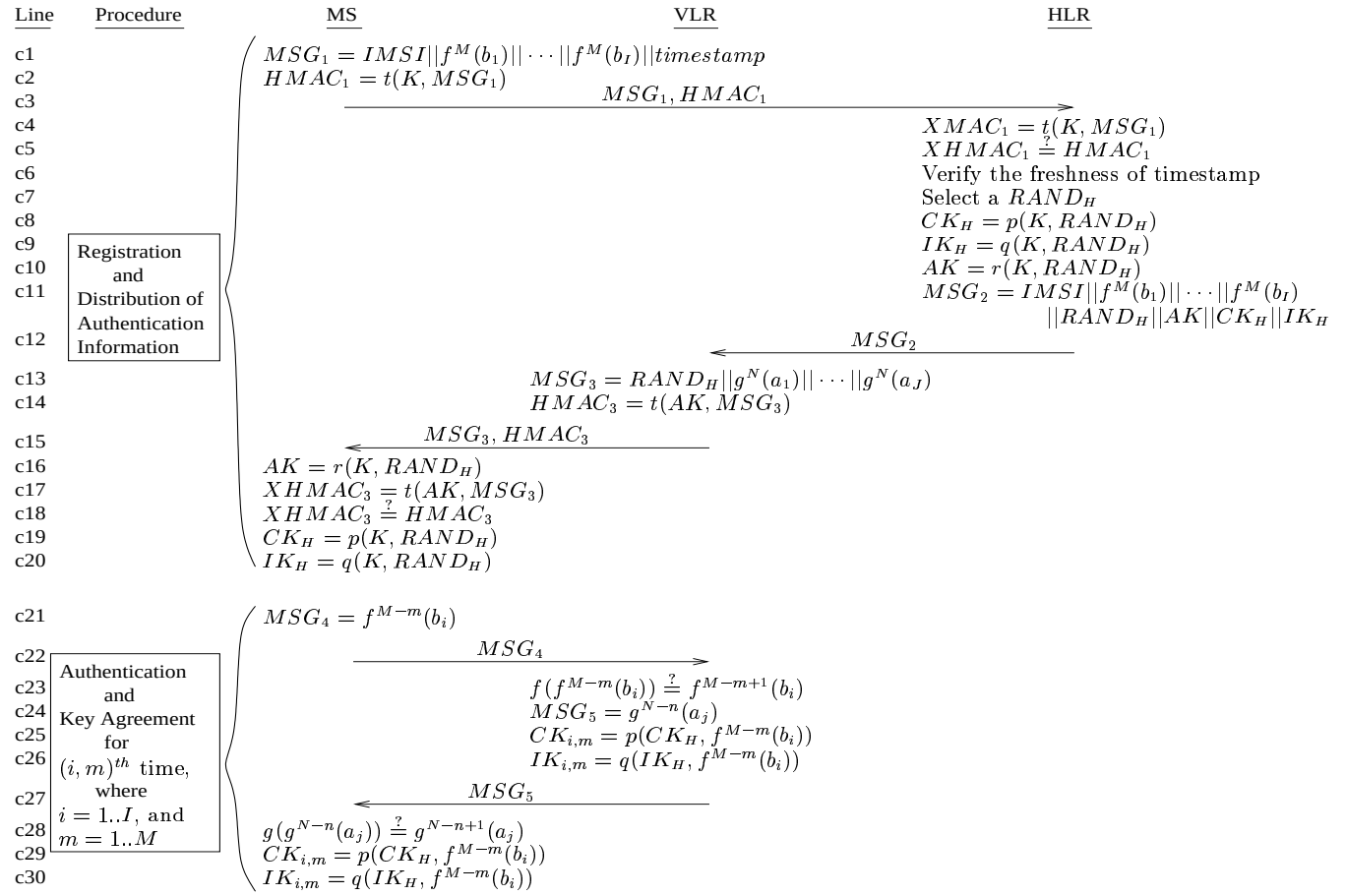


Fig. 3. Enhanced Registration and AKA procedures

– Lines $c19$ and $c20$: After the MS is sure of the authenticity of MSG_3 in lines $c16$ to $c18$, the MS computes master keys CK_H and IK_H based on the master random number $RAND_H$. These master keys are to be used for up to $min(I \times M, J \times N)$ times of AKA invocations subsequently. When either MS or VLR runs out of its set of hash chains, this registration procedure will be invoked again to establish new sets of hash chains. Thus, to minimize the number of registration invocations, these parameters I, M, J, and N should be chosen properly by considering the tradeoff between the storage space and time efficiency.

- Procedure: Authentication and Key Agreement

  In this procedure, since each authentication uses one chain position, the MS can prove its identity to the VLR at most $I \times M$ times, whereas the VLR to the MS $J \times N$ times. The indices (i, m) and (j, n), where $i \leq I$, $m \leq M$, $j \leq J$, and $n \leq N$, are independent of each other as each side steps through its own hash chains at its own pace. Thus, there is no need to synchronize between these two sets of chains. Within each set of hash chains, it can be agreed that the chain with lower id (i.e., i and j) is used. If one side encounters problems in authenticating the other side, the verifier should send an error message with the problematic chain id to the claimant. The claimant then tries to authenticate itself to the verifier starting from the next fresh chain. For example, if the problematic chain id in f series is 8, then the MS should reveal $f^{M-1}(b_9)$ to the VLR to try to correct the authentication problem.

  – Lines $c21$ to $c23$ are used by the VLR to authenticate $MSG4$ sent from the MS.
  – Lines $c27$ to $c28$ are used by the MS to authenticate $MSG5$ sent from a legitimate VLR.
  – Lines $c29$ to $c30$: After both sides are mutually authenticated, the MS computes the session keys $CK_{i,m}$ and $IK_{i,m}$, and then use them for data confidentiality and integrity in the $(i, m)^{th}$ communication session.

2) Advantages: The following list summarizes the advantages of our security enhancements.

- Non-repudiation: For cases such as billing and dispute resolution, the combination of $HMAC_1$ in line $c2$ and $f^{M-m}(b_i)$ can serve as a non-repudiation proof by a VLR as an evidence of m visits in the i^{th} chain made by an MS, and the combination of $HMAC_3$ in line $c14$ and $g^{N-n}(a_j)$ can serve as a non-repudiation proof by an MS as an evidence of n visits in the j^{th} chain made by a VLR. Note that due to the desired property of hash chaining, for each hash chain, the verifier only needs to keep the most recently released chain value (i.e., $f^{M-m}(b_i)$ kept by a VLR and $g^{N-n}(a_j)$ kept by an MS) as an evidence, (see section VI-B for explanation.) This is good for mobile handsets because of their limited space constraint.
- Stronger mutual authentication: To achieve mutual authentication between an MS and a VLR, two hash chain sets are established, one for each direction. The one-way hash chaining algorithm prevents all users, except the legitimate one, from computing backward values using the published one-way value. Our method also removes the assumption of secure channels between VLRs as there is no need to transfer leftover AVs. Therefore, this technique provides stronger mutual authentication than the current 3G protocols.
- Stronger periodical authentication: In UMTS [6], the periodical authentication is achieved by comparing a counter value between an ME and a VLR periodically. The counter value is susceptible to synchronization failure. In our enhanced protocol, either a VLR or an MS can periodically request to authenticate the other by having the other side prove itself. It is only when the submitted value satisfies the hash chain property, is the claimant successfully authenticated. This way is stronger than simply comparing the counter value.
- Mutual authentication without synchronization: Since there are two hash chain sets, one for each direction, and each side authenticates the other at its own pace, there is no need for authentication synchronization between both sides.
- Authentication flexibility: Because of the mutual authentication without synchronization feature, if it is necessary to provide only one-way authentication to function like a 2G system, one can simply omit the undesired set of chains.
- Simplicity and Elegancy: Our enhancements do not use SEQ (sequence number) as in UMTS, or COUNT (call history counter) in cdma2000. As shown in UMTS Security Architecture [6], the management of SEQ complicates both protocol and implementation tremendously, especially with regard to the considerations of simultaneous registration in CS and PS domains, re-synchronization failure recovery, and leftover authentication vector transferring between VLRs, etc.
- Convenience and Security: By using a VLR's own hash chaining set, the VLR has the convenience of the local control in authenticating an MS. Yet an HLR still has the total control in security by means of the HLR-generated master keys CK_H and IK_H and non-repudiation services.
- No leftover authentication vector transferring problem: Each MS and VLR pair has two unique sets of hash chains, one for each direction. When an MS roams out of a VLR domain, the MS will establish two new sets of hash chains with a new VLR. The MS and the old VLR can still keep their old authentication states so that future connections can resume from the point where they leave each other. Thus, our scheme does not have leftover vector transferring problem as in UMTS.
- Ease of re-synchronization: For any connection, if there is an authentication failure, the next fresh hash chain is used, thereby making re-synchronization between an MS and a VLR a simple task.

3) Time and Space Analysis: For each registration with a new service domain, an MS performs $I \times M$ one-way hash computations and one HMAC computation, and a VLR performs $J \times N$ one-way hash computations and one HMAC computation. These computations are good for $min(I \times M, J \times N)$ AKA invocations, since if either an MS or a VLR runs out of its set of hash chains, a new registration will be invoked to establish new sets of hash chains. A slight variation can be done to make only the side running out of chains to establish a new set. However, care must be taken to ensure the security of the modified protocol. The one-way hash computations can be pre-computed and stored in some extra memory storage to reduce the computation delay.

As mentioned in section VI-B, Jakobsson [20], and Coppersmith and Jakobsson [12] proposed a $log_2(M)$ for both space and access time with a chain of M elements. By adopting their algorithm, Table I lists the storage requirement

for both an MS and a VLR.

TABLE I
STORAGE REQUIREMENT

	MS	VLR
Storage of hash chain points for proving its authenticity	$O(I\ log_2(M))$	$O(J\ log_2(N))$
Storage for authenticating the other party	$O(J)$	$O(I)$

In Table I, the reason that only $O(J)$ or $O(I)$ proofs are stored is because an MS or a VLR, respectively, only need to store the most recently released value in each chain for authenticating the other party. For a given hash chain, the most recently released value can be served as a proof for other visits made by the other party (see section VI-B for the detailed explanation.)

There usually is a tradeoff between efficiency and overheads in communications. In GSM (UMTS), one has to consider the number of the triplets (authentication vectors) that are generated by HLR and kept in VLR. In our enhancement, it is the the selection of the values I, M, J, and N. For the limited storage applications such as an MS handset, one can further reduce the space required by the MS in Table I by considering the following solutions:

- Trading space with time implementation: Without storing any immediate f hash chaining values (i.e., $f^1(b_i)$ to $f^M(b_i)$), upon request, an MS can calculate $f^{M-m}(b_i)$ on the fly starting from $f^1(b_i)$, $f^2(b_i)$, and so on.
- Protocol variation: One can adopt the approach of transferring unused authentication data (such as unused hash chains and unused portion of a hash chain) from an old VLR to a new VLR similar to that in UMTS. However, extra steps are necessary to ensure the security of the modified protocol.

VII. CONCLUSION AND SUMMARY

Our main contributions in this paper are the enhancements on the authentication and key agreement protocol in the 3G network access security. To understand the basis of our enhancements, we provide an evolutionary and comparative study of this protocol in two most popular 3G cellular systems, UMTS and cdma2000.

The approaches adopted by the two 3G front runners aim to solve the 2G security problems and satisfy the higher 3G security requirements. Specifically, UMTS uses a sequence number approach to provide network authentication, a feature not in 2G. Cdma2000 has approved the adoption of the same technique. The sequence number record keeping complicates the already complex 3G implementation. In our study, we recommend to use a combination of hash chaining and keyed-Hash Message Authentication Code techniques instead. This combined approach not only simplifies both protocol and implementation, but also provides stronger periodically mutual authentication and non-repudiation services in an elegant way.

ACKNOWLEDGEMENT

We wish to thank Dr. Lily Lidong Chen at Motorola, Inc. and Dr. John Cigas at Rockhurst University for their constructive comments in the initial draft of this paper.

REFERENCES

[1] Al-Muhtadi, J., Mickunas, D., and Campbell, R. "A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices". IEEE Communications Magazine. vol 40. no. 10. April 2002.
[2] Almaimani, M., Korsuwana, P., Twine, M., and Mendelsohn, J. "IMT-2000: A Comparative Analysis of cdma2000 and UTRA".
[3] Rnderson, R., Manifavas, C., and Southerland, C., "NetCard - A Practical Electronic Cash System". Proc. International Workshop on security Protocols. Cambridge, UK. pp. 49-57. April 10-12, 1996.
[4] Asokan, N., Tsudik, G., and Waidner, M. "Server-supported signature". Proc. 4^{th} European Symp. on Research in Computer Security (Lecture Notes in Computer Science). vol 1146. pp. 131-143. 1996.
[5] 3GPP TS 21.133. "3GPP: Technical Specification Group services and System Aspects; 3G Security; Security Threats and Requirements".
[6] 3GPP TS 33.102. "3GPP: Technical Specification Group services and System Aspects; 3G Security; Security Architecture".
[7] 3GPP TS 33.120. "3GPP: Technical Specification Group services and System Aspects; 3G Security; Security Principles and Objectives".
[8] 3GPP2 C.S0004-A-2. "Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems -Addendum 2". File C.S0004-A_v6.0.pdf. February 2002.

[9] 3GPP2 C.S0005-A v6.0. ”Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems -Release A Addendum 2”. File C.S0005-A_v6.0.pdf. February 2002.
[10] 3GPP2 S.S0055-0_v1.0. ”Enhanced Cryptographic Algorithms”. File S.S0055-0_v1.0.pdf. January 21, 2002.
[11] 3GPP2 S.R0032. ”Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP)”. Version 1.0. December 6, 2000.
[12] Coppersmith, D. and Jakobsson, M. ”Almost optimal hash sequence traversal.” Proceedings of the fourth conference on Financial Cryptography (FC’02). Lecture Notes in Computer Science. 2002.
[13] Dalal, Neerav. ”A comparative study of UMTS and cdma2000.” IEEE METROCON. 2001.
[14] Federrath, Hannes. ”Security functions in mobile communication systems.” University of Technology Dresden.
[15] ”The Keyed-Hash Message Authentication Code (HMAC)”. Federal Information Processing Standards Publication. Draft. 2001.
[16] ”Secure Hash Standard”. FIPS publication 180-1. April 17, 1995.
[17] Gennaro, R., and Rohatgi, P. ”How to Sign Digital Streams”. Advances in Cryptography - Crypto’97. pp. 180-197.
[18] Harn, L., and Lin, H. ”Modifications to Enhance to Security of GSM”. 5^{th} National Conference on Informal Security. Taiwan. May 1995.
[19] Harn, L., and Lin, H. ”A Non-Repudiation Metering Scheme”. IEEE Communications Letters. vol 5. no 12. December 2001.
[20] Jakobsson, M. ”Fractal hash sequence representation and traversal.” Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT’02”. pages 437-444. July 2002.
[21] Lamport, L. ”Password authentication with insecure communication”. Communications ACM. vol. 24. no. 11. pp. 770-772. 1981.
[22] Lin, H.Y., and Harn, L. ”Authentication Protocols with Non-Repudiation services in Personal Communication Systems.” IEEE Communications Letters. vol 3. no 8. pp 236-238. August 1999.
[23] Millan, William. ”Cryptanalysis of the alleged CAVE algorithm”. ICISC 1998. pp 107-119.
[24] Mouly, Pautet. ”The GSM system for mobile communication”.
[25] Niemi, Valtteri. ”UMTS security and the rule of PKI”. Eurescom Workshop. June 2001. http://www.eurescom.de/ pub/seminars/past/2001/SecurityFraud/11-Niemi/s1d001.htm
[26] Pesonen, Lauri. ”GSM Interception.” 1999.
[27] Krawczyk, H., Bellare, M., and Canetti, R. ”Keyed-Hashing for Message Authentication”. Internet Engineering Task Force, Request for Comments (RFC) 2104. February 1997.
[28] Madson, C., and Glenn, R. ”The use of HMAC-MD5-96 within ESP and AH”. Internet Engineering Task Force. Request for Comments (RFC) 2403. November 1998.
[29] Madson, C., and Glenn, R. ”The use of HMAC-SHA-1-96 within ESP and AH”. Internet Engineering Task Force. Request for Comments (RFC) 2404. November 1998.
[30] Rose, G. ”Authentication and Security in Wireless Phones”. Qualcomm Australia.
[31] Schneier, B. Applied Cryptography. New York: Wiley. 1996.
[32] Wagner, D., Schneier, B., and Kelsey, J. ”Cryptanalysis of the Cellular Message Encryption Algorithm”. 3/20/97. Crypto’97 Conference, August 17-21, 1997.
[33] Wagner, D., Schneier, B., and Kelsey, J. ”Cryptanalysis of ORYX”, unpublished manuscript. May 4 1997.
[34] Zhang, M., Carroll, C., and Chan, A. ”Analysis of IS-95 CDMA voice privacy”. Selected Areas in Cryptography 2000.