Security Architecture in UMTS Third Generation Cellular Networks

Tomás Balderas-Contreras René A. Cumplido-Parra

Reporte Técnico No. CCC-04-002
27 de febrero de 2004

Luis Enrique Erro 1
Sta. Ma. Tonantzintla,
72840, Puebla, México.

Security Architecture in UMTS Third Generation Cellular Networks

Tomás Balderas-Contreras René A. Cumplido-Parra

Coordinación de Ciencias Computacionales,
Instituto Nacional de Astrofísica, Óptica y Electrónica,
Luis Enrique Erro 1, Sta. Ma. Tonantzintla,
72840, Puebla, MEXICO
balderas@inaoep.mx rcumplido@inaoep.mx

Abstract Throughout the last years there has been a great interest in developing and standardizing the technologies needed to achieve high speed transmission of data in cellular networks. As a result, mobile communications technology has evolved amazingly during the last decades to meet a very demanding market. Third generation (3G) wireless networks represent the more recent stage in this evolutionary process; they provide users with high transmission bandwidths which allow them to transmit both audio and video information in a secure manner. This report concerns a specific implementation of the 3G requirement specification: Universal Mobile Telecommunications System (UMTS), which is considered to be the most important of the 3G proposals. In order to protect the information transmitted through the radio interface, either user data or signaling data, an advanced security scheme was conceived. Among the features of this scheme are: mutual authentication, key agreement, block ciphering, an integrity algorithm and a confidentiality algorithm.
Keywords: Cellular Networks, 3G, UMTS, Security Architecture, AKA, KASUMI block ciphering algorithm, confidentiality and integrity algorithms.

1 Introduction

A cellular communication system is a special kind of wireless system whose features are the following:

Frequency reuse: The whole coverage area is divided into several smaller areas, called cells, in such a way that some transmission frequencies are used across a set of cells, and reused for another set of cells with little potential for interference.

Mobility/Roaming: Subscribers are able to move freely around their home network and from this to another one. This feature requires that the network tracks the location of each subscriber in an accurate way, in order to deliver calls and messages properly.

Handoff/Handover: The subscriber transitions from one radio channel to another as he/she moves from one cell to another while engaged in a conversation.

Throughout the decades the need for ubiquitous communications has driven and encouraged the development, and subsequent deployment, of several technologies to provide users with effective cellular communication means. Managers, executive officers and business people in general need to access their corporations' information while traveling, consult information regarding the stock market, as well as call up their families and employees. For the rest of the people, cellular communications represents a great opportunity to keep in touch with each other by exchanging messages, engaging in voice sessions and transmitting data to/from the Internet; all through low-power mobile handsets.

The third generation (3G) proposal for cellular communications claims to provide global roaming, high transfer rates and advanced services such as: commerce, global positioning system and multimedia messaging services via audio and video. All of these potential services, as well as the kind of information transmitted throughout the network, make security issues more important to consider than before and security requirements even more stronger. This report provides deep information about the features of third generation proposals for cellular communications and the way security issues are addressed within these networks. The rest of the document is organized as follows: section 2 describes the requirement specification for 3G systems and the organization of a UMTS cellular network, section 3 deals with the processes, agreements and algorithms involved in UMTS' security architecture, and section 4 concludes.

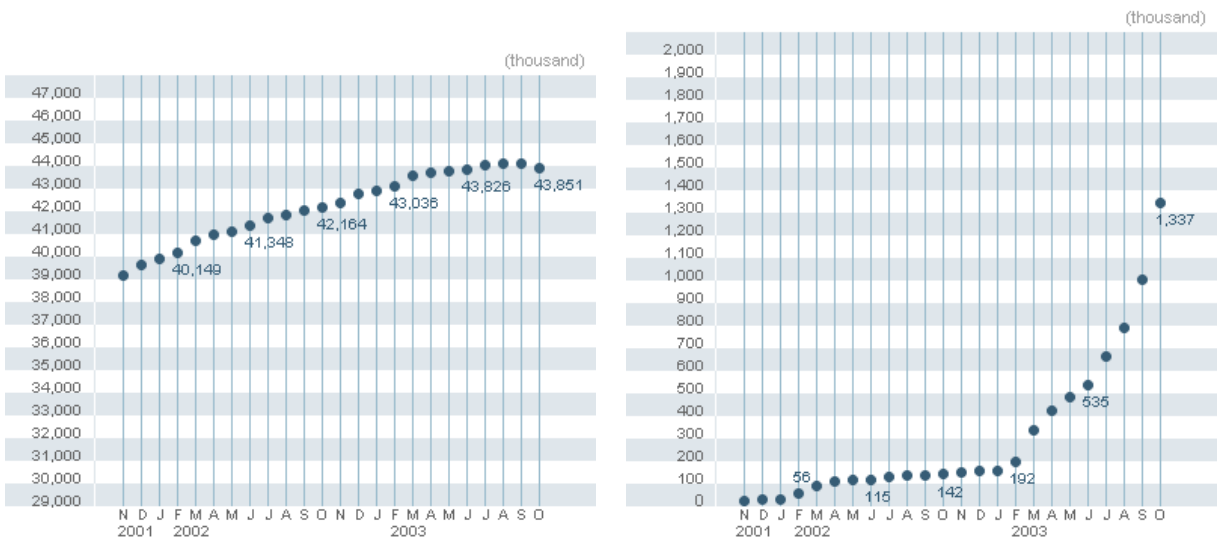
2 Third Generation (3G) networks

That the world is ready to develop a third generation technology for cellular telecommunications has been a generalized opinion during the last two decades. Standardizing organizations, network operators and manufacturers have encouraged development efforts since a long time ago, and the world is witnessing the first results right now. The first 3G network in the world has been servicing plenty of users in Japan for more than two years, and it has been such a great success.

In October 2001 the company NTT DoCoMo, Japan's premier communications company, put the first third generation cellular communications service into operation for the Japanese market. This service is called Freedom Of Mobile multimedia Access (FOMA). Key advantages for users include:

- The ability to speak to another user, face-to-face, by videophone
- Impressive high data rates for data transmission
- Simultaneous communication by voice and packet transmission
- The capacity to download and e-mail multimedia content
- Videoconferencing for up to eight participants
- Secure purchasing thanks to high levels of confidentiality and authentication
- I-mode mobile internet service

Figure 1 depicts some charts which show the subscriber growth of the services provided by the company. As can be seen, there are more than 43 millions of subscribers of the second generation PDC system, and increments have not been dramatic during the last two years. However, for the third generation service the increase in the number of subscribers is far from being linear and the trends are evident. Even though the current number of subscribers hardly surpasses one million,



(*a*) PDC (*b*) FOMA

Figure 1: Subscriber growth rate of the second generation and third generation services provided by NTT DoCoMo (from [9]).

there are great expectations for the next years both in Japan and other countries where third generation networks are being deployed.

Data in figure 1 gives an idea of the great demand for the services from one operator, the one that services only the Japanese market. What can be said about the number of operators in the rest of the world? A certain frequency spectrum, the one that allows greater capacity, was reserved for third generation cellular communications. Figure 2 shows the number of licenses of this spectrum that have been granted to network operators in Europe and Asia since 1999. As can be seen from the figure, almost 150 licenses have been granted to a number of network operators; this is a sign that there is a great interest to deploy third generation services in more and more countries. Moreover, table 1 shows the total amounts that were paid by network operators in each of several countries in order to get, from the corresponding regulator, licenses of use of frequency spectrum needed to begin to commercialize their communications service.

The information provided above shows that there exists a great interest in developing 3G networks worldwide and that several companies have invested lots of money in this effort. As a consequence, this technology will drastically change the way of living of the society in the next years. Not only is it necessary to deploy networks, but the services they provide must be advanced, reliable and secure in order to satisfy the customer's expectations. Meeting these requirements is not an easy task since several complex operations are carried out throughout the network that must be addressed carefully in order to implement them in an efficient way. The rest of this section addresses two important issues concerning 3G: First, the mainstray of the third generation technology: the International Mobile Telecommunications-2000 requirement specification defined by the International Telecommunication Union (ITU). Second, the architecture and components present in UMTS networks. UMTS is the third generation proposal expected to have the greatest success all around the world.

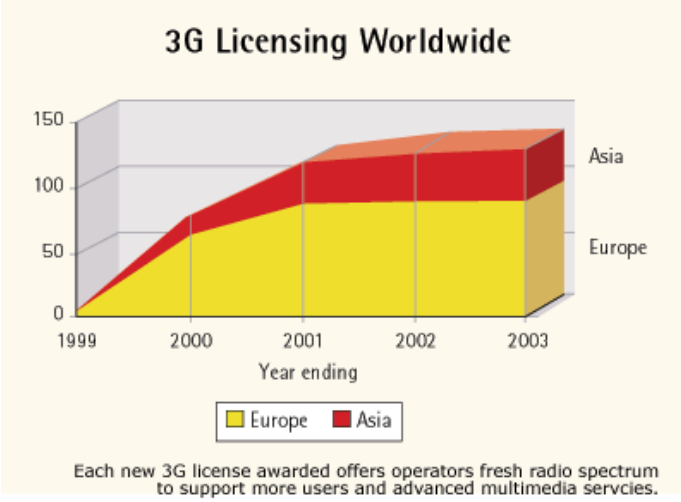


Figure 2: Number of licenses of third generation spectrum granted since 1999.

Table 1: Total cost of 3G spectrum licensing in several countries (from [1]).

Country	Total cost (USD)	Regulator
Australia	351,700,000	Australian Communications Authority
Canada	931,237,000	Industry Canada
Finland	0	The Ministry of Transport and Communication
France	1,102,000,000	Autorité de regulation del télécommunications
Germany	45,850,000,000	Regulatory Authority for Telecommunications and Posts
Israel	157,240,000	Israel Ministry of Communications
Italy	10,070,000,000	Italian Communications Authority
Japan	0	The ministry of Posts and Telecommunications
Norway	44,800,000	Norwegian Post and Telecommunications Authority
Sweden	42,800	The Swedish National Post and Telecom Agency
U.K.	35,390,000,000	Office of Telecommunications

2.1 International Mobile Telecommunications-2000

Everything that 3G is intended to be is well established in a specification defined by the International Telecommunications Union: International Mobile Telecommunications-2000 (IMT-2000) [7]. This document is meant to be a unifying specification that comprises multiple technologies covering many frequency bands, channel bandwidths, modulation formats and network organizations. The following is a list of the general objectives IMT-2000 aims to achieve:

- To make available to mobile users a wide range of services, both voice and data, irrespective of their location
- To provide services over a wide coverage area
- To provide the best quality of service (QoS) possible
- To extend the number of services provided subject to constraints like radio transmission, spectrum efficiency and system economics
- To accommodate a great variety of mobile stations
- To admit the provision of service by more than one network in any area of coverage
- To provide an open architecture which will permit the easy introduction of technology advancements as well as different applications
- To provide a modular structure which will allow the system to start from small and simple configuration and grow as needed, both in size and complexity within practical limits

The specification lays down some other operational objectives that are worth mentioning here:

- To provide for the required user authentication, unique user identification, unique user numbering and unique equipment identification scheme
- To enable each mobile user to request particular services as well as initiate and receive calls. Multiple simultaneous calls are allowed, which might be associated to different services either voice or data
- To minimize the opportunity for fraud by restricting some services which are prone to fraud
- To protect users against misuse of stolen mobile stations by maintaining a list of stolen mobile stations identities and monitoring traffic for their use
- To aid emergency services by providing, as far as possible, useful information along with the emergency call: user identity, location information and other information that might be needed for local authorities
- To support user mobility by registration on different terminals. This can be accomplished by providing users with individual Subscriber Identity Module (SIM) cards
- To allow international operation and automatic roaming of mobile subscribers and their stations
- To provide service to a variety of mobile stations ranging from those which are small enough to be easily carried by a person to those which are mounted in a vehicle

- To provide high speed packet data rates:
  - 2 Mbps for fixed environments
  - 384 Kbps for pedestrian
  - 144 Kbps for vehicular traffic

The exact spectrum band allocated to IMT-2000 by ITU is 1885 MHz-2025 MHz and 2110 MHz-2200 MHz, as shown in figure 3. It can be noticed that the spectrum allocation is very similar in Europe and Japan, but in the United States great part of the spectrum is already used by second generation systems. As a consequence, American network operators will need to gradually replace their existing infrastructure with similar third generation technologies.

In November 1999 the ITU recognized that the following radio interface technology proposals fulfilled IMT-2000's requirements and accepted them as compatible:

- IMT Direct Spread (IMT-DS; also known as UTRA)
- IMT Multicarrier (IMT-MC)

Of these, the most important radio interface standard is Universal Terrestrial Radio Access (UTRA), which is a radio interface based on Wideband-CDMA (WCDMA) technology and operates in two modes: Frequency Division Duplex (FDD) and Time Division Duplex (TDD). It has received support both from the European Telecommunications Standards Institute (ETSI) and the Association of Radio industries and Businesses (ARIB).

In December 1998 the 3rd Generation Partnership Project (3GPP) Agreement was formalized and signed. This collaboration agreement gave rise to a standardization organization which comprises several telecommunications standards bodies, or Organizational Partners. The organization is called 3GPP as well and its goal is to produce specifications for UMTS, a third generation system based on two important technologies: the UTRA radio interface and the extended GSM/GPRS network. Later, the organization's scope was extended to include the maintenance and further development of GSM's technical specifications as well as GPRS' and EDGE's.

Due to ITU's policy of not excluding any serious candidate from IMT-2000 specification, a second radio interface exists. This radio interface, as mentioned above, is called IMT-MC and its use is promoted by the 3GPP2 standardization organization. While 3GPP specifies a new radio interface, 3GPP2 specifies an interface backward compatible with IS-95 systems, which makes transition to 3G systems much easier. This alternative third generation proposal is known as CDMA2000.

2.2 Universal Mobile Telecommunications System's architecture

A UMTS network is logically divided into two parts, which are referred to with the generic terms Core Network (CN) and a Generic Radio Access Network (GRAN) [2, 8, 10, 11]. The core network reuses several elements already present in GPRS and GSM networks, and consists of two overlapping domains: Circuit-Switched (CS) domain and Packet-Switched (PS) domain. CS domain is made up of those entities which allocate dedicated resources for user traffic and control signals when the connections are established, and release them when the sessions finish. Generally, voice calls are always handled by the components belonging to CS domain. The entities in the PS domain transport user data in the form of autonomous packets, which are routed independently of each other; this scheme overcomes the limitations of 2G networks to transmit data efficiently. It is through the CN that the user can set up a connection to and from external packet data networks

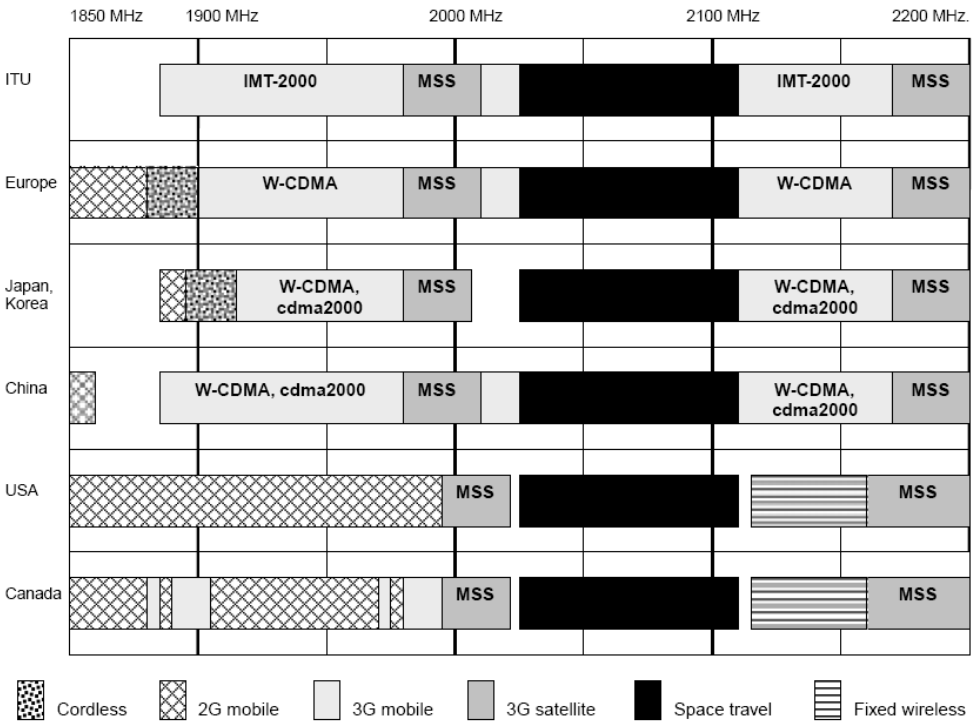


Figure 3: Spectrum allocation for 3G cellular and MSS (Mobile Satellite Service) in several countries.

(e.g. Internet), public switch telephone networks (PSTN) and other wireless networks. The UMTS Terrestrial Radio Access Network (UTRAN) is UMTS' implementation of the GRAN concept. Some of the functions performed by its components are:

- Management of radio resources
- Power control both in the downlink and the uplink direction
- Handover management and allocation of channels for transmission

Since several components in the CN are legacy of GSM/GPRS networks, they allow the connection to GSM radio access networks as well. As a consequence, GSM's Base Station Subsystems (BSSs) and UMTS' Radio Network Subsystems (RNSs) can coexist within a public mobile network's UTRAN.

The first release of UMTS specifications published by 3GPP is known as 3GPP Release 99 due to a naming scheme used with GSM specifications which were released on yearly basis. This release provides specifications concerning the UTRAN radio access network, based on the UTRA (IMT-DS) radio interface, and the enhancements to GSM/GPRS core networks. The next release was originally called 3GPP Release 2000, but the new changes were so significant to be totally included in a single release. Consequently, Release 2000 was divided into Release 4 and Release 5. Currently, Release 6 is under planning.

Figure 4 depicts the architecture of a UMTS network, according to Release 99. The diagram shows both the CN and the UTRAN, the mobile stations, the components of the CS and PS domains, the interfaces that link the components to each other and the external networks that can

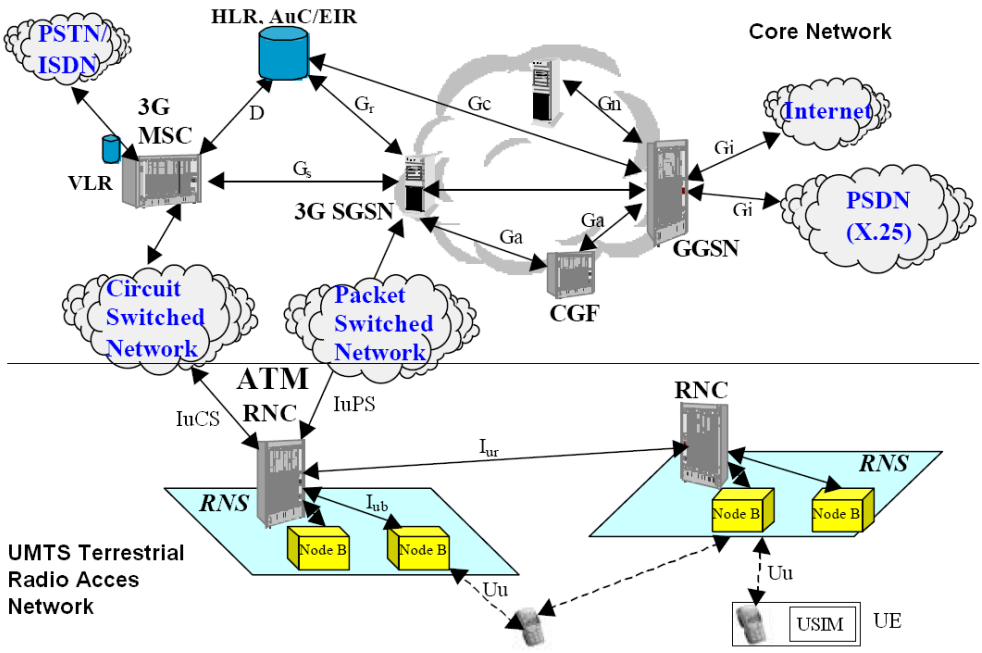


Figure 4: Basic architecture of a UMTS mobile network (Release 99) (from [11]).

be reached. Figure 5 shows the most recent proposal for the organization of a UMTS network: the all-IP multimedia network architecture defined in Release 5. The main feature of this architecture is that both voice and data are carried over IP packets all the way from the mobile station to final destination, thanks to the addition of a new domain in the core network: the IP-Multimedia domain (IM).

The next is a brief description of the UTRAN components:

User Equipment/Mobile Station (UE/MS): Is the physical device used by users. It consists of a Mobile Equipment (ME) and an UMTS Subscriber Identity Module (USIM). The USIM is an application stored in a removable IC card which interoperates with the ME to provide access to 3G services and has the following features:

- Unambiguously identifies a subscriber
- Stores subscriber and subscription related information
- Authenticates itself to the network and vice versa (mutual authentication)
- Provides security functions
- Stores information elements such as: preferred language, IC card identification, International Mobile Subscriber Identity (IMSI), cipher key, among others

Node B: Is the base transceiver station of the UTRAN that serves one or more cells (sectors). Some of its functions include: error detection on transport channels and indication to higher layers, modulation/demodulation of physical channels, radio measurements and notification to higher layers and power weighting. Some vendors offer base stations that support both UMTS and CDMA2000 standards through the use of field-replaceable modules and a high percent of compatible hardware and software. The interface between UE and Node B (Uu in figure 4) is actually the WCDMA-based UTRA radio interface.

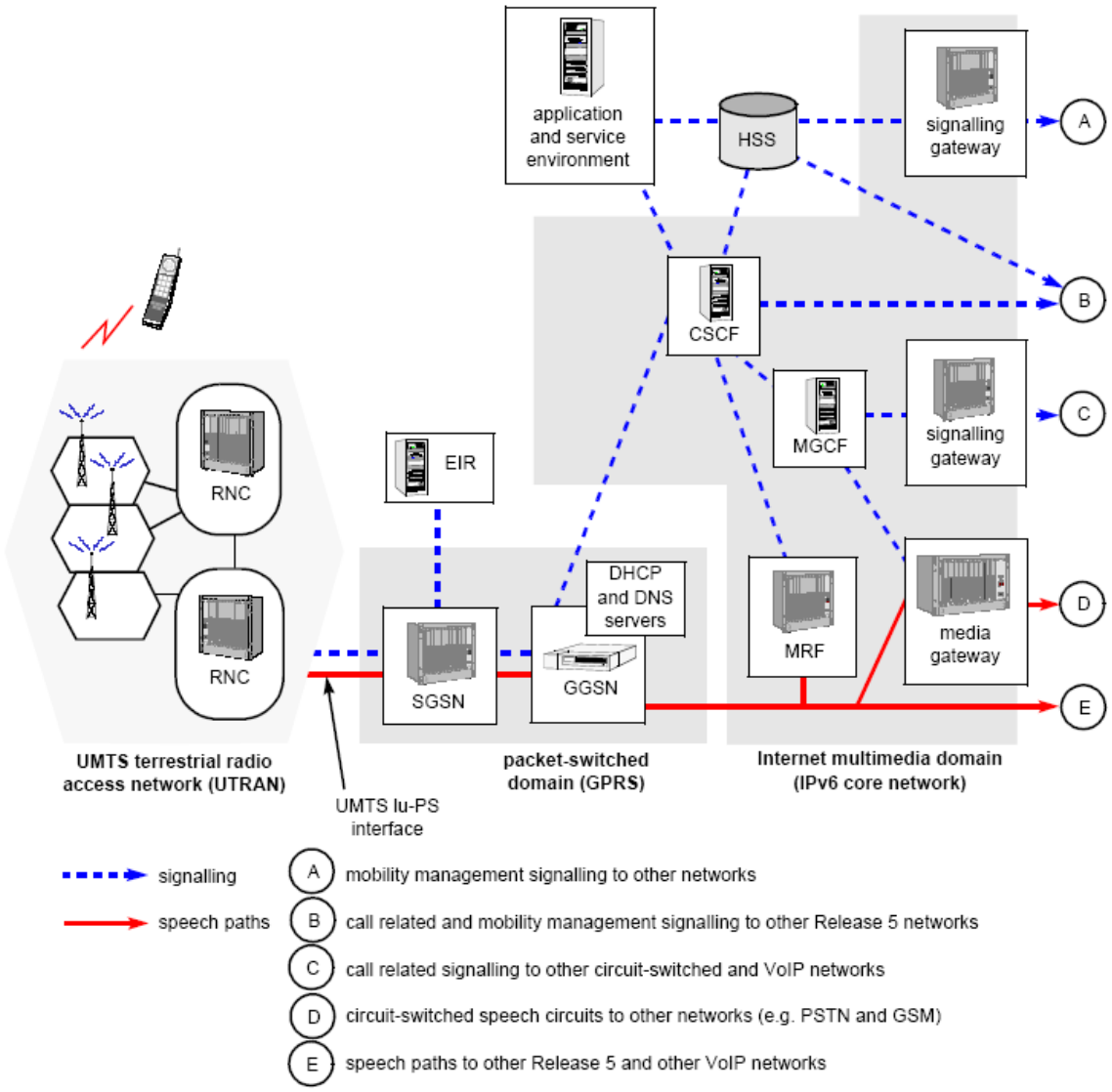


Figure 5: 3GPP IP Multimedia Network Architecture (Release 5).

Radio Network Controller (RNC): Manages the radio resources of each of the Node Bs that are connect to it. Figure 4 shows that the RNC is connected to the core network's CS domain through the IuCS interface, and to the PS domain through the IuPS interface. Not only does the RNC manage the user equipment's radio resources, but it is part of the path to/from the core network for the services being used by the user equipment. Some other tasks performed by RNC include: processing of voice and data traffic, handoff between cells and calls setup and termination.

Now it is time to give a brief description of the elements that are specific the core network's CS domain:

Mobile services Switching Center (MSC): This is the main component of the network's CS domain. It is the interface between the cellular network and external fixed circuit-switched telephone networks such as PSTN. This component performs the routing of calls from the external network to an individual mobile station and all the switching and signaling functions for mobile stations located in a geographical area designated as the MSC area. Additional functions include:

- Carrying out the procedures required for location registration and handover.
- Collection of data for charging purposes
- Encryption parameter management

Additional MSCs might coexist within the cellular network if the traffic requires more exchange capacity than the provided by one of them. The IuCS interface links the MSC with the RNC in the UTRAN and some interfaces exist to the PS domain, the PSTN, other MSCs and the registration components in the network.

The following is a list of entities that were originally defined only for circuit-switched GSM networks, but in GPRS and UMTS standards are shared between CS and PS domains since they are involved in the operations of both domains:

Home Location Register (HLR): This module stores data related with each subscriber of the services provided by the mobile network. This information is entered when the user subscribes to the network. There are two kinds of information in an HLR register entry: permanent and temporary. Permanent data doesn't change unless a subscription parameter is required to be modified. Temporary data change continuously, even from call to call, and some items might not always be necessary. Permanent data relevant for the purposes of this report include the IMSI and an authentication key. A mobile network can have several HLRs depending on the size of its coverage area.

Visitor Location Register (VLR): This component is generally implemented in connection with a MSC, as illustrated in figure 4. The VLR holds information related to every mobile station that roams into the area serviced by the associated MSC. Thus, the VLR contains information about the active subscribers in its network, even from those to whom this network is their home network. As the subscriber registers with different networks, the information in his HLR is copied to the VLR in every network visited, and discarded when the subscriber leaves that network. The information stored by the VLR is quite the same as that stored by the HLR.

Authentication Center (AuC): Physically exists with an HLR, as depicted in figure 4. This component stores, for each subscriber, an authentication key K as well as the corresponding IMSI, which are permanent data entered at subscription time. AuC plays a crucial role in the network's security architecture, discussed later, since it is responsible of the generation of important data used in the authentication and encryption procedures.

The components of the PS domain in the UMTS network, depicted in figure 4, are upgraded versions of those defined for GPRS networks [11]. They are described below:

Serving GPRS Support Node (SGSN): This component is responsible for the mobility management and IP packet session management. It routes user packet traffic from the radio access network to the appropriate Gateway GPRS Support Node, which in turn provides access to external packet data networks. In addition, it generates records to be used by other modules for charging purposes. SGSN helps to control access to network resources, preventing unauthorized access to the network or specific services and applications. The IuPS interface links the SGSN, the main component of the PS domain, with the RNC in the UTRAN, as noticed in figure 4.

Gateway GPRS Support Node (GGSN): This module is the gateway between the cellular network and external packet data networks such as the Internet and corporate intranets. As its partner the SGSN, and other components, the GGSN also collects charging information, which is forwarded to the Charging Gateway Function (CGF), depicted in figure 4, for charging purposes.

3 UMTS' Security Architecture

According to specifications, the security architecture is made up of a set of security features and security mechanisms [3]. A security feature is a service capability that meets one or several security requirements. A security mechanism is an element or process that is used to carry out a security feature. Figure 6 shows the way security features are grouped together in five different sets of features, each one facing a specific threat and accomplishing certain security objectives. The following is a description of these groups of features:

Network access security (I): Provides secure access to 3G services and protects against attacks on the radio interface link.

Network domain security (II): Allows nodes in the operator's network to securely exchange signaling data and protects against attacks on the wireline network.

User domain security (III): Secures access to mobile stations.

Application domain security (IV): Enables applications in the user and in the provider domain to securely exchange messages.

Visibility and configurability of security (V): Allows the user to get information about what security features are in operation or not and whether provision of a service depends on the activation or not of a security feature.

An exhaustive study of the literature revealed that some of the mechanisms that carry out the set of network access security features require the execution of algorithmic processes with the highest performance possible. So, the rest of this section concentrates on describing these algorithmic processes as well as the corresponding security mechanisms and features.

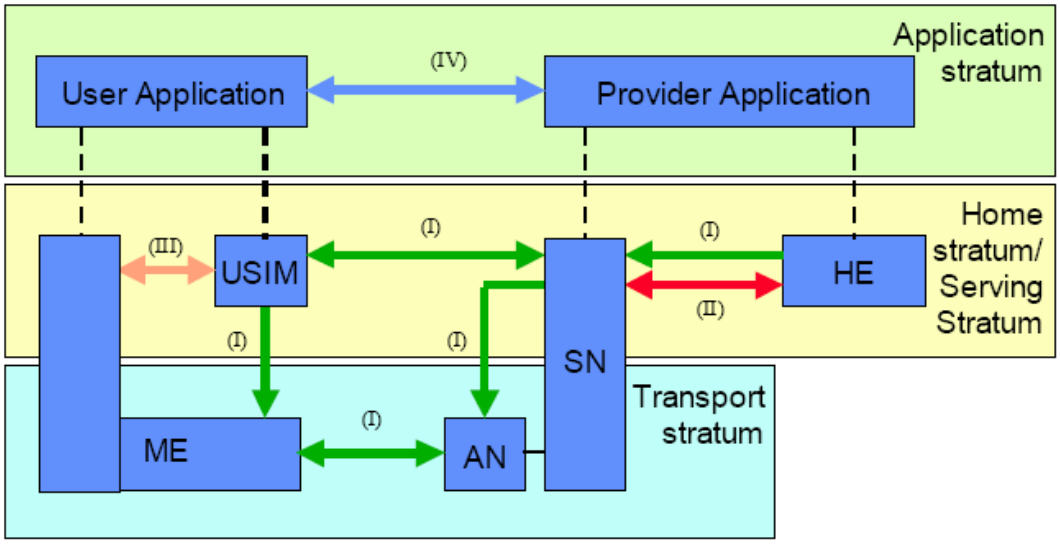


Figure 6: Overview of the security architecture (from [3]).

3.1 Network access security features

Network access security features can be further classified into the following categories: entity authentication, confidentiality and data integrity. The following is a description of the security features classified into the category of entity authentication:

User authentication: The property that the network that provides the service (serving network) corroborates the identity of the user.

Network authentication: The property that the user corroborates that he is connected to a serving network that is authorized by the user's home network to provide him services; this includes the guarantee that this authorization is recent.

The following security features deal with the confidentiality of data on the network access link:

Cipher algorithm agreement: The property that the mobile station and the serving network can securely negotiate the algorithm that they shall use subsequently.

Cipher key agreement: The property that the mobile station and the serving network agree on a cipher key that they may use subsequently.

Confidentiality of user data: The property that user data can not be overheard on the radio interface.

Confidentiality of signaling data: The property that signaling data can not be overheard on the radio interface.

The features provided to achieve integrity of data on the network access link are the following:

Integrity algorithm agreement: The property that the mobile station and the serving network can securely negotiate the integrity algorithm that they shall use subsequently.

Table 2: The structure of an authentication vector.

Field	Description
RAND	Random challenge
CK	Cipher key
IK	Integrity key
AUTN	Authentication token
XRES	Expected response

(a) Structure of an authentication vector

Field	Description
SQN	Sequence number
AMF	Authentication management field
MAC-A	Message authentication code

(b) Structure of the AUTN field of an authentication vector

Integrity key agreement: The property that the mobile station and the serving network agree on an integrity key they may use subsequently.

Data integrity and origin authentication of signaling data: The property that the receiving entity (mobile station or serving network) is able to verify that signaling has not been modified in an unauthorized way since it was sent by the sending entity (serving network or mobile station) and that the origin of the signaling data received is indeed the one claimed.

3.2 UMTS Authentication and Key Agreement (UMTS AKA)

UMTS AKA is a security mechanism used to accomplish the authentication features and all of the key agreement features described above. This mechanism is based on a challenge/response authentication protocol conceived in such a way as to achieve maximum compatibility with GSM's subscriber authentication and key establishment protocol, in order to make easier the transition from GSM to UMTS. A challenge/response protocol is a security measure intended for an entity to verify the identity of another entity without revealing a secret password shared by the two entities. The key concept is that each entity must prove to the other that it knows the password without actually revealing or transmitting such password.

The UMTS AKA process described in this subsection is invoked by a serving network after a first registration of a user, after a service request, after a location update request, after an attach request and after a detach request or connection re-establishment request. In addition, the relevant information about the user must be transferred from the user's home network to the serving network in order to complete the process. The home network's HLR/AuC provides serving network's VLR/SGSN with Authentication Vectors (AVs), each one holding the information fields described in table 2.

The authentication and key agreement process is summarized in the following algorithm and illustrated in figure 7:

Stage 1:

1. Visited network's VLR/SGSN requests a set of AVs from the HLR/AuC in the user's home network.

2. HLR/AuC computes an array of AVs. This is done by means of the authentication algorithms and the user's private secret key K, which is stored only in the home network's HLR/AuC and the USIM in the user's mobile station.

3. Home network's HLR/AuC responds by sending n authentication vectors AV1 ? AVn back to the visited network's VLR/SGSN.

Stage 2:

1. Visited network's VLR/SGSN chooses one AV and challenges mobile station's USIM by sending the RAND and AUTN fields in the vector to it.

2. The mobile station's USIM processes the AUTN. With the aid of the private secret key K, the user is able to verify that the received challenge data could only have been constructed by someone who had access to the same secret key K. The USIM will also verify that the AV has not expired by checking its sequence number (SEQ) field. Provided that the network can be authenticated and that the AV is still valid, the USIM proceeds to generate a confidentiality key (CK), an integrity key (IK) and a response for the network (RES).

3. The user responds with RES to the visited network.

4. Visited network's VLR/SGSN verifies that response is correct by comparing the expected response (XRES) from the current AV with the response (RES) received from the mobile station's USIM.

Mutual authentication is performed in step 5 of the former algorithm. Both the USIM and the VLR/SGSN have authenticated each other after two conditions have met: First, that the USIM has verified that the MAC field in AUTN equals a value computed internally using the key K and the fields SQN, RAND and AMF. Second, that the VLR/SGSN has verified that the RES value transmitted by user's mobile station equals the internal XRES value.

3.3 Integrity and confidentiality algorithms

Since the control signaling information transmitted between the mobile station and the network is so important and sensitive, its integrity must be protected. The mechanism that carries out this security feature is based on an UMTS Integrity Algorithm (UIA) implemented both in the mobile station and in the module of the UTRAN closer to the core network, i.e. the RNC. See figure 4.

The UIA explained in this subsection is the *f9* algorithm, depicted in figure 8. The procedure of data integrity verification is as follows: First, the *f9* algorithm in the user equipment computes a 32-bit message authentication code (MAC-I) for data integrity based on its input parameters, which include the signaling data (MESSAGE). Second, the MAC-I computed is attached to the signaling information and sent over the radio interface from the user equipment to the RNC. Third, once the RNC has received the information and the attached MAC-I, it computes XMAC-I on the signaling data received in the same way as the mobile station computed MAC-I. Fourth, the integrity of the signaling information is determined by comparing the MAC-I and the XMAC-I.

A detailed description of each of the input parameters is out of the scope of this document, further details concerning their meaning can be found in [4] and [5]. Figure 9 shows that the internal structure of the *f9* algorithm uses the shared integrity key IK and is based on a chain of

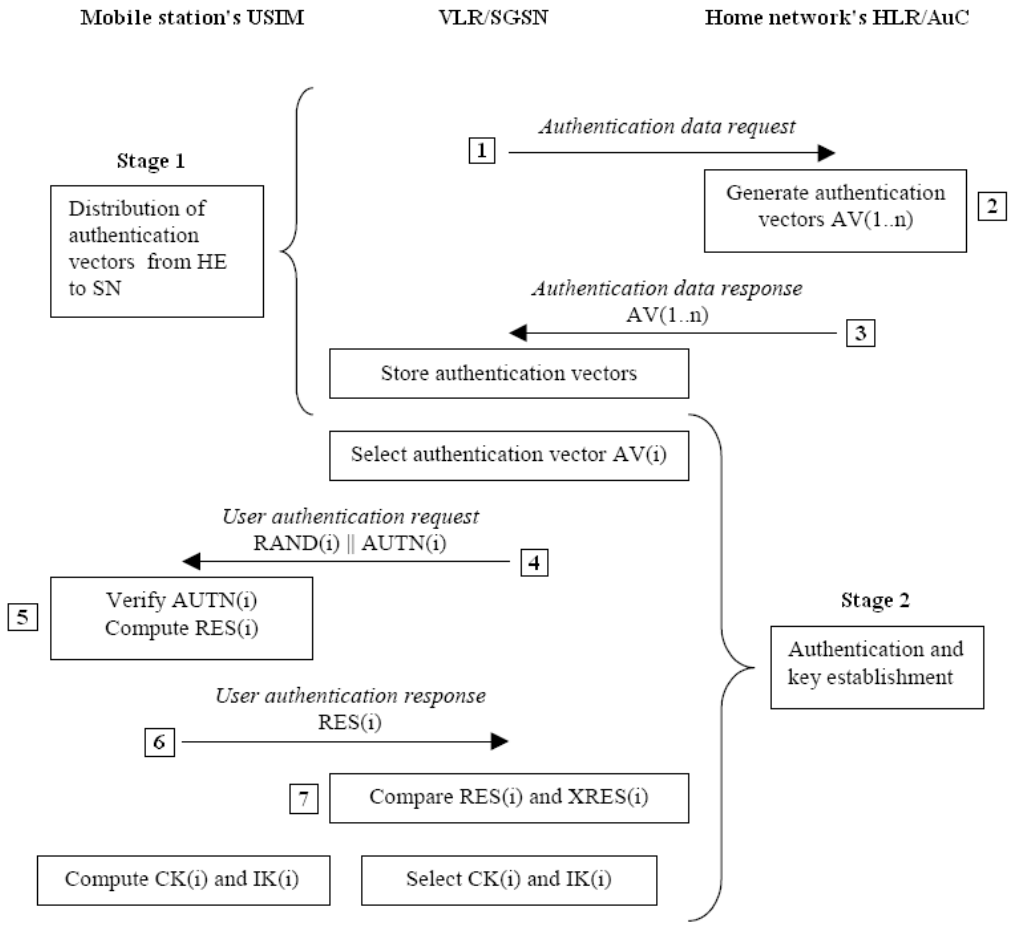


Figure 7: Authentication and key agreement (from [3]).

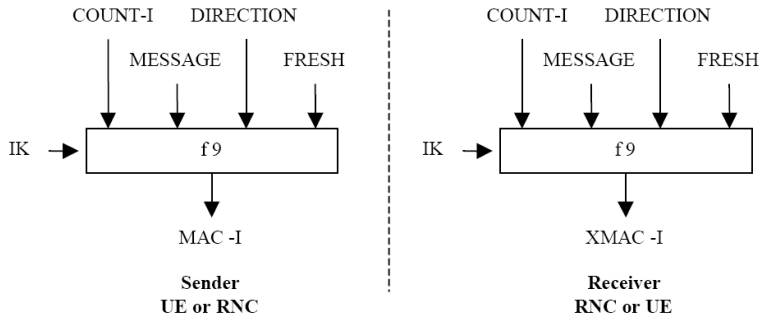


Figure 8: Derivation of Message Authentication Codes from signaling data using the *f9* algorithm (from [5]).

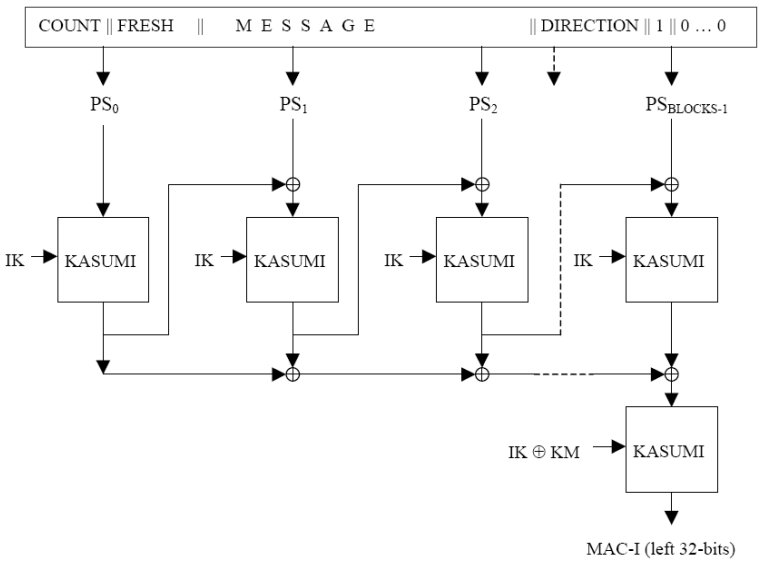


Figure 9: The *f9* integrity algorithm (from [5]).

block ciphers implementing the KASUMI algorithm. The outputs of the block ciphers are 64-bit long, but the output of the whole algorithm is 32-bit long.

Unlike the integrity algorithm, which only operates on signaling information, the confidentiality mechanism operates on both signaling information and user data. The algorithm defined to perform the confidentiality tasks is called *f8* and operates on the following way: First, using the ciphering key CK, and some other parameters, the *f8* algorithm in the user equipment computes an output bit stream. Second, this output bit stream is xored bit by bit with the data stream, also called plaintext, in order to obtain a ciphered data block or ciphertext. Third, the ciphertext is send to the network through the radio interface. Fourth, the *f8* algorithm in the RNC uses the same inputs as the user equipment, including the shared cipher key CK, to generate the same output bit stream that was computed in the user equipment. Finally, the output bit stream is xored with the ciphertext received to recover the initial information. Figure 10 shows this scheme.

Figure 11 depicts the structure of the *f8* algorithm. Once again, it can be seen that several blocks based on the KASUMI block cipher are present, this time the blocks are connected in the so called output-feedback mode. Each block generates 64 bits of the output bit stream and forwards its output to the input of the following block.

3.4 The KASUMI block cipher

As can be noticed from the former subsection, the KASUMI block cipher is at the core of the integrity and confidentiality mechanisms in UMTS networks. KASUMI is a cipher that has a Feistel structure and operates on 64-bit data blocks controlled by a 128-bit key [6]. Due to its Feistel structure, KASUMI has the following features:

- It is based on eight rounds of processing
- Input plaintext is the input to the first round
- Ciphertext is the last round's output

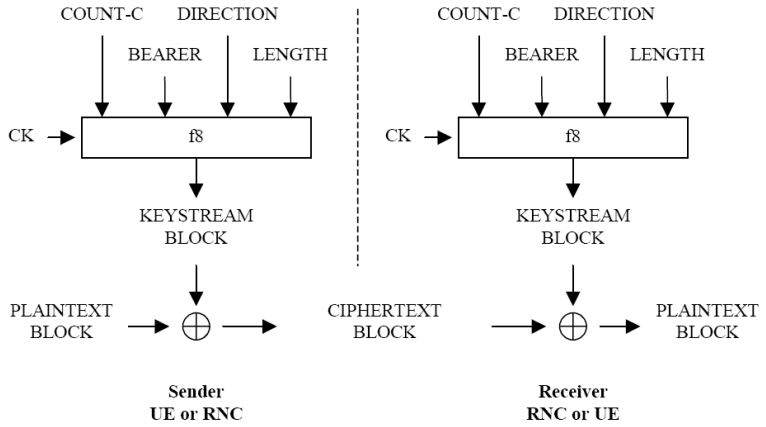


Figure 10: Ciphering of user and signaling data using the *f8* algorithm (from [5]).

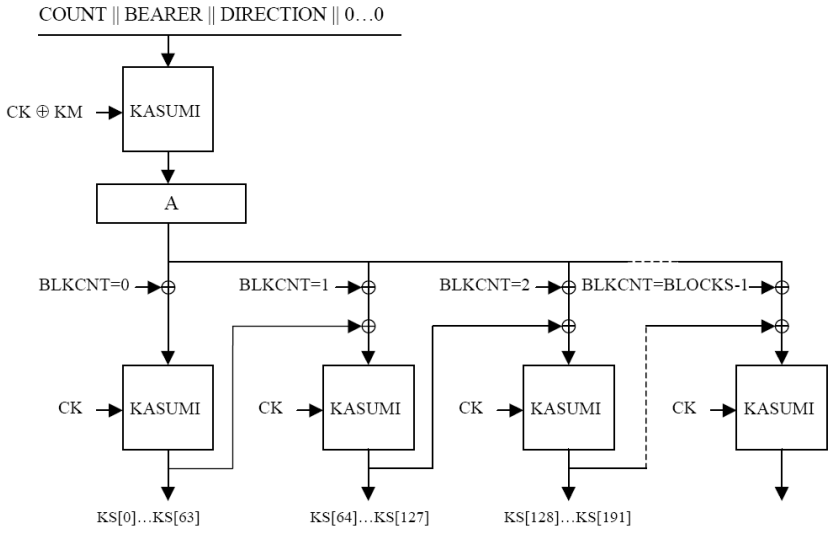


Figure 11: The *f8* confidentiality algorithm (from [5]).

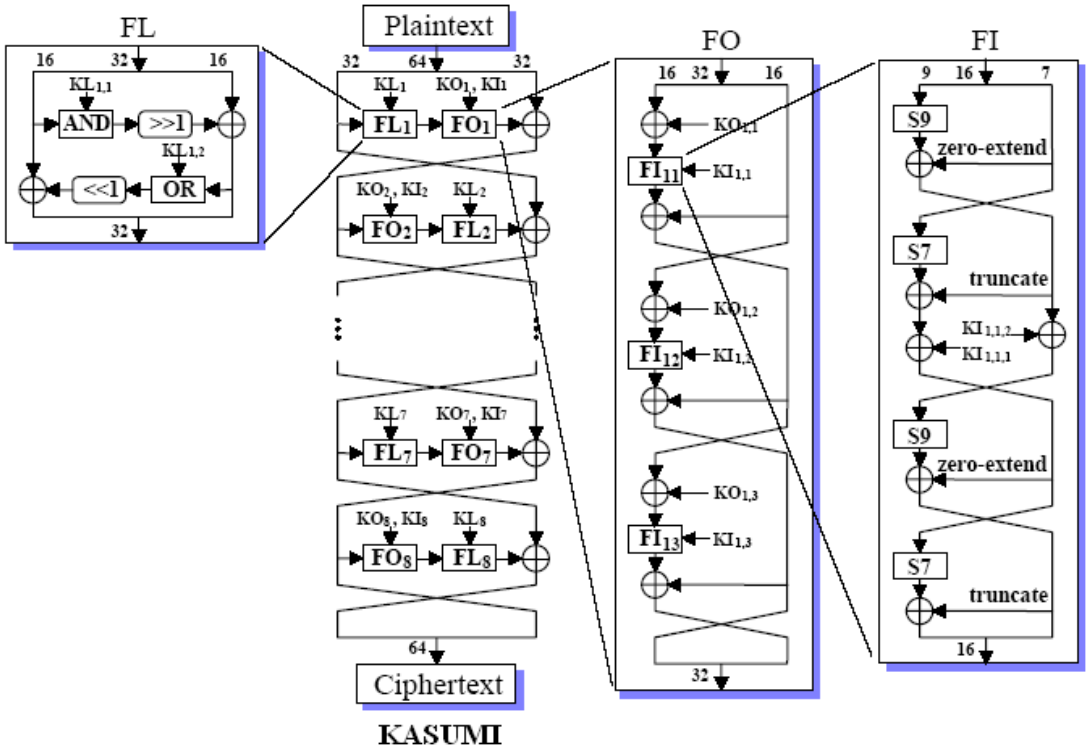


Figure 12: The components of the KASUMI block cipher (from [6]).

- Encryption key K is used to generate a set of round keys (KL_i, KO_i, KI_i) for each round i
- Each round computes a different function, as long as the round keys are different
- The same algorithm is used both for encryption and decryption

The development of the KASUMI block cipher is based on a previous block cipher called MISTY1. MISTY1 was chosen as the foundation for the 3GPP ciphering algorithm due to its proven security against the most advanced methods to break block ciphers, namely cryptanalysis techniques. In addition, MISTY1 was heavily optimized for hardware implementation.

Figure 12 shows the organization of the KASUMI block cipher. It can be seen that the function f computed by each round i is composed of two subfunctions FL_i and FO_i, which depend on the inputs of the round and the corresponding set of round keys. The figure also depicts the internal structure of each of the two functions. The FL function has a simple structure and consists of logical operations and shifts on the inputs. FO is more complicated and has itself a Feistel structure with three rounds, each of which requires computing the FI subfunction that, in turn, is made up of three rounds as well.

According to the specification, both the confidentiality and integrity algorithms were designed to allow a great variety of software and hardware implementation options. In addition, the algorithms must be implemented taking into account several constraints and requirements [4]. Hardware implementations, for instance, are required to use at most 10000 gates, they must achieve encryption rates in the order of 2 Mbps, since that is the likely maximum data rate. The specifications also indicate that in order to meet the throughput requirements the implementation must operate at frequencies upwards 200 MHz. From these comments it can be noticed that a considerable effort

must be performed in order to implement a high performance hardware component that carries out the operations of the KASUMI block cipher.

4 Conclusions

This document provided the reader with introductory information to the field of third generation cellular communications. The IMT-2000 specification, which defines everything that 3G is meant to be, was described in detail. Later, the organization of UMTS networks, the most important third generation standard, was explained. It can be noticed, from data showing the number of 3G spectrum licenses granted and the growth rate of users of 3G services, the great demand that exists from users and the enormous interest on the part of network operators. Therefore, a worldwide deployment is expected in the next years.

UMTS' Security Architecture consists of service capabilities that meet one or more requirements, known as security features, and the processes that carry out such capabilities, so called security mechanisms. The most important features are: mutual authentication, cipher algorithm and cipher key agreement, confidentiality of both user data and signaling, integrity algorithm and integrity key agreement and methods to guarantee both data integrity and origin authentication of signaling data. *f8* algorithm is used to guarantee confidentiality of both data and signals; and *f9* algorithm is employed to guarantee the integrity of signaling information. Both of these algorithms is based on the KASUMI block cipher, based on a Feistel structure.

References

1. 3G Newsroom. 2003. 3G License Information Database. http://www.3gnewsroom.com/3g_licenses_db/index.shtml
2. 3rd Generation Partnership Program. *Network Architecture*. Technical Specification 23.002. Release 5. Version 5.5.0.
3. 3rd Generation Partnership Program. *Security Architecture*. Technical Specification 33.102. Release 5. Version 5.2.0.
4. 3rd Generation Partnership Program. *Cryptographic Algorithm Requirements*. Technical Specification 33.105. Release 4. Version 4.1.0.
5. 3rd Generation Partnership Program. *Document 1: f8 and f9 Specification*. Technical Specification 35.201. Release 5. Version 5.0.0.
6. 3rd Generation Partnership Program. *Document 2: KASUMI Specification*. Technical Specification 35.202. Release 5.Version 5.0.0.
7. International Telecommunications Union. 1997. *International Mobile Telecommunications-2000*. Recommendation ITU-R M.687-2 (02/97).
8. Korhonen, J. 2001. Introduction to 3G Mobile Communications. Artech House, Inc. Norwood, MA.
9. NTT DoCoMo. 2003. Subscriber Growth. http://www.nttdocomo.com/companyinfo/subscriber.html
10. Smith, C. and D. Collins. 2002. 3G Wireless Networks. McGraw-Hill. Boston, MA.
11. Trillium Digital Systems, Inc. 2000. *Third Generation (3G) Whitepaper*. Los Angeles, CA. http://www.trillium.com/assets/wireless3g/white_paper/8722019.pdf