Tatra Mt. Math. Publ. **25** (2002), 109–125

TATRA MOUNTAINS
Mathematical Publications

A SURVEY OF SECURITY MECHANISMS IN MOBILE COMMUNICATION SYSTEMS

Milan Vojvoda

ABSTRACT. Security mechanisms used in mobile communication systems are discussed and main security requirements on wireless communication are outlined as well. Then, we focus on security solutions, used in the second generation (2G) mobile communication system–GSM, resp. in the third generation (3G)–UMTS, and discuss their security.

Mobile telephones are nowadays used worldwide by more than 300 million people. It is forecasted that this number will exceed 1 billion by year 2003. People no longer use mobiles just for voice communication. Applications such as Mobile Internet, GSM banking, etc. have started the era of mobile-commerce. Thus the security issues of mobile communications have become of tremendous interest.

Security of the first generation, analog mobile communications was very weak. It is relatively simple to intercept cellular phone conversations with a police scanner in older analog-based cellular telephone systems such as the Advanced Mobile Phone System and the Total Access Communication System [24]. The authentication of the user to the network is insecure, too. The user is identified through his/her Electronic Serial Number (ESN), that is transmitted unencrypted. It is possible to receive the ESN, impersonate the legitimate mobile user (subscriber) and place calls charged to the legitimate subscriber. This fraud, namely copying the identity, is called cloning. Estimates for cellular fraud in the USA in 1993 are as high as 500 million [24]. Moreover, the anonymity of the subscriber is not well protected. The procedure, wherein the MS registers its location with the system, is also vulnerable to interception and permits the subscriber's location to be monitored even when a call is not in progress.

Security was improved in the second (digital) generation (GSM in Europe). But both the authentication and encryption algorithms were broken [3], [4], [22], [28].

2000 Mathematics Subject Classification: 90B18, 94A60.
Keywords: mobile communications security, GSM, UMTS.

This research was supported by VEGA-grant 1/7611/20.

The third generation mobile system (UMTS) was designed mainly to assign the increasing need for fast wireless data communications. The standard GSM security features were redesigned to provide higher security, and some new, such as data integrity, were introduced.

The structure of this paper is as follows. Section 1 deals with basic GSM communication notions. Special factors influencing security in wireless communications are discussed in Section 2. GSM (resp. UMTS) security mechanisms are explained in Section 3 (resp. 4). Security of some other mobile systems is mentioned in Section 5. Finally, conclusions are to be found in Section 6.

1. Introduction into the GSM

In this section the GSM will be briefly described to provide necessary background for later discussion of the security features. Our description is based mainly on [27].

The Global System for Mobile communications (GSM) is a digital cellular communications system. Although it was developed in order to create a common European mobile telephone standard, it has been accepted worldwide. Its development started in 1982 by the Groupe Spécial Mobile, that was formed by the Conference of European Posts and Telecommunications (CEPT). The European Telecommunications Standards Institute (ETSI) is responsible for the GSM specifications since 1989.

Initial requirements on the new standard were: spectrum efficiency, international roaming, low mobile and base stations costs, good subjective voice quality, compatibility with other systems (e.g., Integrated Services Digital Network (ISDN)), and the ability to support new services.

The Phase I of the GSM specifications were published in 1990, and commercial usage of GSM dates since 1991.

In a cellular system, the covering area of an operator is divided into cells. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power. The idea of a cellular system is to use low power transmitters thus enabling efficient reuse of frequencies. The distance between cells using the same frequency must be sufficient to avoid interference.

A GSM network can be subdivided into the following main parts:

Mobile Stations (MS) consists of two main elements: a mobile equipment (ME), and a Subscriber Identity Module (SIM). Each ME can be uniquely identified through its International Mobile Equipment Identity (IMEI). SIM is a smart card that personalizes the terminal. It is protected by the Personal Identification Number (PIN), that can be 4–8 digits long. SIM holds important information, such as authentication key Ki (in a tamperproof manner), the International Mobile Subscriber Identity (IMSI), phonebook, etc.

Base Station Subsystem (BSS) connects the MS and the NSS. It deals with transmission and reception. Its main parts are: Base Transceiver Stations (BTS), and Base Station Controllers (BSC). Each BTS has between 1 and 16 transceivers, and is usually placed in the center of the cell. The BSC controls a group of BTSs, and manages their radio resources.

Network and Switching Subsystem (NSS) manages the communications between the mobile users and other users (mobile users, fixed telephony users, etc.). It includes databases needed to store information about the subscribers and to manage their mobility. Main NSS parts are:

Mobile services Switching Center (MSC) performs the switching functions of the network and provides connection to other networks.

Home Location Register (HLR) is a database that stores information about the subscribers belonging to the covering area of an MSC, it also stores the current location of these subscribers, and the services to which they have access.

Visitor Location Register (VLR) contains necessary information from a subscriber's HLR to provide the subscribed services to visiting users. When a subscriber enters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR is usually implemented together with an MSC.

Authentication Center (AuC) is used for security purposes. It provides the parameters needed for authentication and encryption functions, respectively.

Equipment Identity Register (EIR) contains a list of all valid terminals, thus allowing avoidance of calls from stolen or unauthorized terminals.

Operation and Support Subsystem (OSS) controls and monitors the GSM system.

To allow mobility of GSM subscribers, a location management need to be undertaken. When an MS is powered on, it performs a location update procedure by indicating its identity to the network. An MS also performs periodically location updating. The location updating message is sent to the (new) MSC/VLR which gives the location information to the subscriber's HLR. If, after the updating time period, the MS has not been registered, it is then deregistered. When the MS is powered off, it tells the network that it is no longer connected.

A movement of GSM user can produce the need to change the channel or cell, especially when the quality of communication is decreasing. MS controls continuously its own signal strength, and the signal strength of neighboring cells. When the quality of transmission decreases, the power level of the mobile is increased until it has no effect on the quality of the signal. Otherwise a *handover* is performed (channel or cell is changed).

A mix of Frequency Division Multiple Access (FDMA), and Time Division Multiple Access (TDMA), combined with frequency hoping has been adopted as the multiple access scheme for GSM. Using FDMA a frequency is assigned to a user. TDMA allows several users to share the same channel (each member of a set of users sharing a common channel is assigned his own burst within a group of bursts called a frame). A burst is the unit of time in a TDMA system, which lasts approximately 0.577 ms. A TDMA frame is formed with 8 bursts. Each of these eight bursts are assigned to a single user.

Two practical mechanisms reducing interference, and having an impact on communications security are:

- **frequency hoping**: frequency is changed with every TDMA frame (slow frequency hoping). It reduces the effects of co-channel interference and makes interception more difficult. BTS does not have to support it necessarily. On the other hand, an MS has to accept frequency hoping when BTS decides to use it.
- **discontinuous transmission** (DTX): since users speak less than 40 or 50 percent during the conversation, the MS is designed to detect the silence in communication and stops transmission for an appropriate time. DTX helps reduce interference, thus increasing the capacity of the system.

The main sources for GSM security are [10], [11], [12], and [13].

2. Security threats in mobile communications

Mobile communications have a number of special features that must be considered when dealing with security [8].

The most important one is the radio link. The radio link may be accessed (unnoticeably) by any entity. Thus the use of encryption is the only way of achieving confidentiality of communications on the radio link. Another one is roaming. In addition to their home networks/environments (HE) users may use different serving networks in various countries. This requires the transport of security parameters from HE to the relevant serving network. And finally some practical issues about mobile phones must be considered, like costs, the need to store authentication keys securely, encryption speed, power consumption of the additional encryption hardware, etc.

The following basic security threats can be identified in a mobile communications system:

- fraudulent calls and cloning,
- breach of user privacy (the compromise of a mobile station location, interception of the user (voice, data) traffic, interception of the signalling information, etc.),
- theft of mobile terminal/station.

GSM security mechanisms

GSM provides three basic security mechanisms:

- anonymity,
- authentication,
- confidentiality.

Anonymity

The subscriber is uniquely identified by its IMSI (stored in SIM–not protected). The use of Temporary Mobile Subscriber Identity (TMSI) assures the anonymity of users. It thus prevents location tracing of individual mobile users by intercepting the radio link traffic. All mobiles and networks must be capable of supporting this service, but its use is not mandatory.

When an MS is powered on for the first time, it indicates to the network the IMSI in plaintext. Prior to this no TMSI has been yet assigned to this MS. After successful authentication the network generates the temporary identity TMSI for the MS and sends it back encrypted to the MS under the key Kc (see the authentication procedure below). Late, when an MS is asked to show its identity, it does so by sending its TMSI. The network may generate a new TMSI for the MS.

However there are special situations when the network asks the MS to send its IMSI (e.g., when the TMSI sent by the MS to the network is unknown, or unrecognizable, possibly due to a database failure). Such an occasion gives the opportunity to an active attacker to masquerade as a BTS (the so called false base station attack) to instruct the MS to send its IMSI in the clear.

Authentication

Security of GSM is based on a secret 128-bit authentication key Ki (stored in SIM, and in AuC). If this key is compromised, an attacker can impersonate the legitimate subscriber.

Authentication is based on a simple challenge-response protocol. When an MS attempts to access the system, the network (VLR) sends a request to the user's

AuC to produce an authentication triplet. The AuC knows the authentication key Ki of the individual subscribers of the network the AuC belongs to, and contains implementations of algorithms A3 and A8. AuC generates a random 128-bit challenge RAND, computes the 32-bit expected response SRES=A3(Ki, RAND), the 64-bit cipher key Kc=A8(Ki, RAND), and sends back to the asking network the authentication triplet (RAND, SRES, Kc). In practice the AuC sends an array of authentication triplets. Each triplet is used for one authentication. The network (BTS) sends the MS only the obtained random challenge RAND. The SIM in the MS has a microprocessor and contains a software implementation of algorithms A3 and A8, as well as the AuC. The MS computes the response SRES'=A3(Ki, RAND) and the cipher key Kc=A8(Ki, RAND). The MS sends to BTS the value SRES' (encrypted under the key Kc, see the confidentiality below). If SRES=SRES', the MS is authenticated, otherwise access is denied. A schematic description of GSM authentication is shown in Figure 1.

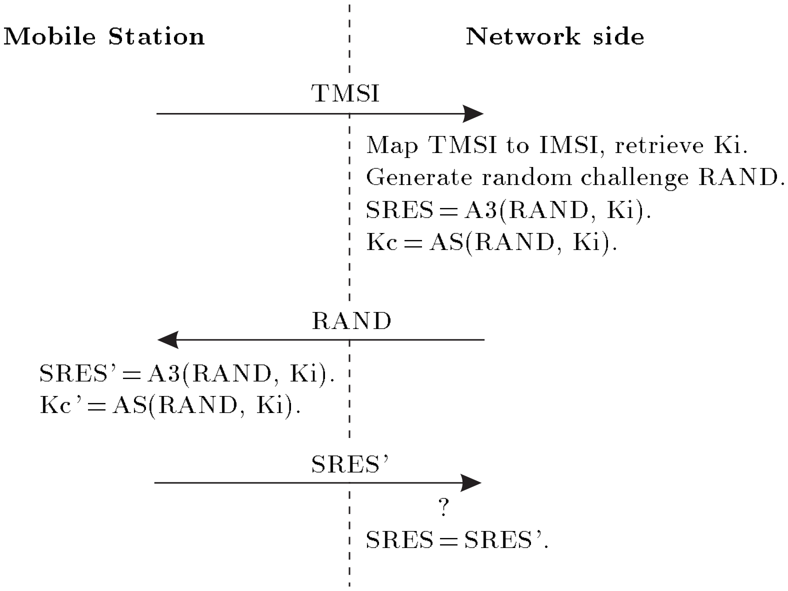

Figure 1. GSM authentication.

The key Ki is stored in the SIM securely so that it cannot be read out. The only operations allowed with Ki are algorithms A3, and A8.

Note that the individual subscriber authentication key Ki is never transmitted over the radio link.

The authentication mechanism in GSM solves elegantly the problem of authentication when roaming. The serving network (SN) does not need to know the authentication algorithm used by the user's home network/environment (HE). The SN asks the AuC in HE to generate the authentication triplet, then sends the obtained challenge RAND to the MS and performs the check of the MS response. It thus enables the use of different algorithms A3, A8 by different GSM networks/operators. The length of cipher key Kc is determined by the GSM encryption algorithm (see below).

However, the GSM authentication mechanism works only in one way, i.e., the user is authenticated by the network, but has no chance to authenticate the network. Thus he cannot be sure he is not communicating with an attacker masquerading as a base station.

In practice two algorithms A3 and A8 are combined into a single algorithm, called A38, which is used to compute simultaneously SRES and Kc from RAND and Ki.

COMP128 was chosen as the reference algorithm for the authentication pointed out by the GSM Consortium. It can be used by network administrations who do not want to develop their own A38 algorithms. The algorithm itself was kept secret, but later its implementation leaked out [6]. COMP128 generates both the SRES response and the session key Kc. The last 54 bits of the COMP128 output form the session key Kc. However the key Kc is 64-bit long. The remaining bits are filled with zeros, thus reducing the keyspace.

A chosen challenge attack against COMP128 algorithm was described by Goldberg and Wagner. The attack exploits low diffusion in the first two rounds of COMP128 compression function. The attack was practically realized. The SIM was accessed through a smart card reader connected to a PC. The PC made about 150000 challenges to the SIM and the SIM generated the corresponding SRES and Kc. The Ki could be deduced from the SRES responses through differential cryptanalysis. The attack required about 8 hours to conduct. Goldberg and Wagner are confident that the same attack can be launched over the air as well (using the false base station attack). The over the air attack is based on the fact that the MS is required to respond to every authentication challenge made by GSM network. Estimates of this attack vary from 8 to 13 hours.

Another security procedure relies on checking the equipment identity IMEI. If the IMEI of the mobile is authorized in EIR, the MS is allowed to connect the network. However IMEI is stored insecurely.

Confidentiality

Privacy of communications is achieved by means of an encryption algorithm A5. A5 is a synchronous binary additive stream cipher. The keystream is produced under the control of a cipher key Kc and then bitwise added modulo 2 to the data transferred on the radio link between MS and BTS.

A partial source code implementation of the GSM A5 algorithm was leaked in June, 1994. There are various versions of this encryption algorithm (A5/1–the stronger, used in the Western Europe, A5/2–the weaker version was approved for export to most other countries, including the Central and Eastern Europe). There is also the A5/0 algorithm that provides no encryption (in some countries the use of encrypted communication is illegal). The GSM standard defines 7 encryption algorithms, but there is no information about the remaining algorithms available.

Communication in GSM is transmitted in frames. The frame can be identified through its 22-bit TDMA frame number. For each frame a total of 114 bits are produced for encryption/decryption of data transferred from MS to BTS and an additional 114 bits are produced for decryption/encryption of data received at the MS from the BTS. Each frame lasts for 4.6 ms, so that the encryption algorithm has to produce the 228 bits long keystream in this time. Only the radio link between the MS and BTS is encrypted in the GSM network. Once the frames have been received by the BTS, it decrypts them and sends them in plaintext to the operator's backbone network.

The A5/1 is a stream cipher based on three linear feedback shift registers (LFSRs) R1, R2, and R3, 19-, 22-, and 23-bits long, all with associated primitive polynomials (R1: $1 + x^5 + x^{14} + x^{18} + x^{19}$, R2: $1 + x^{21} + x^{22}$, R3: $1 + x^8 + x^{21} + x^{22} + x^{23}$). The keystream bit is produced as the xor of the outputs of the individual registers. Registers R1, R2, and R3 are clocked in a "stop-and-go" fashion. Each of the registers has one bit (clocking bit) that has influence on clocking. C1 is the 8th bit of R1, C2 the 10th bit of R2, and C3 the 10th bit of R3. In each step the majority of C1, C2, and C3 is computed, and those registers that have their clocking bit equal to the computed majority are clocked. Thus in each step at least 2 registers are clocked.

The initial loading of the generator is composed from the cipher key Kc and the frame number. The detailed description of the key setup can be found in [4].

Because of speed considerations algorithm A5 is implemented in hardware, directly in ME.

An important fact is that the encryption is controlled by the network and can be switched off. The user does not know if it is on or off.

Here is a list of known attacks on the A5 stream cipher:

- An attacker masquerading as a base station (false base station attack) is able to send to the MS a command to switch the encryption off [2].
- It is possible to break A5/2 with complexity $O(2^{16})$ (D. Wagner, Crypto '99 rump session).
- A known-plaintext divide-and-conquer attack on A5/1 was presented in [1]. Guessing the loadings of registers R1, and R2, respectively, makes it possible to calculate the loading of R3. The average complexity is $O(2^{45})$ (due to the clocking dependence).
- Another known plaintext divide-and-conquer attack with average complexity $O(2^{40.16})$ was found by Golic, [22]. The idea of this attack is

to guess 10 bits in each register and to calculate the remaining bits by solving a system of equations.

The period of the A5 keystream generator is only slightly bigger than 2^{23} [22].

- A time-memory-tradeoff attack has also been presented in [22]. The initial loading of the generator can be found using 2^{22} random accesses into the table with 2^{42} 128-bit long words (64 terabytes). It is possible to decrease the length of the table to 862 GB, but consequently the number of table accesses increases to $O(2^{28})$.
- Another time-memory-tradeoff attack was presented in [4]. It takes only a few seconds to conduct the attack on a PC with 128 MB RAM and two 73 GB HDD analyzing the keystream used in two minutes of a GSM conversation. The idea of the attack is to choose a specific pattern, preprocess the initial loadings that generate the chosen pattern, and search the given keystream for the chosen pattern.
- Recently, in [3] there was presented an attack on A5/1 with total work complexity $O(2^{39.91})$ of A5/1 clockings, given $2^{20.8}$ known plaintext.

4. UMTS security mechanisms

The development of the third generation (3G) Universal Mobile Telecommunications System (UMTS) started in 1996. UMTS is targeted at providing globally available personalized and high quality mobile communication services, speech and service quality comparable to current fixed networks, service capability up to multimedia, separation of service provision and network operation, the capacity and capability to serve over 50 percent of the population, seamless and global radio coverage and radio bandwidth capabilities up to 2 Mbit/s. UMTS will support both interactive and distribution services. An important consideration is to make as much use of existing infrastructure as possible [5]. As teleservices and applications are not in general standardised, it is difficult to predict their exact nature [14].

UMTS will [17]

- build on the security of second generation systems,
- improve the security of second generation systems,
- offer new security features.

3G security will retain (and improve) the following security elements of 2G systems [17]:

- authentication of subscribers for service access,

- radio interface encryption,
- subscriber identity confidentiality on the radio interface,
- the SIM,
- SIM application toolkit features.

The trust of HE in SN for security functionality will be minimized

The following weaknesses were identified in 2G systems [17]:

- active attacks using a "false BTS" are possible [9],
- cipher keys and authentication data are transmitted in clear between and within networks,
- cleartext transmission of user and signalling data across microwave links (in GSM, from BTS to BSC),
- data integrity is not provided,
- there is no HE knowledge or control of how SN uses authentication parameters for HE subscribers roaming in that SN,
- 2G systems do not have the flexibility to upgrade and improve security functionality over time.

Mechanisms for lawful interception under authorization were included in 3G specifications from the start [14].

UMTS security is based on the use of a physically secure device called UMTS Integrated Circuit Card (UICC) that can be inserted and removed from the terminal equipment. UICC shall contain one or more applications at least one of which must be the User Services Identity Module (USIM). USIM is an application that represents and identifies a user and his association with a HE. The USIM contains functions and data needed to identify and authenticate users when 3G services are accessed (the most important is the authentication key Ki), and the user's International Mobile User Identity (IMUI). IMUI uniquely identifies a user, and is stored in USIM and in the home environment database, but need not be known to the user.

It is supposed that the terminal will be used as a platform for e-commerce and other applications. Multi application smartcards can be used with the terminal. It should be possible to download applications to UICC. This makes it theoretical possible to change the USIM itself if the UMTS authentication algorithm were broken.

A possible security problem is that 3G terminal equipment will support GSM phase 2 and phase 2+ SIMs as access modules to 3G networks (the decision on the acceptance of GSM SIMs is left to network operators).

The following threats were evaluated to be of major or medium level (a complete list of threats can be found in [17]):

- MAJOR: eavesdropping user traffic,

- MEDIUM: eavesdropping signalling or control data,
- MAJOR: masquerading as a communication participant,
- MAJOR: passive traffic analysis,
- MEDIUM: masquerading as another user,
- MAJOR: masquerading as a user,
- MAJOR: use of a stolen terminal and UICC,
- MAJOR: use of a stolen terminal,
- MAJOR: manipulation of the identity of terminal,
- MAJOR: confidentiality of authentication data in UICC/USIM.

UMTS introduces the integrity protection of signalling messages, uses stronger encryption than was used in GSM, and finally the new authentication and key agreement mechanism provides mutual authentication.

The security functions were designed with a view to their continuous use for a period of at least 20 years. Responsibility for designing the algorithms was delegated to ETSI SAGE (Security Algorithms Group of Experts).

Authentication

The method is composed of a challenge-response protocol identical to GSM subscriber authentication and key establishment protocol, combined with a sequence number-based one-pass protocol for network authentication. This protocol was derived from the standard ISO/IEC 9798–4 [5]. As in GSM, the operators can have their own (secret) authentication and key agreement protocols.

AuC on a request generates an array of quintets (equivalent of the GSM triplet) as follows [16]:

- generates a fresh sequence number SQN from a counter SQNHE,
- generates an unpredictable challenge RAND = f0(),
- computes a message authentication code for authentication MAC-A = f1(Ki, SQN $\|$ RAND $\|$ AMF), where AMF is the authentication management field,
- computes an expected response XRES = f2(Ki, RAND),
- computes a cipher key CK = f3(Ki, RAND),
- computes an integrity key IK = f4(Ki, RAND),
- computes an anonymity key AK = f5(Ki, RAND), and computes the concealed sequence number SQN $\oplus$ AK, if SQN is to be concealed,
- assembles the authentication token AUTN = SQN [$\oplus$ AK] $\|$ AMF $\|$ MAC-A, the quintet Q = (RAND, XRES, CK, IK, AUTN), and updates the counter SQNHE.

Each quintet can be used for one authentication and key agreement between VLR and ME/USIM. The requirements on the previously mentioned functions f0–f9 can be found in [16]. Functions f1–f5, f1* and f5* should be designed so that it is possible to implement them on an integrated circuit (IC) with an 8-bit 3.25 MHz microprocessor, 8KB ROM, and 300B RAM. Time to calculate AK, XMAC-A, RES, CK, IK should not exceed 500 ms.

The user, resp. MS is sent the parameters RAND and AUTN.

The processing upon receipt of RAND and AUTN in USIM is as follows:

- If the sequence number is to be concealed, USIM computes the anonymity key AK = f5(Ki, RAND) and retrieves from AUTN the unconcealed sequence number SQN = (SQN $\oplus$ AK) $\oplus$ AK.
- USIM computes XMAC-A = f1(Ki, SQN $\|$ RAND $\|$ AMF) and compares XMAC-A with MAC-A. If they are different a user authentication response with indication of integrity failure is sent to the network and the procedure is abandoned.
- USIM verifies, if the received sequence number SQN is acceptable (for details see [15]).
- If the SQN is acceptable the procedure proceeds further, otherwise a user authentication response with an indication of synchronization failure, including the resynchronization token is sent back, and the procedure is abandoned.
- USIM computes cipher key CK = f3(Ki, RAND) and integrity key IK = f4(Ki, RAND).
- USIM computes the response RES = f2(Ki, RAND) and sends back to network a user authentication response with indication of successful receipt of the signed challenge and including the response RES.

Upon receipt of RES the network checks whether RES = XRES. If equality holds, the user is allowed to use the network and its services, otherwise access is denied.

The formal analysis of the described AKA mechanism can be found in [18].

Possible adaption of an asymmetric technique was considered but its usage was refused. The main problem was the reusage of the existing infrastructure and the uncertainty about the ability of USIM to provide an asymmetric protocol efficiently.

Integrity protection

The main reason for introducing integrity protection is to prevent the connection hijacking. GSM has no integrity protection. The Message Authentication Function f9 is used to authenticate data integrity and data origin of signalling data transmitted between Radio Network Controller (RNC) and Mobile Equipment (ME) [2], [16], [19]. It computes a 32-bit MAC which is appended to the frame being transmitted, and is checked by the receiver to verify that the frame originated from the correct party, and has not been modified during transmission. f9 is a variant of the standard CBC-MAC construction [20] and is based on the KASUMI algorithm [21].

The best known attack is one that requires 2^{48} chosen messages (L. Knudsen and Ch. Mitchell [23]).

Confidentiality

The function f8 is used to protect confidentiality of user data and the signalling data sent over the radio link. It is a symmetric synchronous stream cipher. The f8 algorithm will be used to encrypt frames of variable length up to approximately 5000 bits [2], [16], [19], [20]. Encryption is done as the bitwise XOR of the plaintext and the produced keystream.

UMTS encryption function should meet the following hardware requirements: one instance of the algorithm should be possible to be implemented using less than 10000 gates, the encryption speed must be 2 Mbit/s in each direction.

The encryption function f8 is built on the basis of the KASUMI cipher in a variant of the standard Output Feedback Mode (OFB), with a 64-bit feedback.

KASUMI cipher

Due to a short time left for the design of the cryptographic algorithms (6 months) the ETSI SAGE (led by G. Roelofsen) took the approach to use an existing cryptographic algorithm as a starting point, and modify it to meet the requirements (hardware, encryption speed, etc.). There was also a strong argument to design the f8 and f9 algorithms with a common core, to save on implementation costs [2]. M. Matsui as well as the external experts from Nokia, Ericsson, and Motorola led by K. Nyberg contributed to the design of algorithms.

The algorithm MISTY1 (Mitsubishi Electrical Corporation), developed by M. Matsui, was taken as the starting point. MISTY1 is an 8-round block cipher operating on 64-bit blocks with a 128-bit key. The design of MISTY1 is based on the provable resistance against linear and differential cryptanalysis, and is suitable for implementation in hardware or software. MISTY1 is one of the selected algorithms for the second phase evaluation in project NESSIE (`http://www.cryptonessie.org`).

The only cryptanalytic results on MISTY1 are the attacks against modified (simplified) versions of MISTY1. No attack faster than exhaustive key search has been found against the full MISTY1.

The modified version of MISTY1 was designed and named KASUMI. Changes were done to strengthen aspects of the algorithm without increasing its complexity, and to simplify implementation without decreasing security [2].

The algorithms were analysed by three independent external teams: KU Leuven (L. Knudsen, B. Preneel, V. Rijmen, J. Borst, M. Robshaw), Ecole Normale Superiere (J. Stern, S. Vaudenay), and Royal Holloway (F. Piper, S. Murphy, P. Wild, S. Blackburn).

The short summary of the cryptanalytic results [2]:

- no weak keys were found,
- found chosen plaintext/related key attacks against KASUMI reduced to five rounds, with the possibility to extend it to 6 rounds,
- statistical evaluation does not exploit any deviation from random behaviour,
- no properties of KASUMI were found that would make it vulnerable against timing attacks, simple power and differential power analysis attacks,
- no practical attacks against the f8 and f9 constructions were found,
- the attacks found do not practically threaten the security of the KASUMI cipher,
- The KASUMI cipher meets the requirements on the encryption speed.

5. Other mobile communications systems

GSM is of course not the only one digital wireless communication system. Among other systems we can list: Personal Digital Cellular (PDC), Japanese Digital Cellular (JDC), Personal Communications Systems (PCS), etc.

IS-41 is the US standard for the North America 2G wireless communication systems [8]. It uses the following cryptographic algorithms:

- Cellular Authentication and Voice Encryption (CAVE)—primarily a challenge response algorithm, but is also used for further key generation. It is an unkeyed hash function. In 18-bit output mode applications the collisions can be generated using randomly generated inputs, and in 128-bit output mode a reconstruction attack is possible [8].
- Cellular Message Encryption Algorithm (CMEA) is used to encrypt the control information. It is a byte oriented variable width block cipher with a 64-bit key. There are two attacks on CMEA presented in [30]. One is a known plaintext attack of the complexity $O(2^{24})$–$O(2^{32})$, with 40–80 known plaintexts required. Another is a chosen plaintext attack. It requires 338 chosen plaintexts, and a small amount of computation.

- ORYX is used for data services encryption. It is a synchronous stream cipher based on LFSRs with a 96-bit key. A known plaintext attack of complexity $O(2^{16})$ is presented in [29]. The attack uses a guess and check approach and requires 25–27 bytes of keystream.
- Voice privacy is achieved via a limited size XOR masking operation. Different methods are used in TDMA and CDMA (Code Division Multiple Access) systems. (See [8] for their cryptanalysis.)

The General Packet Radio Service (GPRS) is the mobile communication system built over GSM. In addition it uses two new nodes, namely Serving GPRS Support Node (SGSN), and Gateway GPRS Support Node (GGSN). The existing radio system is virtually unchanged [5]. GPRS is used to implement high speed data transmission between the MS and some other party [25]. The GPRS data rate is in theory 170 kbit/s (the GSM data rates were 9.6 kbit/s or 14.4 kbit/s). In GPRS the encrypted frames are transmitted from the MS to the SGSN. This is done because the GPRS uses multiple time slots in parallel in order to achieve a greater transmission rate. To BTS the use of one time slot is seen as a separate call. Thus BTS is unable to put frames from one MS together. The frames are decrypted at SGSN (i.e., deeper in the inner network than it was in GSM). The encryption algorithm used in GPRS is GEA. Its strength is roughly equivalent to the A5 used in GSM [26].

Another system used in mobile communications is WAP. WAP devices include their own security protocol, Wireless Transport Layer Security (WTLS), based on a less-resource-intensive encryption algorithms, such as elliptic curve cryptography. WAP phones do not have the CPU power and memory necessary for RSA encryption, a key element of SSL [7].

There are of course many more mobile communication systems, whose security could be discussed (e.g., Bluetooth, which is the standard for a short-range (10–100 meters) radio link, intended to replace cable to printers, and other peripherals, etc.).

6. Conclusions

A comprehensive overview of GSM and UMTS security mechanisms was presented in this paper. The GSM authentication and encryption algorithms were described and their current security status was presented. The new security features of UMTS were presented, as well as the main results of their security analysis. It is a question raised in the mobile communication market whether UMTS will be used in practice. If so, this will naturally result in increased interest in the cryptanalysis of the UMTS security mechanisms.

Acknowledgement. The author would like to thank to Professor Otokar G r o š e k for many helpful discussion and his continuous support during preparation of this paper.

REFERENCES

[1] ANDERSON, R.—ROE, M.: A5, `http://jya.com/crack-a5.htm` (1994).

[2] BABBAGE, S.: Design of Security Algorithms for Third Generation Mobile Telephony, Information Security Technical Report, Vol. 5, No. 3 (2000), pp. 66–73.

[3] BIHAM, E.—DUNKELMAN, O.: Cryptanalysis of the A5/1 GSM Stream Cipher, Proceedings of INDOCRYPT 2000, pp. 43–51.

[4] BIRYUKOV, A.—SHAMIR, A.—WAGNER, D.: Real Time Cryptanalysis of A5/1 on a PC, presented at the Fast Encryption Software Workshop 2000 in New York City on April 10, 2000.

[5] BLANCHARD, C.: Security for the Third Generation (3G) Mobile System, Information Security Technical Report, Vol. 5, No. 3 (2000), pp. 55–65.

[6] BRICENO, M.—GOLDBERG, I.—WAGNER, D.: An implementation of the GSM A3A8 algorithm. (Specifically, COMP128), 1998, `http://www.iol.ie/~kooltek/a3a8.txt`.

[7] HANCOCK, B.: The Wireless Great Divide–But Getting Smaller, Computers & Security, Vol. 20, No. 1, pp. 15–17.

[8] DAWSON, E.—BOYD, C.—MILLAN, W.: Cryptographic Algorithms for Mobile Communications, in: Proceedings of the Dalian–Hong Kong International Computer Conference 1998, pp. 8–18.

[9] ETSI: Countermeasures to active attacks on the radio access link, ETSI SMG10 99C019.

[10] ETSI: Security Aspects, GSM 02.09.

[11] ETSI: Subscriber Identity Modules, GSM 02.17.

[12] ETSI: Security Related Network Functions, GSM 03.20.

[13] ETSI: Security Related Algorithms, GSM 03.21.

[14] ETSI: Security Threats and Requirements, ETSI TS 121 133 v3.1.0.

[15] ETSI: Security Architecture, ETSI TS 133 102 v3.3.1.

[16] ETSI: Cryptographic Algorithm Requirements, ETSI TS 133 105 v3.6.0.

[17] ETSI: Security Principles and Objectives, ETSI TS 133 120 v3.0.0.

[18] ETSI: Formal Analysis of the 3G Authentication Protocol, ETSI TS 133 902 v4.0.0.

[19] ETSI: General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms, TR 133 908 v4.0.0.

[20] ETSI: Specification of the 3GPP confidentiality and integrity algorithms, TS 135 201 v4.1.0.

[21] ETSI: KASUMI algorithm specification, TS 135 202 v4.0.0.

[22] GOLIC, J.: *Cryptanalysis of Alleged A5 Stream Cipher*, Proceedings of Eurocrypt '97, LNCS, Vol. 1233, pp. 239–255.

[23] KNUDSEN, L. R.—MITCHELL, C. J.: *An analysis of the 3GPP*-MAC *scheme*, in: Proceedings of WCC 2001, (D. Augot and C. Carlet, eds.), Paris, France, 8-12 January 2001, pp. 319–328. Also published in Electronic Notes in Discrete Mathematics 6 (April 2001).

[24] MARGRAVE, D.: GSM Security and Encryption, `http://spyhard.narod.ru/phreak/gsm-secur.html`.

[25] PESONEN, L.: GSM Interception, http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-9900/a5/Netsec/netsec.html.

[26] RAUTPALO, J.: GPRS Security–Secure Remote Connections over GPRS.

[27] SEMPERE, J. G.: An Overview of the GSM system, http://www.comms.eee.strath.ac.uk/~gozalvez/gsm/gsm.html.

[28] WAGNER, D.: GSM Cloning, http://www.isaac.cs.berkeley.edu/isaac/gsm.html.

[29] WAGNER, D.—SIMPSON, L.—DAWSON, E.—KELSEY, J.—MILLAN, W.—SCHNEIER, B.: *Cryptanalysis of* ORYX, Proceedings of SAC '98, Springer Verlag, pp. 296–305.

[30] WAGNER, D.—SCHNEIER, B.—KELSEY, J.: Cryptanalysis of the Cellular Message Encryption Algorithm, Proceedings of CRYPTO '97, LNCS Vol. 1294, Springer Verlag 1997, pp. 526-537.

Received April 2, 2002

Department of Mathematics
Faculty of Electrical Engineering
and Information Technology
Slovak University of Technology
Ilkovičova 3
SK–812 19 Bratislava
SLOVAKIA
E-mail: vojvoda@kmat.elf.stuba.sk