European Congress on Computational Methods in Applied Sciences and Engineering
ECCOMAS 2004
P. Neittaanmäki, T. Rossi, S. Korotov, E. Oñate, J. Périaux, and D. Knörzer (eds.)
Jyväskylä, 24–28 July 2004

CRYPTOGRAPHIC ALGORITHMS FOR UMTS

Kaisa Nyberg

Nokia Research Center
P.O. Box 407, FIN-00045 Nokia Group, Finland
e-mail: Kaisa.Nyberg@nokia.com

Key words: cellular security, GSM, UMTS, modes of operation, stream cipher, block cipher, message authentication code, f8, f9, KASUMI, MILENAGE

Abstract. *The cryptographic algorithms of GSM have received a lot of interest and activity from the cryptographic research community and some potential points of failure have been identified. These include secret designs of cryptographic algorithms and weak integrity protection over the air interface. The objective of this talk is to discuss the design strategies for the cryptographic algorithms in the third generation cellular networks. In particular, we consider how the problems found in GSM were addressed in the design of the 3GPP specifications for the Universal Mobile Telecommunications System (UMTS) networks. We also present an overview of the results achieved by researchers within the cryptographic community. In addition to the topics of the talk this paper gives also an introduction to the main concepts of the UMTS security architecture. The presentation of the paper is to large extent based on [25], where a more comprehensive treatment of this subject can be found.*

1 INTRODUCTION

The Global System for Mobile Communications (GSM) is the largest second generation mobile system. Its security system formed the starting point of the development of security features for subsequent generations. The fundamental goal of the standard GSM security features was to ensure correct billing of the phone calls. Previous incidents from the analog mobile phone systems had shown how easy it is to impersonate a legitimate subscriber if no secure authentication mechanism is applied. Subscriber authentication in GSM is based on a secret key stored in the SIM card that is placed inside the mobile phone. A cryptographic algorithm is used to protect authentication of the subscriber. Another cryptographic algorithm is used to protect the phone call over the air interface so that the communication resources are used only for transmitting calls to and from the subscriber that was identified at the beginning of the call. The GSM security system has performed quite well in fulfilling this fundamental requirement of correct billing. The losses due to SIM cloning are negligible compared with the losses due to credit card fraud, for example, where about one third of all losses are due to counterfeit cards. GSM subscribers still trust the billing information of the basic voice and data services given in their phone bills. However, even if performing quite well in practice, GSM security system is far from being perfect. Since designed to ensure secure billing, the architecture is too simple to satisfy the growing needs of various services that are being developed on top of GSM. Also as technology advances, the attacks that were not present and could not be foreseen as realistic at the time of development are gradually becoming a reality. Such attacks include advanced cryptanalytic tools, efficient false base stations, real-time computer analysis, etc.

Although the GSM security architecture has many weak points, it has one excellent feature: it is almost invisible to the user. If the security relies on some user action, it is almost certain that at least one of the users will cause a security failure. Human errors cannot be avoided. In GSM, after the user has activated the phone and the SIM, no security related action is required from the user other than the intuitive one, keeping good hold of your phone. The same basic architecture was adopted for the third generation cellular systems. In addition, several enhancements and changes were made to it in order to meet the growing telecommunication system's new needs to secure not only voice communication, but also a growing variety of other services.

The cryptographic algorithms of GSM have received a lot of interest and activity from the cryptographic research community and many points of failure were identified. These include secret designs of cryptographic algorithms and weak integrity protection over the air interface. The objective of this talk is to discuss the design strategies for the cryptographic algorithms in the third generation cellular networks. In particular, we take a look how well these algorithms have resisted the public cryptanalytic efforts during the first five four of their existence.

In this paper we present an extended version of the talk by including some background information about the general security architecture of the GSM and UMTS systems. The

presentation is based on [25], where a more comprehensive treatment of this subject can be found. Some recent updates have been added. The rest of the paper is organised as follows. In Section 2 we give an overviev of the GSM security system. In Section 3 the main features of the UMTS security architecture is presented. The security of the 3GPP authentication and key agreement algorithms is discussed in Section 4. The encryption algorithm f8 and its kernel block cipher KASUMI are discussed in Section 5 and the integrity algorithm f9 in Section 6.

2 GSM SECURITY

2.1 The GSM system

In the beginning of 1990s, the second-generation mobile systems were introduced. The most successful of them has been GSM, which had more than 800 million users worldwide in the beginning of the year 2003. In the United States, the leading second generation technology has been the TDMA, and in Japan, the PDC system. The most important new feature in the second generation was the introduction of digital information transmission in the radio interface between the mobile phone and the base station. In all of the afore-mentioned systems, the multiple access technology is TDMA. The most immediate advantages of the second generation over its predecessor were increased capacity of the network (due to more effective use of radio resources), better speech quality (due to digital coding techniques) and the possibility for communicating data much more easily. Also, it was now possible to enhance security of the system significantly.

2.2 Security goals

The goal of the security design for GSM system was clear: the security has to be as good as that of wireline systems. On the other hand, mechanisms introduced were not allowed to reduce the usability of the system. The most important security features in the GSM system are:

- authentication of the user,
- encryption of communication in radio interface, and
- protecting user privacy by using temporary identities.

The success of GSM also emphasised finally the limitations of its security. A popular technology becomes a very tempting target for attackers. The properties of GSM that have been most criticised on the security front are the following:

- active attacks towards the network are possible (in principle),
- sensitive control data such as authentication triplets containing keys used for radio interface ciphering, are sent between different networks without protection, and

- some essential parts of the security architecture are kept secret. This does not create trust on them in the long run because they are not available for analysis by novel methods. Also global secrets tend to be revealed eventually.

2.3 Authentication of the subscriber in GSM

There exists a permanent secret key K_i for each user. This key is stored in two locations:

- in the users Subscriber Identity Module (SIM) card, and
- in the Authentication Centre (AuC).

The key K_i never leaves either of these two locations. The user is authenticated based on this secret in user's mobile equipment. The authentication is a standard challenge-response mechanism based on a one-way function [13]. The network sends to the mobile a challenge, which typically contains a randomly generated value, but may also be based on a sequence number or time-stamp. The main requirement is that the challenge is fresh, non-repeating and unpredictable. When the mobile equipment receives the challenge, it gives it to the SIM module, which computes a response as an output from the one-way function under the control of the secret key K_i. The response is sent to the network. The network has computed its own copy of the response, also called as the expected response. When the network receives mobile's response it compares it with the expected response. If these two values are equal, the mobile has been correctly authenticated.

Unfortunately, this authentication paradigm has a fundamental flaw. Assume that an active attacker has access to some network node that is situated in the middle of the communication channel between the mobile and the network. Simply by relaying the challenges and responses, the attacker can pretend to be the end of the communication channel, where the mobile is expecting the correct base station to be. The problem is well understood, at least in this basic scenario. One common solution to handle this problem is that, in addition to the response values, the mobile and the network also compute a cryptographic key value that is used to protect the subsequent communication. The man-in-the-middle is still able to copy and send forward anything sent by the network, but it is not able to decrypt or modify the communication, or make its own phone calls on the expense of the other user.

The challenge is a random 128-bit string $RAND$ and is sent to the mobile phone. The phone transfers the parameter to the SIM card that is inside the phone. The SIM also contains an algorithm, denoted by A3, that takes two inputs: K_i and $RAND$. The output is a 32-bit response value $SRES$ that is sent back to the network where the correctness of the response is checked.

A temporary session key K_c (ciphering key) is generated as an output of another one-way function A8 which takes the same input parameters K_i and $RAND$. This key is used to encrypt phone calls on the radio interface. The serving network has no knowledge of the subscriber's secret key K_i and, therefore, it cannot handle all of the security alone.

Therefore the other relevant parameters ($RAND$, $SRES$, K_c) are sent by the home network to the serving network in a package called as the authentication triplet.

The A3 and A8 algorithms are usually implemented combined in one single A3/A8 algorithm and they are operator specific. This means that every operator can select its own algorithm. A famous example of a poor A3/A8 algorithm is COMP128. This algorithm was provided by the GSM association, the GSM operators' organization, and was broken soon after its details were recovered [7]. The weakness in COMP128 allows a holder of the SIM card to extract the master key K_i from the card and clone the SIM [21]. Many other A3/A8 algorithms are in use. Some of them are publicly available such as the GSM MILENAGE algorithm, which is derived from the 3GPP MILENAGE algorithm using standard GSM-to-UMTS conversion rules.

2.4 GSM ciphering

During the authentication a secret session key K_c is established. With this key all calls are encrypted between the phone and the base station until the next authentication occurs. The encryption algorithm is called A5 and it is a stream cipher. Currently three different A5 algorithms have been standardized. They are called A5/1, A5/2 and A5/3. The specifications of the first two are still confidential and managed by GSM Association [12], which delivers them under specific license to vendors that produce GSM equipment. The third algorithm is new. It is based on the UMTS ciphering algorithm f8, and is publicly available on the GSM Associations web site. In General Packet Radio Service (GPRS) the radio interface ciphering by the algorithm A5 is replaced by another stream cipher, called GEA (GPRS Encryption Algorithm).

The goal of GSM ciphering is two-fold: to protect the call from being eavesdropped between the mobile phone and the base station, on the one hand, and to prevent the call service from being used by a non-paying subscriber. The public discussion has focused almost only on the first goal, the effect of ciphering algorithm to call confidentiality. However, the second goal is more fundamental to the correct performance for the GSM system. It is well known in cryptography that a stream cipher is not the right mechanism to ensure communication integrity. But in GSM the integrity of the radio channel is protected only using encryption with a stream cipher. Moreover, since GSM does not have a standardized interface for law enforcement, national security authorities set restrictions to the strength of encryption. This has also deteriorating impact to achieving the second goal of call integrity.

Ciphering is switched on or off by the base station, which also selects the algorithm in use. Since only ciphering is used to protect the integrity of the communication over the air interface, and some of the ciphering algorithms are weak, it was recently shown in [5] that a well-equipped man-in-the-middle can possibly hi-jack a GSM call. Fortunately, the cost of the equipment and resources that a man-in-the-middle would need to perform such an attack in practise is still prohibitive. Therfore it is still quite hard to exploit this attack and run profitable business by selling stolen phone calls.

This flaw in the GSM security architecture has been corrected in the third generation cellular networks by implementing separate algorithms for integrity and confidentiality over the radio path and by implementing mutual authentication.

2.5 User identity confidentiality

The permanent identity of the user, International Mobile Subscriber Identity (IMSI), is protected in GSM against eavesdroppers by restricting the number of occasions where it has to be used. Instead of IMSI, a Temporary Mobile Subscriber Identity (TMSI) is used for identification of the user. The identity TMSI is changed every time it has been used and the new TMSI is always transmitted to the user over the encrypted channel. Similar mechanism is used also in UMTS.

3 UMTS SECURITY

3.1 The 3GPP

At the same time when second-generation systems were launched, it became clear that there is also a next step to be taken at some point. The work to design third generation system was initiated in organizations like European Posts and Telecommunications Conference (CEPT) and UMTS Forum, and later European Telecommunications Institute (ETSI) began to develop the work further. One of the leading ideas for 3G was to ensure fully global roaming: to make it possible for the user to use the mobile system services all over the world. In the global International Telecommunication Union (ITU), this goal was stated for the IMT-2000 standard.

The success of GSM had a two-fold effect on the development of the new generation system. From the positive side, success of mobile communication technologies made it easier to find resources for subsequent research and development. The other side of the coin was the fact that there seemed to be no immediate need for a new system since GSM had proven to be such an effective system. Thus, for several years development of UMTS was done on theoretical basis only. On the security side, lots of effort was put on, e.g., development of new authentication mechanisms. Most of the state-of-the-art cryptographic techniques were proposed for UMTS security. However, many proposals and options remained open.

In the year 1998, five standards organizations decided to combine their efforts to accelerate the work and guarantee the global interoperability. The organizations, ETSI from Europe, ARIB and TTC from Japan, Standards Committee on Telecommunications (T1) of American National Institute of Standards (ANSI) from North America, and Telecommunications Technology Association (TTA) from South Korea formed the 3rd Generation Partnership Project (3GPP). Soon afterwards, a sixth partner from China joined the project. The current Chinese partner in 3GPP is China Communications Standards Association (CCSA). All 3GPP specifications are available at [1].

While the radio access technology is changed from TDMA to WCDMA when the 3rd

generation mobile networks are introduced, the requirements for access security remain unchanged; access authentication, air interface confidentiality and user privacy must be provided. In addition, availability and reliability of the UMTS service is clearly important for a subscriber who is paying for it. Therefore all radio network signalling is integrity protected; it is checked that all control messages have been created by authorised elements of the network.

At the time when the GSM security architecture was designed, the threat imposed by the known weaknesses was estimated inferior in comparison with the added cost of trying to circumvent them. However, as the technology advances, also the attackers have access to better tools. That is why the outcome of a similar comparison between cost and security led to a different conclusion in the case of the third generation mobile networks.

In most countries, legislation and regulations set the requirement that authorities must have a way to access sensitive information, for example, to use it as evidence in court cases. In GSM, the lawful interception functionality was added afterwards to an existing complete system. Since it is clearly more effective to use standardized mechanisms for lawful interception, these features have been standardized as an integral part of the UMTS system.

3.2 Mutual authentication in UMTS

The three entities involved in the authentication mechanism of the UMTS system are:

- Home environment and Authentication Center (AuC),
- Serving network with Visitor Location Register (VLR), and
- Terminal, more specifically USIM (typically in a smart card).

Similarly as in GSM the serving network checks subscriber's identity by a challenge-response technique while the terminal checks that the serving network has been authorised by the heme environment to do so. The latter part is a new feature in UMTS compared to GSM and through it the terminal can check that it is connected to a legitimate network.

The AuC has a copy of the subscriber's master key K. By request from the serving network AuC derives authentication vectors of five components $RAND$, $XRES$, CK, IK, and $AUTN$ of which the latter four are computed from the $RAND$, K and a sequence number SQN. In the serving network, one authentication vector is needed for each authentication instance. The serving network sends a user authentication request to the mobile terminal. This message contains two parameters from the authentication vector, $RAND$ and $AUTN$. These parameters are transferred into the USIM module that resides inside a tamper-resistant environment called as Universal Integrated Circuit Card (UICC). The USIM contains the master key K, and using it with the parameters $RAND$ and $AUTN$ as other input values, USIM carries out the computations using the Authentication and Key Agreement (AKA) algorithms. The result of the computation

gives USIM the ability to verify whether the parameter $AUTN$ was indeed generated in AuC, and was not sent before to USIM. This verification is essentially based on the value of SQN. For this purpose, two counters are maintained synchronised in the AuC and in the USIM. If the USIM accepts the verification, the computed response parameter RES is sent back to the serving network in the user authentication response message. The serving network compares RES with the expected response $XRES$, which it received included in the authentication vector. In the case of match, authentication ends positively.

3.3 Cryptographic algorithms for UMTS

In summer 1999, the 3GPP was facing the task to define and agree on the design process for the encryption and integrity algorithms. Previous examples of design processes of cryptographic algorithms intended for use in public systems existed, but there was no standard strategy for performing such a task. The first such effort was the design of the public Data Encryption Standard (DES) by NIST in 1977. In the area of telecommunication, public cryptographic solutions were designed for the Wireless Local Area Network (WLAN) standard IEEE 802.11 (published in 1997) and Bluetooth (published in 1999).

In 1999 NIST had just started the AES project for finding a replacement for DES. The results of the NIST project would not be available until 2001. As a 128-bit block cipher, the AES would probably also be too large to fit within the 10 000 gates of hardware that had been specified as the maximum size for the handset implementations.

Facing the task of selecting confidentiality and integrity algorithms for UMTS, 3GPP made an assessment of different options it had for performing this task. Following three specification strategies were identified:

1. Select an off-the-shelf algorithm.
2. Invite submissions.
3. Commission a special group to design an algorithm.

It was clear that different strategies have different implications to suitability, security, and timely delivery of the algorithm. On the other hand, feasibility of each strategy is based on different assumptions about availability of resources such as expert knowledge and time.

Whichever of the three specification strategies is selected, it was understood that a separate strategy must be defined for the security evaluation of the specified algorithm before it is adopted for use. The evaluation can either rely on voluntary efforts or special groups of experts could be commissioned. For open designs, the voluntary efforts will become available as soon as the algorithm is published. During the 1990s, the formerly secret art of cryptanalysis had developed into an open science, and the researchers were continuously looking for suitable objects for study. On the other hand, it should not happen that the algorithms get broken immediately after publication. Since only limited time was available, it was not sufficient to rely on voluntary efforts.

3GPP also decided to publish the methods and results of the analysis performed by the design team and the independent evaluators [2, 3] prior to publication. Descriptions of the algorithms can also be found in these reports, as well as references to the specification documents.

4 3GPP AKA ALGORITHMS

4.1 MILENAGE

In total, five one-way functions are used to compute the authentication vector. These functions are denoted by f1, f2, f3, f4 and f5, and their choice is in principle operator-specific. This is because they are used only in the AuC and in the USIM and the same home operator controls both of them. However, to achieve interoperability of different USIM implementations with the AuC version of the algorithm may require substantial effort, and would be easier if a standard algorithm is used. Also the design and implementation of a strong cryptographic algorithm is never a trivial task, and may not be an option available to all operators. Therefore 3GPP provided an example set of AKA algorithms that could be used by operators that do not wish to provide one of their own.

This set of AKA algorithms is commonly denoted as MILENAGE. The name of the 3GPP authentication algorithm is of French origin and is instructed in the specifications to be pronounced as a French word - something like "mi-le-nahj". The construction makes use of a strong 128-bit encryption algorithm as a kernel function and it includes an additional configuration field parameter selected by the operator. The example design recommends the use of the AES [27] as the kernel function, but an operator could change this to any block cipher that meets the requirements for interface parameters.

4.2 The kernel algorithm

The main cryptographic strength of MILENAGE is due to its kernel block cipher. The chosen kernel algorithm AES has undergone extensive cryptanalysis by many different teams [27, 28]. Due to its status as a standard, its secure implementation and protection against side-channel attacks has also received much more attention than algorithms in average. After Courtois and Pieprzyk published their analysis on AES [9], critical opinions about its security increased, and many people believed that its lifetime as a standard may be shorter than originally intended. The attack of Courtois and Pieprzyk makes use of systems over overdefined algebraic equations, which the Rijndael block cipher was not designed to handle. Subsequently, another alarming finding was due to Murphy and Robshaw, who were able to describe the entire relationship of the Rijndael plaintext, key and ciphertext by means of a sparse system of equations that involve at most quadratic (degree 1 or 2) polynomials [23]. Opinion is divided as to the efficiency of these attacks, but some people estimate that the complexity of breaking the AES block cipher could be as low as about 2^{100} operations. But it is generally agreed that the discovered vulnerabilities do not pose any practical threat. They only mean that the theoretical security of the

kernel of MILENAGE is somewhat reduced from the assumed strength of a 128-bit block cipher.

4.3 The modes

The most distinctive features of the MILENAGE can be captured in the following simplified functional model

$$z_i = E_K(E_K(x) \oplus a_i), \text{ where } i = 1, 2, \ldots, t. \tag{1}$$

The parameter t is fixed and it denotes the number of distinct output blocks of size n from the kernel block cipher algorithm E_K. The values a_1, a_2,...,a_t are assumed to be any t fixed known distinct offset constants. For the MILENAGE construction of functions f2 to f5*, we have $t = 4$.

The goal of the security proof for such a construction is to show that there is no way to use any combination of significantly less than $2^{n/2}$ output values z_1, z_2,...,z_t to predict any new output value for any of the blocks z_i. More generally, it should be shown that if E_K behaves like a random permutation of the set $\{0,1\}^n$, then the function f, which maps x to the t-tuple z_1,z_2,...,z_t, cannot be distinguished from a random function f^* from $\{0,1\}^n$ to $\{0,1\}^{nt}$ in an efficient way.

The comparison is based on an arbitrary distinguishing algorithm (distinguisher) $\mathcal{A}$ of unlimited computation power. It is given as a black box, which contains a function. The function inside is either function f or function f^*. Then the distinguisher is allowed to make a fixed number of queries about the output values of the function for distinct chosen or adaptively chosen input values. After seeing the results, the distinguisher outputs one bit value, 0 or 1. Denote by p the probability that $\mathcal{A}$ outputs 1 when the function inside is f, and by p^* the probability that $\mathcal{A}$ outputs 1 when the function inside is f^*. Then it is said that f cannot be distinguished from a perfect random function f^* if, for any distinguisher $\mathcal{A}$, the probabilities p and p^* are about the same. The absolute value $|p-p^*|$ is called the advantage of $\mathcal{A}$ and it is denoted by $\mathrm{Adv}\mathcal{A}(f, f^*)$. In [3] the following theorem is stated.

Theorem. *Let n be any fixed integer. Let f denote the function from $\{0,1\}^n$ to $\{0,1\}^{nt}$ obtained by replacing E_K in (1) by a random permutation, and let f^* denote a perfect random function from $\{0,1\}^n$ to $\{0,1\}^{nt}$. Then for any distinguishing algorithm $\mathcal{A}$ using a fixed number q of queries we have* $\mathrm{Adv}\mathcal{A}(f, f^*) \leq 3t^2q^2/2^{n+1}$.

This theorem was improved and equipped with a proof by Gilbert [11]. The new formulation of the theorem incorporates also the offset constants and the advantage bound is decreased to $t^2q^2/2^{n+1}$.

Previously, Bellare et al. studied a similar "one-block-to-many" construction called the XOR mode [6]. However, the XOR mode is defined as an encryption mode of operation, and its security was evaluated for this functionality only. In this model the attacker is only allowed to choose a plaintext and see the resulting ciphertext, but is assumed

to have no access to the input of the keystream generator. For the MILENAGE construction, however, it is essential to prove security also in the case, when the attacker can choose the random challenges and other input parameters. In the model used in [6], distinguishability is limited to a special type of distinguishers, which attempt to determine given two plaintexts and an encryption, which of two plaintexts was encrypted using the keystream generated by the function. This distinguishability notion is known as "left-or-right distinguishability".

The use of different attack models also explain the essential difference in the security bounds by [6] and [11]. Both bounds are quadratic in the number of queries, but the bound by [6] is only linear in the number t of the blocks.

5 UMTS ENCRYPTION ALGORITHM

Once the user and the network have authenticated each other they may begin secure communication. As described above, a cipher key CK is shared between the serving network and the terminal after a successful authentication event. Before encryption can begin, the communicating parties have to agree on the encryption algorithm. In UMTS, implemented according to 3GPP Release 1999, one algorithm f8 is defined. At the time of writing, specification process has begun for designing another encryption algorithm for fall-back purposes.

The specification of the UMTS encryption algorithm is publicly available. The GSM encryption algorithms had created a lot of controversial discussion in the public press. The algorithm had been specified as a secret algorithm, but in the late 1990's, it was reverse-engineered by a team of cryptographers in University of California at Berkeley. One of the main goals of the third generation mobile networks had been to fix the problems that were found in the second generation systems. It was understood that keeping the cryptographic algorithms secret was no longer a good approach. It would be very difficult to gain public confidence in UMTS security if the cryptographic solutions were kept secret. Also the common trend was towards using publicly available cryptographic algorithms.

The UMTS encryption algorithm f8 is a stream cipher. This type of encryption has the advantage that the mask data can be generated even before the actual plaintext is known. Then the final encryption is a very fast bit operation. This stream cipher is built around a block cipher using a special mode of operation. Examples of such standard modes are the counter mode and the output-feedback mode [26]. The f8 stream cipher mode can be seen as a combination of these two standard modes. It also makes use pre-whitening of the feedback data. These three features, output feedback, counter and pre-whitening are combined around a block cipher algorithm.

5.1 The kernel algorithm

The f8 algorithm makes use of a block cipher KASUMI that was specially developed for this purpose by the 3GPP algorithms task force. KASUMI is a modification of MISTY1

[22], which is one of the NESSIE candidates, and has been extensively evaluated by cryptographers within and outside of the NESSIE project [24].

After the publication of KASUMI, public scrutiny on the MISTY type algorithms extended also to KASUMI algorithms. Since many attacks of MISTY1 may also be relevant to 3GPP KASUMI, and the other way round, the extensive analysis on MISTY1 has also consolidated the position of KASUMI as a secure cryptographic primitive.

Before publication, the design team and independent evaluation teams had already tested KASUMI using cryptanalytical methods such as higher order differentials and impossible differentials. The method using higher order differentials had some further developments. Babbage and Frisch showed that even if certain components would be replaced by some other functions of higher nonlinear degree the resistance of MISTY1 against higher order linear cryptanalysis would not be improved [4]. In a subsequent study Canteaut and Videau analysed this phenomenon [8]. The question is about how fast the degree of composed functions increases. Typically, after two applications of functions with degree 3 components we have a function of degree 9, three subsequent applications would produce a function with components of degree 27 and so on. It was shown in [45] that the optimally nonlinear functions have the property that if composed with some other function the algebraic degree grows significantly slower than usually. The functions used in the design of MISTY1 and KASUMI are typical examples of such functions.

At Eurocrypt 2001 conference, Kühn presented analysis on reduced-round MISTY and applied it also to KASUMI [19]. His attack was based on a five-round impossible differential, which is known to exist for a Feistel structure with bijective round functions. These results were already known to the designer team and reported in the evaluation report [2]. Kühn's main result was a method to find part of the key of six rounds of a simplified version of MISTY1. This attack would require 2^{54} chosen plaintext and computation equivalent to 2^{61} encryptions. The attack was applicable only to the simplified version of MISTY1. Later Kühn applied a special technique called Slicing Attack to analyse four rounds of MISTY1 with $2^{22.25}$ of data and 2^{45} of time complexity [20]. In the same workshop, Knudsen and Wagner applied a different analysis technique, Integral Cryptanalysis, to obtain a key recovery attack on five rounds of MISTY1 with the complexity of 2^{34} of data and 2^{48} of computation time [18].

The MISTY1 and KASUMI constructions have also been proven to provide pseudorandomness. The early paper by Sakurai and Zheng had shown that the MISTY structures were not as efficient in providing pseudorandomness as the Feistel construction used by the DES algorithm [29]. However, later Gilbert and Minier [10] and indepedently, Kang et al. [15] showed that the four-round MISTY type transformations are pseudorandom permutations. Later Kang et al. also provided a proof of security of the KASUMI construction by showing that the four-round KASUMI is indistinguishable from a random permutation [16].

One possible line of attacks that may still occur, are the algebraic attacks already applied to the AES block cipher [9, 23]. KASUMI makes use of similar low-degree power

polynomials as the AES algorithm. While such attacks, if successful at all, are not expected to cause any security threat to the practical 3GPP applications, 3GPP has already initiated work for a development of a new fall-back cipher in case of a serious failure of the KASUMI based f8 algorithm.

5.2 The stream cipher mode

The "left-or-right" distinguishability notion has been used to evaluate distinguishability of block cipher modes of operation [6]. This notion was also used by Kang et al. [16] in their attempt to prove that the 3GPP encryption mode f8 is a secure encryption function if the kernel block cipher is a pseudorandom permutation. But later it was shown that their result was not correct, and moreover, that it is impossible to achieve security proof under the assumption that the block cipher is a pseudo random permutation. In [14] a new security proof for the f8 stream cipher mode is given under the assumption that the block cipher is secure under related key attacks.

6 UMTS INTEGRITY ALGORITHM

The purpose of the integrity protection is to authenticate individual control messages. This is important, since a separate authentication procedure gives assurance of the identities of the communicating parties only at the time of the authentication. Then there is a door open for the following attack: a man-in-the-middle acts as a simple relay and delivers all messages in their correct form until the authentication procedure is completely executed. After that, the man-in-the-middle may begin to manipulate messages freely. However, if messages are protected individually, deliberate manipulation of messages can be observed and false messages can be discarded.

The integrity key IK is generated during the authentication and key agreement procedure, similarly as the cipher key CK. The integrity protection mechanism is based on the concept of a message authentication code. This is a one-way function, which is controlled by the secret key IK. The function is denoted by f9 and its output is $MAC\text{-}I$: a 32-bit random-looking bit string. On the sending side, the $MAC\text{-}I$ is computed and it is appended to each signalling message. On the receiving side, $MAC\text{-}I$ is also computed and it is checked that the result of the computation equals to the bit string appended to the message. Any change in any of the input parameters affects the $MAC\text{-}I$ in an unpredictable way. The algorithm for integrity protection is based on the same core function as the encryption, the KASUMI block cipher.

6.1 The MAC mode

Given a block cipher a MAC algorithm is most commonly constructed using a CBC mode of operation [26]. The 3GPP integrity function is not a standard CBC mode construction but has an additional coupling. The main reason for this is the relatively short block length of KASUMI. In the standard CBC mode, the internal state of the algorithm

is equal to the block size of the kernel function. With the enhanced construction the size of the internal state is doubled.

By the Birthday paradox, a CMC mode MAC with a 64-bit block cipher only about 2^{33} messages are required to yield an internal state collision. After an attacker has identified a pair of padded strings M and M', for which such a collision occurs, the attacker can be sure that the padded strings $M||X$ and $M'||X$ have the same MAC for any extension X. Then if the attacker can obtain the MAC for $M||X$, then he can forge the MAC for $M'||X$. This attack would be unrealistic in the 3GPP context, but nevertheless it was decided to increase the internal state to prevent from a collision attack with such a small number of messages, because it does not seem to introduce any other weaknesses. The straightforward collision attack on this construction requires 2^{65} chosen input data, which is completely out of reach.

However, it is not clear what is the actual advantage of the new construction over the standard CBC mode is. The best known attack on f9 found by Knudsen and Mitchell [17] requires approximately 2^{48} chosen input messages, which is still considerably more than for the regular CBC-MAC mode. Knudsen and Mitchell investigate a number of different types of attacks both for key recovery and MAC forgery. The complexity of each attack is determined in terms of the block length n and the final MAC length m. All presented key recovery attacks are infeasible for f9. The best known attack found by Knudsen and Mitchell is a MAC forgery attack which can be launched if $m < n$. It requires in average $2(n+m)/2$ known data string/MAC pairs and $2n - m/2$ chosen data string/MAC pairs. These numbers are equal, exactly if $m = n/2$. For the block size of f9, the numbers of known pairs and chosen pairs required for this attack are equal ($= 2^{48}$), if the MAC length is 32. With shorter MAC lengths the attack would require more chosen input string/MAC pairs and with longer MAC lengths the number of required known pairs would have been larger. Hence with respect to these attacks the chosen MAC length seems to offer the weakest security. But it should be kept in mind that independently of the used MAC generation algorithm there is a straightforward MAC forgery attack, which requires in average 2^{m-1} online MAC verifications. The MAC length of 32 bits can be seen as a compromise between the straightforward MAC forgery attack and the limited bandwidth resources over the air interface.

Similarly as for f8, a security proof has recently been given for f9 after some failed attempts [14]. The security proof suggests that at least for block ciphers that are secure against the related key attacks the security of the 3GPP MAC algorithm is at least as good as the security of the standard CBC-MAC. Now the question is whether it is strictly stronger as the designers anticipated? The best known attack by Knudsen and Mitchell requires 2^{48} chosen input messages while the CBC-MAC security bound is 2^{32}. Closing the gap between 2^{32} and 2^{48} poses an interesting challenge for cryptographic research.

7 CONCLUSION

We gave a brief overview of the basic security functions of GSM and UMTS access networks highlighting the lessons learnt form the history of GSM security. It is clear that access security to cellular network is not sufficient to satisfy service level security requirements such as end-to-end security of phone calls and SMS messages. The WAP system includes its own security specifications that exploit public key cryptography to ensure the security of the WAP services. A more advanced and comprehensive application layer system is the IP Multimedia CN Subsystem (IMS) that has been developed to run on top of any mobile access technology, not only on UMTS or GSM/GPRS access networks, but also on Wireless LAN access systems.

We also described what kind of security services the cryptographic algorithms provide for the UMTS system. How the cryptographic algorithms are used in the system also determine what kind of attacks can be launched in practise to break the algorithms. However, the practical constraints are not usually taken into account when cryptographic algorithms are analysed, but algorithms are considered independently of the application environment and tested against all known cryptanalytic attacks. A failure in some test, even if the test were completely impractical, would prohibit the use of the algorithm for all applications. For each UMTS algorithm we summarised the results achieved by the open cryptographic research community during these four or five years that passed after the publication of the algorithms. We also suggested some directions of analysis which are still unexplored. We conclude that all results achieved so far are in alignment with the views of the design team.

REFERENCES

[1] 3GPP Specifications, http://www.3gpp.org

[2] 3GPP TR 33.909 V1.0.0 (2000-12) Technical Report; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms (Release 1999)

[3] 3GPP TR 35.909 V5.0.0 (2002-05) Technical Report; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation (Release 5)

[4] S.Babbage and L. Frisch. On MISTY1 Higher Order Differential Cryptanalysis. *Proceedings of ICISC 2000*, Lecture Notes in Computer Science 2015, Springer-Verlag, 2000, 22–36.

[5] E. Barkan, E. Biham and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. *Proceedings of Crypto 2003*, Springer-Verlag, 2003.

[6] M. Bellare, A. Desai, E. Jokipii and P. Rogaway. A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation. *Proceedings of 38th Annual Symposium on Foundations of Computer Science*, IEEE , 1997. Full paper available at http://charlotte.ucsd.edu/users/mihir/papers/sym-enc.html

[7] M. Briceno, I. Goldberg, and D. Wagner. GSM cloning, 1998. http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

[8] A. Canteaut and M. Videau. Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis. In Lars Knudsen (Ed.) *Advances in Cryptology - Eurocrypt 2002*, Lecture Notes in Computer Science 2332, Springer-Verlag, 2002, 518–533.

[9] N. Courtois and J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. *Advances in Cryptology - Asiacrypt 2002*, Lecture Notes in Computer Science 2501, Springer-Verlag , 2002, 267–287.

[10] H. Gilbert and M. Minier. New results on the pseudorandomness of some block cipher constructions. In M. Matsui (Ed.) *Fast Software Encryption - FSE 2001*, Lecture Notes in Computer Science 2355, Springer-Verlag, 2002, 248–266.

[11] H. Gilbert. The Security of "One-Block-to-Many" Modes of Operation. In Thomas Johansson (Ed.) *Fast Software Encryption - FSE 2003*, Lecture Notes in Computer Science, Springer-Verlag, 2003.

[12] GSM Association, http://www.gsmworld.com/using/algorithms/index.shtml

[13] ISO/IEC 9798-4: 1999, Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.

[14] T. Iwata and T. Kohno. New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms. In W. Meier and B. Roy (Eds.) Proceedings of FSE 2004, Lecture Notes in Computer Science, Springer-Verlag, 2004.

[15] J. S. Kang, O. Y. Yi, D. W. Hong, H. S. Cho. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. *Proceedings of ACISP 2001*, Lecture Notes in Computer Science 2119, Springer-Verlag, 2001, 60–73.

[16] J. S. Kang, S. U. Shin, D. W. Hong, O. Y. Yi. Provable Security of KASUMI and 3GPP Encryption Mode f8. *Advances in Cryptology - Asiacrypt 2001*, Lecture Notes in Computer Science 2248, Springer-Verlag, 2001.

[17] L.R. Knudsen and C.J. Mitchell. An analysis of the 3gpp-MAC scheme. In Daniel Augot and Claude Carlet (Eds.) *Workshop on Coding and Cryptography, WCC 2001*, Les Ecoles de Cotquidan, 2001, 319-328.

[18] L.R. Knudsen and D. Wagner. Integral Cryptanalysis. In J. Daemen and V. Rijmen (Eds.) *Fast Software Encryption - FSE 2002*, Lecture Notes in Computer Science 2365, Springer-Verlag, 2002, 112–127.

[19] U. Kühn. Cryptanalysis of Reduced-Round MISTY. In B. Pfitzmann (Ed.) *Advances in Cryptology - Eurocrypt 2001*, Lecture Notes in Computer Science 2045, Springer-Verlag, 2001, 325–339.

[20] U. Kühn. Improved Cryptanalysis of MISTY1. In J. Daemen and V. Rijmen (Eds.) *Fast Software Encryption - FSE 2002*, Lecture Notes in Computer Science 2365, Springer-Verlag, 2002, 61–75.

[21] Magic SIM, http://www.magicsim02.com/Eng/e_index.htm

[22] M. Matsui. New Block Encryption Algorithm MISTY. In E. Biham (Ed.) *Fast Software Encryption - FSE '97*, Lecture Notes in Computer Science 1267, Springer-Verlag, 1998, 54–68.

[23] S. Murphy and M. Robshaw. Essential Algebraic Structure within the AES. In M. Yung (Ed.) *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science 2442, Springer-Verlag, 2002, 1–16.

[24] NESSIE, Project Home page: https://www.cosic.esat.kuleuven.ac.be/nessie/ or https://www.cryptonessie.org/

[25] V. Niemi and K. Nyberg. *UMTS Security*, John Wiley & Sons, Chichester, 2003.

[26] NIST FIPS PUB 81, DES Modes of Operation, http://csrc.nist.gov/publications/fips/fips81/fips81.htm

[27] NIST FIPS PUB 197, Announcing the Advanced Encryption Standard, Specification for the Advanced Encryption Standard (AES), November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[28] NIST AES Home page: http://csrc.nist.gov/CryptoToolkit/aes/

[29] K. Sakurai and Y. Zheng. On non-pseudorandomness of block ciphers with provable immunity against linear cryptanalysis. *IEICE Trans. Fundamentals*, vol. E80-A, no. 1, 1997, 19–24.