3GPP TSG-SA3 Meeting #26
Oxford, England, 19-22 November

Tdoc ⌘S3-020656

CR-Form-v7

CHANGE REQUEST

⌘ **TR 55.919** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Algoritms for ECSD and EGPRS
Source:	⌘	Ericsson, Telia
Work item code:	⌘	
Date:	⌘	14/11/2002
Category:	⌘	**F**
Release:	⌘	REL-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ At SA3 #25 Ericsson presented a discussion paper in S3-020545 asking for clarification on the algorithm to be used for EGPRS. The following extract has been taken from the SA3 #25 meeting report:

"TD S3-020545 A5/3 and GEA3 and their relation with EGPRS. This was introduced by Ericsson and questions the use of A5/3 for EDGE and the data-rate for EGPRS and asks SA WG3 to discuss the issues raised in order to provide any necessary CRs to the next SA WG3 meeting. It was confirmed that A5/3 and GEA3 were suitable for both GSM/GPRS and EDGE variants, the algorithm specifications are unclear on this: ***The modulation scheme used in the PS domain does not affect the GEA3 algorithm mechanism. A5/3 (CS domain) has 2 modes of use, GSM standard mode and GSM EDGE mode****. No CR to TS 43.020 was thought necessary, as implementers need to look at the algorithm specifications where the two modes of operation are clarified. It was agreed, however, to create a CR to the Technical Report TR 55.919 to clarify the use of the term "EDGE" in the specifications and the EGPRS bit-rates.* ***K. Boman agreed to do this for the next SA WG3 meeting****."*

Summary of change: ⌘ The term "EDGE" has been deleted from TR 55.919 as it very confusing i.e. the definition is unclear in 3GPP whether it applies for enhanced circuit-switched data or enhanced GPRS or both.
The term ECSD has been introduced as it is defined in 21.905 Vocabulary for 3GPP Specifications and stands for enhanced circuit-switched data.
The term EGPRS has been introduced as it is defined in 21.905 Vocabulary for 3GPP Specifications and stands for enhanced GPRS.
It's been clarified that GEA3 shall be used for EGPRS.
It has been clarified in chapter 6.4.2 that the technical data as data-rates and initialisations and so on are not applicable for EGPRS.

Consequences if not approved:	⌘	It's unclear whether: - the term EDGE means enhanced circuit-switched data or enhanced GPRS or both; - what algorithm that shall be used for EGPRS.

Clauses affected:	⌘	1, 2, 3, 5, 6, 7, 9, 10, 11			
Other specs affected:	⌘	**Y** / **N** ☐ / ☐ ☐ / ☐ ☐ / ☐	Other core specifications Test specifications O&M Specifications	⌘	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TR 55.919 V6.0.0 (2002-09)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Specification of the A5/3 Encryption Algorithms for GSM and ECSD~~DGE~~, and the GEA3 Encryption Algorithm for GPRS ~~and EGPRS~~;
Document 4: Design and Evaluation Report
(Release 6)

Keywords

3GPP, GPRS, security, algorithm

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This Report has been produced by ETSI SAGE Task Force for the design of the GSM A5/3 and GEA3 encryption algorithms.

The work described in this report was undertaken in response to a request made by Security Group GSM Association. The work was done under supervision of the ETSI Mobile Competence Centre (MCC) and the GSM Association.

1 Scope

This Technical Report has been prepared by the ETSI SAGE GSM A5/3 Task Force, and gives a detailed report on the design and evaluation of the **A5/3** encryption algorithms for GSM and ECSD~~DGE~~, and of the **GEA3** encryption algorithm for GPRS (~~and~~including EGPRS).

This document is an accompanying report to the specification and test data documents listed below. Together with the 3GPP Kasumi specification, ref [7], these documents form the entire specifications of the **A5/3** and **GEA3** algorithms:

- Specification of the A5/3 Encryption Algorithms for GSM and ~~EDGE~~ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications.
- Specification of the A5/3 Encryption Algorithms for GSM and ~~EDGE~~ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 2: Implementors' Test Data.
- Specification of the A5/3 Encryption Algorithms for GSM and ~~EDGE~~ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 3: Design Conformance Test Data.

This public report contains a detailed summary of the work performed during the design and evaluation of the GSM A5/3 algorithm for GSM and ECSD~~DGE~~ and the GEA3 Encryption algorithm for GPRS~~ and EGPRS~~. It contains all results and findings from this work and should be read as a supplement to the formal specification documents, ref. [3] - [5]. Some of the results in this report were initially published in the 3GPP Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms, ref. [8].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[2] GSM Association Specification for A5/3. "Requirements Specification for the GSM A5/3 Encryption Algorithm (Version 2.0 final)".

[3] TS 55.216: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ~~EDGE~~ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications".

[4] TS 55.217: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ~~EDGE~~ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 2: Implementors' Test Data".

[5] TS 55.218: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ~~EDGE~~ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 3: Design Conformance Test Data".

[6] 3GPP TS 35.201 version 4.1.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: *f8* and *f9* Specification".

[7] 3GPP TS 35.202 version 4.0.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

[8] "Security Algorithms Group of Experts (SAGE); Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms". Version 2.0, 2000-10-06.

[9] ISO/IEC 9797-1:1999(E): "Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1".

[10] ISO/IEC 10116:1996: "Information technology – Security techniques – Modes of operation for an *n*-bit block cipher algorithm".

Additional references to external documents are provided in Annex A.

3 Abbreviations

For the purpose of the present report, the following abbreviations apply:

APN	Almost perfect non-linear
A5/3	Encryption algorithm for GSM and ECSD~~DGE~~
BLCKCNT	Blockcounter used in A5/3 and GEA3
CA	Input parameter to the KGCORE function – 8 bit

CB	Input parameter to the KGCORE function – 5 bit
CBC	Cipher Block Chaining
CC	Input parameter to the KGCORE function – 32 bit
CD	Input parameter to the KGCORE function – 1 bit
C_i	Round constant used in KASUMI key scheduling
CK	Cipher Key
CO	Output bitstream from the KGCORE function
DSP	Digital Signal Processor
~~EDGE~~	~~Enhanced Data rates for GSM Evolution~~
ETSI	European Telecommunications Standards Institute
FI	Component function of KASUMI
FL	Component function of KASUMI
FO	Component function of KASUMI
f8	UMTS confidentiality (encryption) algorithm
f9	UMTS integrity algorithm
GEA3	Encryption algorithm for GPRS ~~and EGPRS~~
GF(q)	The finite field of q elements
3GPP	3rd Generation Partnership Project
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GSMA	GSM Association
IV	Initialisation Vector
K_C	GSM Cipher Key
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KI	Component of round key in KASUMI
KL	Component of round key in KASUMI
KO	Component of round key in KASUMI
MAC	Message Authentication Code
MCC	Mobile Competence Centre
MS	Mobile Station
LP	Linear probability
OFB	Output feedback mode
SAGE	Security Algorithms Group of Experts
SAGE TF 3GPP	SAGE Task Force for the design of the standard 3GPP Confidentiality and Integrity Algorithms
S7	Substitution box used in KASUMI
S9	Substitution box used in KASUMI
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	User Services Identity Module
XOR	Exclusive Or operation

4 Structure of this report

The material presented in this report is organised in the subsequent clauses, as follows:

- Clause 5 provides background information on KASUMI and the development of GSM A5/3 and GEA3;
- Clause 6 provides a summary of the algorithm requirements;
- Clause 7 provides a summary of design and evaluation criteria;
- Clause 8 provides a brief description of the KASUMI block cipher and the A5/3 and GEA3 modes of use;
- Clause 9 provides some background information on the chosen design;
- Clause 10 gives an overview of the evaluation work carried out by ETSI SAGE Task Force and other parties and the conclusions of the evaluations;
- Clause 11 lists the specific quality measures taken during the project.

- Annex A includes a list of external references that are related to the results in this report.

5 Background to the design and evaluation work

The development of new standardised encryption algorithms for use in GSM (including ECSD~~DGE~~) and GPRS (including EGPRS) systems was conducted by an enlarged ETSI SAGE task force in response to a request from the GSMA security group. The purpose was to develop a modern and strong encryption algorithm for use in these systems based upon previous work done for 3GPP (ref. [8]). It was especially mentioned in the requirements that the algorithm should be based on the 3GPP algorithm KASUMI. It was also clear that available resources would not allow to develop a new algorithm from scratch.

The ETSI SAGE group decided on the following strategies for the work:

- Invite external experts from the 3GPP task force to enlarge the ETSI SAGE group for the project.
- Make re-use of results and analysis from the 3GPP project, but achieve necessary cryptographic separation between the different designs.
- Invite interested manufacturers to comment on the needs for compliance with the 3GPP f8 confidentiality function.
- Try to avoid or minimise the need for additional statistical testing and external evaluation.

6 Summary of algorithm requirements

This section gives a summary of the algorithms requirements described in ref. [2].

6.1 Use of the algorithm

The algorithm shall only be used for GSM, ECSD~~DGE~~, GPRS and EGPRS encryption as described in ref.[1].

More specifically the use of the algorithm is as follows:

- The algorithm is used to encrypt user and signalling data over the air interface;
- The algorithm will be used for GSM;
- The algorithm will be used for ECSD~~DGE~~, enhanced circuit-switched data in GSM;
- The algorithm will be used for GPRS packet radio service in GSM.
- The algorithm will be used for EGPRS, enhanced GPRS in GSM.

6.2 Types of implementation

The normal method for implementing the algorithm is in hardware or DSP.

6.3 Type and parameters of algorithm

The type and parameters of the algorithm are identical to those of the A5 algorithm, which are specified in ref.[1]. Also some additional requirements applied. The requirements are summarised here.

- The algorithm shall be based on KASUMI as defined by 3GPP
- The algorithm is a binary key stream generator.
- The inputs are the key K_c, a time variant parameter COUNT and optionally a direction bit DIRECTION.

- The outputs of the ciphering algorithm are two binary blocks BLOCK1 and BLOCK2.

Relation of the input and output parameters is illustrated in figure 1.

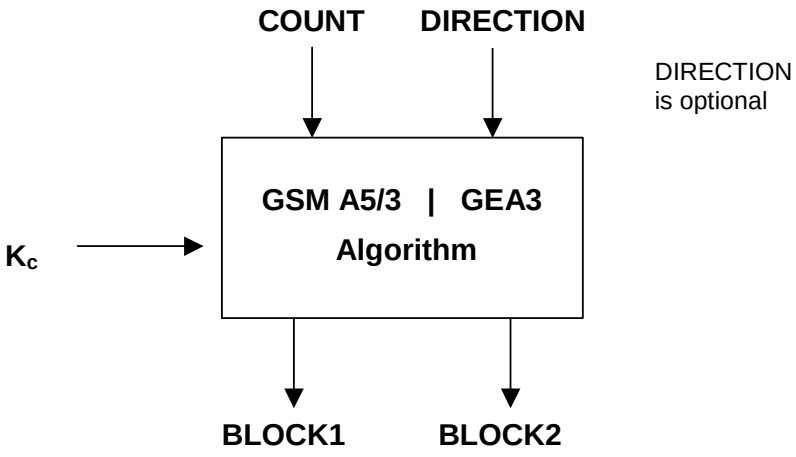

Figure 1 – Algorithm Parameters

The parameters of the algorithms are to be as follows:

Table 1: Algorithm parameters

	GSM (A5/3)	ECSD~~DGE~~ (A5/3)	GPRS ~~and EGPRS~~ (GEA3)
K_c	64 – 128 bits	64 – 128 bits	64 – 128 bits
COUNT	22 bits	22 bits	32 bits
BLOCK1	114 bits	348 bits	M bytes
BLOCK2	114 bits	348 bits	Not Applicable
DIRECTION	Not Applicable	Not Applicable	1 bit

6.4 Implementation and operational considerations

6.4.1 GSM/ECSD~~DGE~~

The performance requirements for the A5 cipher algorithm used for GSM/ECSD~~DGE~~ are given in GSM 03.20. The current version is 8.1.0.

GSM

For ciphering, Algorithm A5 produces, each 4.615 ms, a sequence of 114 encipher/decipher bits (here called BLOCK) which is combined by a bit-wise modulo 2 addition with the 114-bit plain text block.

For each slot, deciphering is performed on the MS side with the first block (BLOCK1) of 114 bits produced by A5, and enciphering is performed with the second block (BLOCK2). As a consequence, on the network side BLOCK1 is used for enciphering and BLOCK2 for deciphering. Therefore Algorithm A5 must produce **two blocks of 114 bits** (i.e. BLOCK1 and BLOCK2) **each 4.615 ms**.

ECSD~~DGE~~

In ECSD~~DGE~~ the block size is greater than 114 bits. With ECSD~~DGE~~ a modification of the usage of the A5 algorithm is employed which produces BLOCK 1 and BLOCK2 which **each contain 348 bits**. The other parameters are not

modified. The modified algorithm produces **both blocks** during a TDMA frame duration, i.e. **4.615 ms**. The blocks are combined by bit-wise modulo 2 addition with the plaintext data.

It is possible in ECSD~~DGE~~ that the plaintext data block for either uplink or downlink is shorter than 348 bits. In this case only the first part of the corresponding output parameter BLOCK is used in the bit-wise addition and the rest of the bits are discarded.

6.4.2 ~~6.4.2~~ GPRS~~/EGPRS~~

Notice that the following GPRS performance requirements for the MS in this chapter are not applicable for EGPRS.

The GPRS performance requirements are specified in GSM 02.60. In **GSM 01.61 version 8.0.0 release 1999**, Section 6.4, the requirements for the GPRS ciphering algorithm are stated as follows:

> Requirements refer to an MS, which admits only 1 timeslot GPRS communication (see note 1), and to an MS, which admits GPRS communication over the maximum number of timeslots (see note 2).
>
> NOTE 1: An MS which admits only one time slot GPRS communication, the maximum capacity in each direction is 21.4 kbit/s (total rate up to 42.8 kbit/s), 12 initialisations per second are assumed (assuming packet length of 500 octets) (scenario 1).
>
> NOTE 2: An MS would have a maximum throughput of all 8 timeslots in both directions each transmitting and receiving at their maximum rate of 21.4 kbit/s (total rate up to 342.4 kbit/s), 100 initialisations per second are assumed (assuming packet length of 500 octets) (scenario 2).

The performance requirements, on the GPRS ciphering algorithm, as used in scenario 1, are expected to be similar to the performance of the existing A5 algorithm.

It is also expected that the performance increases linearly depending on the number of timeslots, the MS is able to use for GPRS.

The clock speed of the mobile may be assumed to be 50MHz.

6.4.3 Implementation complexity

It should be possible to implement the algorithm in hardware using available technology with less than 10000 gates.

6.5 Security of the algorithm

- The algorithm needs to be designed with a view to its continuous use for a period of at least 15 years.
- The security shall be such that there are no known plaintext attacks on the algorithm needing significantly fewer operations than an exhaustive key search.

7 Design and Evaluation Criteria

7.1 Design Criteria:

Based upon the requirements listed in section 6, the task force agreed on the following criteria for the algorithm design:

- The design should be based on the GSM Association Requirements Specification of A5/3, ref. [2];
- There should be one common design that supports the GSM, ECSD~~DGE~~, ~~GPRS~~ and ~~E~~GPRS modes.
- The new design should be as close to the UMTS f8 design as possible.
- Any differences with the UMTS f8 design should in the first place be achieved through the algorithm inputs.
- The modes for GSM, ECSD~~DGE~~, ~~GPRS~~ and ~~E~~GPRS should be cryptographically separated; Preferably these modes should also be cryptographically separated from the UMTS f8.

- The complexity and performance of the algorithm should be comparable to the UMTS f8.

7.2 Evaluation criteria

The agreed criteria for the evaluation work are summarised in the following principles:

- The evaluation of the A5/3 should where possible use the results of the UMTS f8 evaluation; the evaluation should be focused on the aspects where A5/3 and UMTS f8 differ.
- Statistical evaluation is not required, unless there are good arguments for statistical evaluation of specific aspects of the A5/3 design.
- The A5/3 Algorithm needs to be designed with a view to its continuous use for a period of at least 15 years.
- The security shall be such that there are no known keystream attacks on the algorithm predicting a significant amount of additional keystream even with chosen input needing significantly fewer operations than an exhaustive key search (note)

NOTE: An inherent limitation on the GSM security is that the frame counter is limited to 22 bits.

- The algorithm should be no more vulnerable to attacks distinguishing the keystream from a random sequence than other well known block-cipher based constructions, e.g. output feedback mode.

8 GSM A5/3 and GEA3 Encryption Algorithms

The detailed specifications of the A5/3 and GEA3 algorithms are found in ref. [3] and ref. [7]. For this report we include a general overview of the design. The basic building block is the block cipher KASUMI, which is a Feistel block cipher with a block size of 64 bits and a 128-bit cipher key.

8.1 KASUMI

The structure of KASUMI is depicted in the following diagrams:

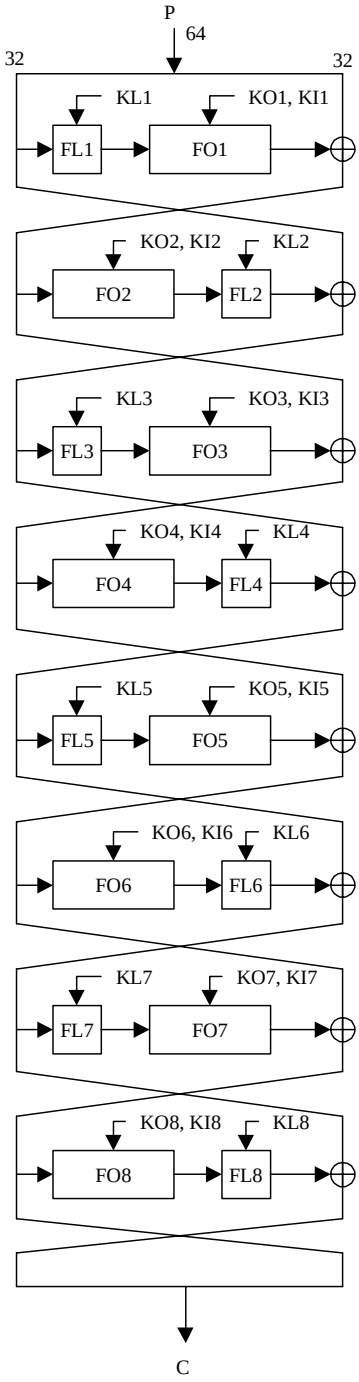

Fig. 2: KASUMI

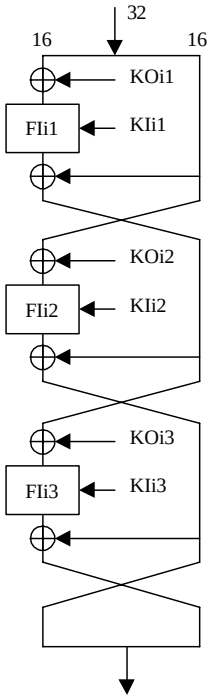

Fig.3: FO Function

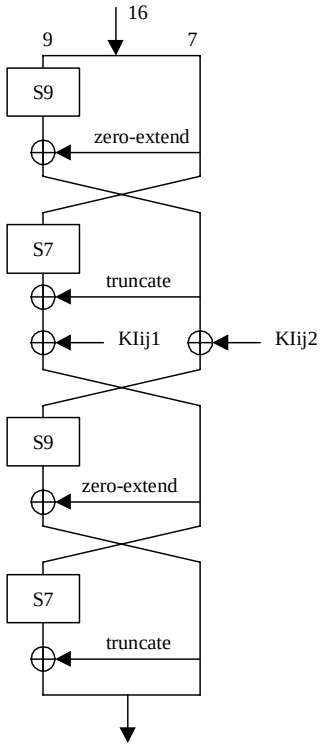

Fig.4: FI Function

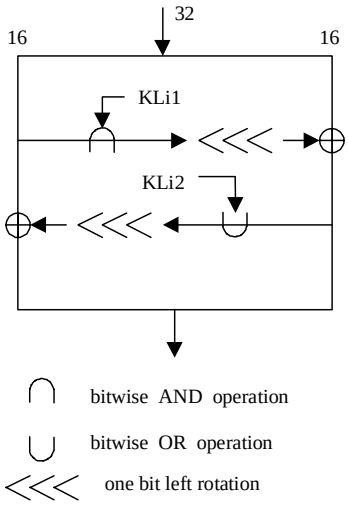

Fig.5: FL Function

KASUMI encrypts a 64-bit input by iterating a round function 8 times. The round function consists of the composition a 32-bit non-linear mixing function (FO) and a 32-bit linear mixing function (FL). The FO-function is again an iterated "ladder-design" consisting of 3 rounds of a 16-bit non-linear mixing function FI. In turn, FI is again defined as a 4-

round structure using non-linear look-up tables S7 and S9. All functions involved will mix the data input with key material. See ref. [7] for details on the specification of S-boxes and generation of round keys.

8.2 Confidentiality function KGCORE

The stream cipher KGCORE used for encryption of data frames in A5/3 and GEA3 is constructed from KASUMI in a variant of the standard Output Feedback Mode (OFB) ref. [10], with 64-bit feedback. The construction is depicted in the following diagram:

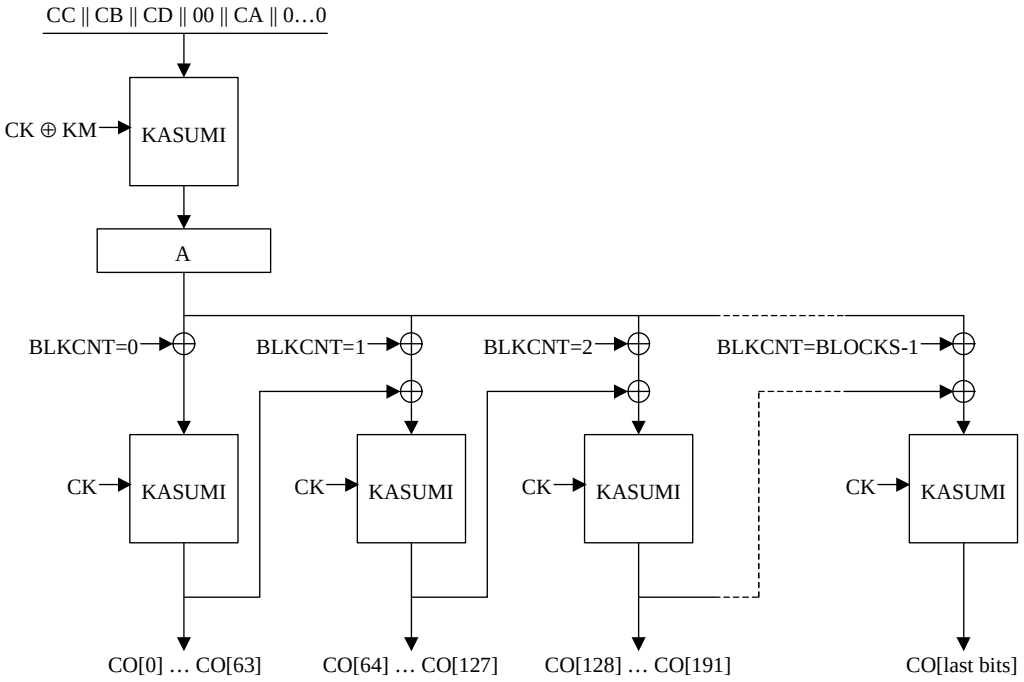

Figure 6: The confidentiality function KGCORE

During a pre-computation phase, the system parameters CC, CB, CD and CA are padded with zeroes to become a full length data block and KASUMI encrypted with a derived key CK⊕ KM. The output of this process is a 64-bit register value A, which is part of the input in each subsequent KASUMI computation. The input parameter CA is used to provide the cryptographic separation between the use of the algorithm within the three systems, and also with the UMTS f8 function.

Subsequent blocks (64 bits) of keystream are then generated by running KASUMI in output feedback mode with additional input of A and the block counter (BLKCNT) to the feedback. The cipher text is then produced as the exclusive or of the keystream bits and the plaintext bits.

9 Rationale for the chosen design

9.1 General comments

The essential design goals for the A5/3 and GEA3 encryption algorithms were that the algorithm should:

- provide a high level of security within the GSM/ECSD~~DGE~~/GPRS~~/EGPRS~~ context;
- meet their implementation requirements - in particular, allow a low power, low gate count implementation in hardware.

The designers have therefore deliberately avoided over-designing the algorithm. They wanted the algorithms to be secure against all practical attacks in the GSM/ECSD~~EDGE~~/GPRS~~/EGPRS~~ context, and carefully decided not to over-complicate them just to provide a very high security margin against unrealistic theoretical attacks.

The following types of attacks against the underlying block cipher KASUMI were particularly considered:

- linear cryptanalysis;
- differential cryptanalysis, and variants such as impossible differentials, "miss in the middle", etc;
- higher order differential cryptanalysis and interpolation, including probabilistic higher order analysis;
- identifying any classes of weak keys.

No weak keys were found. There are chosen plaintext and/or related key attacks against KASUMI reduced to 5 rounds, see section 9.2. We believe that with further analysis it might be possible to extend some attacks to 6 rounds, but not to the full 8 round KASUMI. In any case, the more powerful attacks do not translate to practical attacks against the A5/3 and GEA3 algorithms in the operational context.

There are several obvious ways to increase the security margin offered by KASUMI. These include:

- increasing the number of rounds;
- adding a fourth round to the FO function;
- making the key schedule more complicated.

All of these were considered, and rejected as adding complexity for no practical gain.

Attacks against the A5/3 and GEA3 constructions were also considered. The current construction is a good example of the pragmatic approach to the design. Given a very long sequence of keystream (of order 2^{38} bits), it would be possible to identify a small amount of structure in the keystream, which could be classified as an attack (or at least an imperfection); but in the GSM/ECSD~~EDGE~~/GPRS~~/EGPRS~~ context, such long frames of keystream will not occur, so the designers saw no need to protect further against this kind of attack.

9.2 Design Policy of MISTY1

The A5/3 and GEA3 crypto engine KASUMI is based on the block cipher MISTY1, ref. [21], which was designed according to the following three principles:

- MISTY should have a numerical basis for its security;
- MISTY should be reasonably fast in software on any processor;
- MISTY should be sufficiently fast in hardware implementation.

The algorithm was designed to be provably secure against differential and linear cryptanalysis. This results from building the algorithm according to provable constructions from smaller components with known resistance against these two types of attacks. The Feistel structure of MISTY1 is recursively repeated in the smaller round function FO and in the kernel FI.

The unequal division of FI is due to the fact that bijective functions of odd size are generally better than those of even size from the viewpoint of provable security against linear and differential cryptanalysis.

In selecting the S-boxes *S*7 and *S*9, the following criteria were adopted:

- Their average differential/linear probability must be minimal;
- Their delay time in hardware is as short as possible;
- Their algebraic degree is high, if possible.

The resulting functions were found by searching for functions of the form $A(x^t)$ over $GF(2^7)$ and $GF(2^9)$, where A is a bijective linear transformation. The non-linear degree of *S*7 is 3 and the non-linear degree of *S*9 is 2.

For the purpose of avoiding possible attacks other than differential and linear cryptanalysis, the design of MISTY1 was supplemented with the simple and fast function FL. This function is linear for a fixed key, but has a variable form depending on the key value.

The key scheduling part of MISTY1 was designed according to the following principles:

- The size of the key is 128 bits;
- The size of the subkey is 256 bits;
- Every round is affected by all key bits;
- As many subkey bits as possible affect every round.

9.3 Changes from MISTY1 to KASUMI

This section summarises the changes that have been done to MISTY1 during the design of KASUMI.

9.3.1 Data Encryption Part

a) *Changing the location of the FL functions.*
This makes hardware simpler; (but a bit slower - this drawback is recovered with other changes. Note that this structure does not block parallel computation of two FI functions).

b) *Removing the subkey KO_{i4} in the FO function.*
This makes hardware simpler and faster; as the FO function now has a simple repetitive structure.

c) *Adding rotate shift functions in the FL function.*
It is assumed that this makes cryptanalysis harder and has no negative impact on hardware size and speed.

d) *Changing of the substitution table S7.*
This is not a significant change, and is in fact equivalent to just rearranging the bit order before and after the original *S*7. We have not found a better table from the viewpoint of hardware implementation.

e) *Changing of the substitution table S9.*
This makes hardware smaller (and possibly faster). The total number of "terms" of the new *S*9 in its algebraic normal form is smaller than that of the original *S*9. We searched all polynomials and normal bases, all powers whose hamming weight is two, and all linear combinations of t_j's for shorter y_i's (see [5]), where the length of y_i is defined as the number of terms (except a constant value) in its algebraic normal form. For the new *S*9, the average length of yi's is 11.2, while for the original version it is 11.7.

f) *Adding another S7 in the FI function*
This makes the security level significantly higher but hardware bigger. We expect that this increase will be compensated with the reduction of the key scheduling part. Note that the penalty on hardware speed is not particularly significant because *S*9 and *S*7 can be performed in parallel.

9.3.2 Key Scheduling Part

a) Removing all FI functions in the key scheduling part.
This makes hardware smaller and/or reduces key set-up time. We expect that related key attacks do not work for this structure.

b) Adding the constant values Ci and rotate shift operations.
This avoids using the same subkey values in different rounds.

9.4 Rationale for the A5/3 and GEA3 design

The construction of the KGCORE confidentiality function is quite similar to the one used for the 3G confidentiality function f8. The two main distinctive features of this construction are the following:

(1) the precomputation of a prewhitening constant A (based upon the initial values CA, CB, CC and CD and upon the modified key value (CK ⊕ KM)

(2) the technique used to produce a sequence of keystream blocks is **neither a mere counter mode nor a mere OFB mode, but a mixture of both techniques.**

The main reason for choice (1), i.e. the precomputation of a prewhitening constant A, was to provide some protection of the underlying blockcipher (KASUMI) by preventing the access by an adversary to blockcipher outputs corresponding to known or chosen inputs. Moreover, as will be shown in section 10.4 , the fact that the prewhitening constant A depends upon the initial values CA, CB, CC and CD provides extra protection against some distinguishing attacks.

The main reasons for choice (2) were to avoid some undesirable properties resulting from a mere OFB mode or a mere counter mode. As a matter of fact:

- **A mere OFB mode, whether or not combined with the precomputation of a prewhitening constant A**, would have allowed for short cycles in the keystream. Though short cycles would not occur with a very high probability, they represent a more serious practical threat than most other distinguishing properties (because they may lead to the disclosure of a much larger amount of information), and are therefore to be avoided.

- **A mere counter mode, if combined with the precomputation of a prewhitening constant A (choice 1), would lead to distinguishing attacks of substantial probability requiring only about 2^{32} keystream blocks.** Let us indeed assume that two keystream blocks, corresponding to blockcounter values i and j and prewhitening values A and A' are equal, i.e. A ⊕ i = A' ⊕ j. Then, other pairs of colliding keystream blocks corresponding to pairs of blockcounter values of the form (i+d, j+d) are likely to exist. For instance if i and j are both even, then two subsequent keystream blocks (corresponding to blockcounter values i+1 and j+1 respectively) are also equal, since i+1 = i ⊕ 1 and j+1 = j ⊕ 1, and therefore A ⊕ (i+1) = A' ⊕ (j+1).

- **In the case of a mere counter mode not combined with the precomputation of a prewhitening constant A (choice 1)**, the former distinguishing attack could be avoided, if the KASUMI input block in the computation of each keystream block consisted of CA, CB, CC, CD, the blockcounter value, and of some filling bits. However, the advantage resulting from choice (1) mentioned before would be lost and moreover, another kind of distinguishing property requiring about 2^{32} keystream blocks would exist, namely the fact that the keystream blocks corresponding to distinct (CA,CB,CC,CD, Blockcounter) values would necessarily be pairwise distinct, whereas some collisions of pairs of keystream blocks would be likely to occur in the case of a perfectly random keystream generator.

10 Algorithm evaluation

In this section we summarise the results of the algorithm evaluation. Much of this work was done as a part of the 3GPP Standard Confidentiality and Integrity algorithms project and for more details we refer to the report ref. [8]. The scope for this latter evaluation work was:

- Analysis of the various components of KASUMI;

- Analysis of KASUMI as a generic 64-bit block cipher;

- Analysis of the encryption mode used for A5/3 and GEA3.

All of these aspects have been exposed to mathematical and statistical evaluation by the task force and by external evaluators. No attacks that threatens the use of A5/3 and GEA3 within GSM/ECSD~~DGE~~/GPRS~~/EGPRS~~ systems have been identified and the general conclusion is that the algorithm is well suited for its intended use.

10.1 Properties of KASUMI components

Each functional component of KASUMI has been carefully studied to reveal any weakness that could be used as a basis for an attack on the entire algorithm. The following are the main results from this work.

10.1.1 FL function

The FL function is a linear function, and the security of the algorithm is not meant to depend on this function. Its main purpose is to be a low cost additional scrambling, making individual bits harder to track through the rounds.

The FL function has the property that for any key KL, an input of $0^{16}1^{16}$ always gives an output of 1^{32}. Hence for some round inputs, some of the key bits in KL can be changed without having any effect on the output of that round. This property can be used to guarantee a zero difference at the end of the first round, thus effectively removing the first round. More generally, small changes to the input to FL only make small output changes, and this can be useful going either forwards or backwards through FL.

The fixed point is used in some of the differential attacks mentioned later, but no attack exploiting this property that extends beyond 5 rounds of KASUMI has been found.

10.1.2 FI function

This is the basic randomising function of KASUMI with 16 bits input and 16 bits output. It is again composed of a four-round structure using two non-linear substitution boxes S7 and S9. Using theorem 4 of ref. [21], we can show that the average linear and differential probability of FI is less than $(2^{-9+1})(2^{-7+1}) = 2^{-14}$ assuming uniform distribution of the subkeys in use. S7 and S9 have been designed in a way that avoids linear structures in FI. This fact has been confirmed by statistical testing.

10.1.3 The S7 box

The S7 box in KASUMI is essentially the same as S7 in MISTY1 (see [21]); the KASUMI S7 was made by rearranging the bit order before and after the original S7. The S7 box is specially designed to be easy to implement in hardware using combinatorial logic, and as a consequence the non-linear order is 3. The algebraic normal form of this function can be found in ref. [7].

10.1.4 The S9 box

The S9 box is different from the S9 box in MISTY1[21], but it has been constructed in much the same way. That is, it is easy to implement in hardware (actually easier than the original S9), and has non-linear order 2. The algebraic normal form of this function can be found in ref. [7]. S9 can been seen as a composition of the power function $x \# x^5$ and a linear output transformation defined over $GF(2)^9$, it is known that it achieves almost perfect non-linearity.

10.1.5 Key schedule

The key schedule of KASUMI is very simple, but this fact has not been found to constitute any real weakness, and there seems to be no gain in practice by making it more complicated. Each of the 128 bits of secret key is used once and only once in every round. They are used in different ways in different rounds, and also at different parts within those rounds, and at times the values are altered using key modifications constants.

Due to the use of the constants C1 to C8 in the key schedule, there is no fixed recurrence relation between consecutive round keys. This property is required to prevent chosen plaintext attacks that are faster than exhaustive search. Further, there exists no equivalent, more compact representation of the expanded key.

Even if regularity and symmetry in the key scheduling do not introduce weaknesses in the algorithm, care should be taken such that shorter keys e.g. 64 bit keys are not extended to a full-length key in a very symmetric way. Just padding with zeroes could give some advantage to an attacker and should not be recommended.

In his analysis of MISTY1 ref.[21] Matsui shows that if the subkey bits are independent, the average differential and linear probabilities are less than 2^{-56}. Some concern has been expressed that with the simple key schedule in KASUMI, the assumption of subkey independence might be too optimistic. However, we have no indications in this direction.

10.1.6 Statistical testing of components

The two S-boxes S7 and S9 are Almost Perfect Non-linear (APN) bijective Boolean Mappings. It is known from the literature (e.g. [14] and [24]) that those functions have specific properties. Some results from the calculations and tests made are due to the construction of the S-boxes. The statistical tests confirmed the design principles of the actual constructions.

The linear approximation test showed that in the case of S7 the maximal Hamming distance of each linear combination of the output components of S7 from the set of affine functions is equal to 64 + 8 = 72, i.e. each linear combination of the output components can be approximated by at least one affine function up to 64 + 8 = 72 values. For S9 the value for the Hamming distance described above is equal to 256 + 16 = 272. That is because the Walsh transform of each linear combination of the output components of the S7 and S9 mappings are three-valued (see [14]).

S7 has no linear factors. But for each linear combination of the output components of S9 one can find one linear factor. That is due to the fact that the component functions of S9 are quadratic (see [24]), i.e. the algebraic normal form of the component function has quadratic terms at the most.

Concerning the cycle structure, S7 and S9 have no obvious deficiencies, e.g. a lot of transpositions.

S7 and S9 are not random S-boxes. The dependence test showed that each output bit of both mappings is dependent on every input bit. But for S9 there are output bits which always change when one input bit is toggled. This is because of the linear structures of S9. S7 satisfies the Avalanche effect, S9 does not.

For the FI and the FO functions no linear structures were found. The dependence test showed that each output bit of both functions is dependent on every input bit. Both functions satisfy the Avalanche effect. But a closer look at the FI function shows that it doesn't behave like a random function according to the dependence test.

10.2 Analysis of KASUMI as a generic 64-bits block cipher

10.2.1 Differential cryptanalysis

From its construction it is clear that, provided that subkeys are independent, three rounds of KASUMI have no differential or linear characteristics with probability larger than 2^{-56}. It should be noted that the upper bounds on FI, see 10.1.2, is tight. It is possible to find differential characteristics for FI with probability 2^{-14}. It is also important to note that the differential effect of FL is low.

In this section we review some of the differential attacks that have been found on reduced versions of KASUMI.

A differential chosen plaintext attack

A chosen plaintext attack on 5 rounds of KASUMI that can be used to recover the key is described in ref. [8]. The attack requires roughly 2^{38} chosen plaintexts, and 2^{80} small operations. It might be possible to extend this attack to 6 rounds, but not to the full 8 rounds of KASUMI.

Differential related key attacks

Though related key attacks seem not to be a threat within the A5/3 and GEA3 use of context, such attacks were considered. It was concluded that it is possible to perform differential related key attacks on four and five rounds of KASUMI. The four round attack requires the encryptions of approximately 2^9 chosen plaintext pairs X and X^* under keys K and K^* respectively, where K and K^* differ in only one bit. The average complexity of this attack is approximately 2^{41}. The five round attack, which is an extension of the four round attack, requires the encryptions of on average $3 \cdot 2^{17}$ chosen plaintext pairs, and has an average complexity of approximately 2^{36}.

Impossible differentials

In the FI function there are no impossible differentials, because of its four-round structure. In the three round FO function, however, several impossible differentials occur since the round function FI is bijective. These lead to impossible differentials over 2 and 3 rounds of KASUMI without the FL function.

The FL functions seem to destroy most of these impossible differentials, or more precisely, make their existence key dependent. We were not able to derive any impossible differentials for the true KASUMI from those known to exist for the FO function.

Hence we are not aware of other impossible key-independent differentials for the KASUMI cipher, than the well-known five-round impossible differential of the form:

$$(0, A) \rightarrow (A, 0) \rightarrow (*, A) \rightarrow (A, *) \rightarrow (0, A) \rightarrow (A, 0)$$

where A is a non-zero 32-bit block, 0 is a 32-bit block of all zeros and each occurrence of $*$ can be replaced by any (possibly different) non-zero block.

This differential can however be used to distinguish 5 round KASUMI from a truly random function, see [8] for details.

An attack on KASUMI reduced to 6 rounds has been found that requires 2^{55} chosen plaintexts and computation of approximately 2^{119} FI values. Another attack against 6 rounds of KASUMI has been found requiring $2^{53.3}$ chosen plaintexts with a complexity of the order of 2^{100} encryptions. Both attacks exploit impossible differentials and the structure of the FO function.

No similar attack on the full 8 rounds of KASUMI has been found, and in the actual context these attacks are not applicable.

Truncated differentials

The best way that has been found to exploit truncated differentials for KASUMI leads to an attack on 3 or 4 rounds of KASUMI without the FL function. This attack uses the fact that the function FO restricted to the 16 leftmost input bits, is bijective onto the leftmost 16 bits in the output.

3 rounds can be broken using about 2^{35} plaintext pairs derived from 2^{18} chosen plaintexts. The 4 round attack requires 2^{48} chosen plaintexts. The FL function will complicate the attack, and in any case, KASUMI with 5 rounds or more is secure against this attack.

10.2.2 Linear cryptanalysis

The validity of the proofs of security given by Matsui in [21] has been examined. That is, how average is the behaviour of fixed keys with respect to linear approximations over the FI function. Mathematical calculations using the Walsh-Hadamard transform and experimental calculations were carried out independently and reached the same conclusions.

LP^{FI} was estimated to be on average smaller than 2^{-14} for any linear hull over FI, but there are specific key values and linear hulls for which $LP^{FI} \approx 2^{-12}$. Of course there will also be key values for which the actual bias is much less than the average case. The maximal amounts of correlation are not high enough to make it possible to chain them to a useful linear approximation path over rounds of KASUMI. For construction of overall approximations one needs to consider all possible paths, and not only the ones which give large biases (correlations).

One attack on five rounds of KASUMI might be possible, but it would require a work effort of at least 2^{95}, around 2^{58} known plaintexts and only be applicable to a fraction of 2^{-3} of the key space. A variant may potentially reduce the work effort to 2^{93} and require around 2^{49} known plaintexts, but will only be applicable to a fraction of 2^{-41} of the key space.

We conclude that, for the full 8 round KASUMI, all keys of the FI function behave pretty much like an average key with respect to the studied linear approximation relations.

10.2.3 Higher order differential attacks

Quite a lot of analysis has been conducted in Japan concerning the strength of the Misty algorithms. Tanaka et al. shows in [31] that 5 round Misty1 without the FL function can be attacked using 1,408 chosen plaintexts, with a method using 6^{th} and 7^{th} order differentials.

It can be shown that the differential property leading to this attack is actually due to the choice of the *S*7 box. Further, it can be shown that it is actually not possible to find an *S*7 box coming from a mapping $x \# x^{e_3}$ with an exponent e_3 of Hamming weight 3, that is at the same time an optimum from the points of view of average differential/linear probabilities and of the 7^{th} order differential property. Finally, the product of any two output bits from S7 will have an algebraic degree bounded by 5.

However, we do not believe that this 7^{th} order differential property still holds for KASUMI, due to the modification of the FI function. Further, we are convinced that traditional attacks based on higher order differentials will work for at most 5 rounds of KASUMI, and no other variants have been found that work for more than 5 rounds of KASUMI.

In [30] Sugita shows the relation between inputs and outputs of 6 rounds of a "Misty-like" transformation, and proves it is not a locally random function. The relation is used in a higher order differential attack to guess the key of 5 round Misty1 without the FL function.

10.3 Implementation attacks

KASUMI has also been analysed with respect to differential attacks like *timing attacks, simple power analysis and differential power analysis.* This investigation did not reveal any properties of KASUMI that would make it particularly vulnerable to these type of attacks. Specifically KASUMI has a favourable key scheduling with respect to power attack methods that try to derive information about the Hamming weight of subkey bytes. The restricted use of KASUMI in the 3GPP environment will also reduce the possibilities for such attacks. In an application where an attacker can do measurements of time of execution and/or power consumption, specific care should be taken to guarantee resistance against implementation attacks.

10.3.1 Statistical evaluation of KASUMI

The block cipher KASUMI itself was tested by statistical methods. We used the dependence test to see if KASUMI satisfies the plaintext-ciphertext Avalanche effect and the key-ciphertext Avalanche effect. The Avalanche effect demands that about 32 bits of the output block shall change if one bit of the 64-bit input block is toggled if the key is fixed, or if one bit of the 128-bit key is toggled provided the same input block is used. We performed the dependence test on KASUMI reduced to two rounds, reduced to four rounds and on the full round KASUMI.

KASUMI reduced to four rounds already satisfies the key-ciphertext and the plaintext-ciphertext Avalanche effect.

To check how good KASUMI destroys redundancy in the input data, we generated a sequence of 16384 blocks of 64 bits by consecutive applications of the block cipher algorithm in ECB-mode, where between two encryption operations the input block is increased by one, starting with the all-zero block. The key was randomly chosen and the same for all calls of KASUMI. For the first sequence the output blocks were concatenated to a sequence of 1,048,576 bits. For the second sequence we built 64 sequences of 16384 bits each out of the i^{th} bits of the 16384 blocks, i.e. one sequence consisting of the first bits of all 16384 blocks, one sequence consisting of the second bits of all blocks, …, one sequence consisting of the 64^{th} bits of all blocks. These 64 sequences were then concatenated again to a sequence of 1,048,576 bits.

The following statistical tests (stream cipher tests) were applied on the two sequences (for a description of most of the tests see for example ref.[17]):

- Frequency test
- Overlapping *m*-tuple test
- Gap test
- Run test
- Coupon-Collector's test
- Universal Maurer test
- Poker test
- Correlation test
- Rank test
- Linear-complexity test
- Ziv-Lempel complexity test
- Maximum-order-complexity test

The two sequences generated to verify that KASUMI destroys redundancy in the input passed all stream cipher tests, i.e. there is no indication that these sequences deviate from random behaviour.

10.4 Analysis of the encryption mode used for A5/3 and GEA3

10.4.1 Distinguishing attacks on A5/3 and GEA3

If we take into account the A5/3 and GEA3 context of operation, namely the fact that the maximum length (in 64-bit blocks) of any keystream sequence is equal to $N = 2^{13}$ blocks in the worst case, i.e. in the GPRS ~~and EGPRS~~ case, we are not aware of any distinguishing attack on A5/3 and GEA3 requiring only 2^{32} keystream blocks, due to the following facts:

- Given any fixed initial value IV = (CA,CB,CC,CD), collisions on two keystream blocks of the keystream sequence associated with IV are predictable and correspond to (i,j) pairs of blockcountervalues such that XOR of the two feedback blocks B and B' involved in the computation of keystream blocks i and j **1** be equal to $i \oplus j$. But the probability for such collisions to occur among the at most N blocks of the keystream associated with IV is less than $N^2/2.2^{-64} \approx 2^{-39}$. Thus the number of N-blocks keystream sequences required in order for such a distinguishing event to occur with a probability close to 1 is about 2^{39} - which represents more than the at most 2^{33} distinct IV values available in the GPRS ~~and EGPRS~~ case. Therefore even if an adversary is provided with the keystream sequences associated with all possible count values (i.e. $2^{33}.2^{13} = 2^{46}$ keystream blocks), the probability of such a distinguishing event remains low (about $2^{33}.2^{-39} = 2^{-6}$)

- Given any two distinct initial values IV = (CA,CB,CC,CD) and IV'= (CA',CB',CC',CD'), the prewhitening constants A and A' differ, and it becomes difficult to predict for which IV and IV' values the corresponding keystream blocks are equal. On the other hand, the observation of two equal keystream blocks (of numbers i and j) associated with two distinct IV values IV and IV' provides an adversary with an equation in the A and A' unknowns, namely the $A \oplus A'$ value: $A \oplus A' = B \oplus B' \oplus i \oplus j$ (where B and B' represent the feedback blocks associated with the keystream blocks corresponding to IV and i and IV' and j respectively). This does not represent by itself a distinguishing information, but if a sufficiently large system of such equations can be collected by an adversary, a "linear consistency test" can be applied, and the fact that inconsistencies are never detected represents a distinguishing information. An order of magnitude of the K number of distinct keystream sequences required in order for the resulting distinguishing probability to become close to 1 can be computed using the following heuristic argument. The number of pairs of colliding blocks is about $(K \cdot N)^2/2.\ 2^{-64} = K^2.2^{-39}$, and each pair of colliding blocks provides an equation of the form $A \oplus A' = B \oplus B' \oplus i \oplus j$, i.e. an equation with GF(2) coefficients in the K unknown A prewhitening constants. A consistency test on such a system is likely to provide a distinguishing information when linear dependencies among the equations are likely to exist, which can be expected to happen when the number of equations is close to the number of unknowns, i.e. when $K \approx K^2.2^{-39}$, i.e. when $K \approx 2^{39}$. Thus even if an adversary is provided with the keystream sequences associated with all possible count values ($K = 2^{33} << 2^{39}$) the probability of this second kind of distinguishing event can be expected to be low.

This analysis shows that typical types of collision-based distinguisheres seems not to produce any distinguishing attacks on the A5/3 and GEA3 keystream generator taking into account the limitations of the number of keystream blocks per keystream sequence ($N = 2^{13}$ in the worst case, i.e. GPRS ~~and EGPRS)~~ and of the number of distinct keystream sequences for the whole system ($K < 2^{33}$ for GPRS ~~and EGPRS).~~

10.5 External evaluation

The KASUMI cipher and the 3GPP f8 and f9 algorithms were analysed by three independent evaluators. Reports from these groups are included in ref. [8] together with comments the task force made to given recommendations from the groups.

The external evaluation did not reveal any flaws or security weaknesses in KASUMI or the f8 and f9 algorithms. The design was found to resist known attacks against block ciphers and the use in the f8 and f9 modes provide the necessary level of security for the intended systems.

Since A5/3 and GEA3 make use of the same underlying block cipher and the chaining mode is very similar to f8, the task force did not recommend to spend additional time and money on a formal external evaluation for this design.

---

1 The feedback block B corresponding to the blockcounter value i is defined as the zero block if i = 0, and as the i-1th keystream block if i>0.

10.6 Complexity evaluation

Independent manufacturers have tested the implementation complexity of the 3GPP confidentiality and integrity algorithms. Their finding concludes that the proposed algorithms fall within the requirements specified in section 6. A high-level realisation of KASUMI has been conducted. The conclusion is that the circuit size is manageable and below 3000 gates. The similarity between the use of KASUMI in 3GPP and in GSM/ECSD~~DGE~~/GPRS~~/EGPRS~~ means that A5/3 and GEA3 will meet the required implementation complexity as well.

11 Quality control

11.1 Algorithm approval

Prior to the release of the A5/3 and GEA3 algorithm specification and test data, the following approvals were gained:

- All members of the ETSI SAGE A5/3 Task Force stated that they have reviewed the technical and security related aspects of the A5/3 and GEA3 algorithms and confirmed that the specifications meet all requirements found in "Requirements Specification for the GSM A5/3 Encryption Algorithm (Version 2.0 final)", ref.[2].

- All members of the ETSI SAGE A5/3 Task Force approved the release of the A5/3 and GEA3 algorithm specifications and the test data to the Algorithm Design Authority (ETSI MCC).

11.2 Specification testing

In addition to peer reviews by the ETSI SAGE A5/3 Task Force, one of the companies involved has been assigned a dedicated task of "Specification Testing". This process involves careful review of the specifications by experts outside the Task Force with regard to the technical content, readability and the editorial presentations. The written contribution from this activity has been incorporated in the final documents.

11.3 Independent implementations

Based on the Algorithm Specification documents, ref.[3] and [7], two different companies represented in the Task Force have produced two independent implementations of the A5/3 and GEA3 algorithms. Both parties have used their implementation for simulations confirming the test data found in Document 2: Implementors' Test Data, ref. [4] and Document 3: "Design Conformance Test data", ref.[5].

11.4 Test data documents

The Task Force has produced two test data documents:

- Document 2: Implementors' Test Data, ref. [4]. This document contains detail simulations for the blockcipher KASUMI , A5/3 for GSM, A5/3 for ECSD~~DGE~~ and GEA3 for GPRS~~ and EGPRS~~. The document gives corresponding input/output values for all the component functions of KASUMI during the 8 rounds. A specific repetition test is included to check that all entries in both S-boxes have been tested. For each of the three applications the document provide detail simulations corresponding to the actual parameters and block sizes of data. This document is intended for implementors who need intermediate values to verify their implementation and correct errors.

- Document 3: "Design Conformance Test data", ref.[5]. This document provides sets of input/output test data for 'black box' testing of self-contained implementations of A5/3 (GSM and ECSD~~DGE~~) and GEA3 (GPRS~~ and EGPRS~~). These tests could be used to develop power-up and maintenance tests proving correctness of the algorithm operation.

11.5 Algorithms distribution procedures

In this case the distribution procedures and related documents were not produced by the ETSI SAGE Task Force; they are the joint responsibility of the ETSI Mobile Competence Centre and the GSM Association. The ETSI SAGE A5/3 Task Force did not draft nor reviewed any distribution procedures or related documents.

Annex A:
External references

NOTE: Not all references in this list are directly referred by this report. However, they contain information that are of relevance to the reading and understanding of the details. They are referred by the more detailed 3GPP report ref. [8].

[11] 3G TS 25.321 V3.0.0: 3rd Generation Partnership Project; Technical Specification Group (TSG) RAN; Working Group 2 (WG2); MAC protocol specification.

[12] S. Ar, R.J. Lipton, R. Rubinfeld, and M. Sudan, "Reconstructing algebraic functions from mixed data", *SIAM J. of Comput.*, Vol. 28, No. 2, 1998, pp 487-510.

[13] E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials*, Technical Reports of the Computer Science Department in the Technion, 0947.

[14] Hans Dobbertin, Almost Perfect nonlinear Power Functions on GF(2^n): The Welch case, *IEEE Transactions on Information Theory*, Vol. 45, NO.4, May 1999

[15] T. Jakobsen, *High-Order Cryptanalysis of Block Ciphers*,PhDThesis, Department of Math., Technical University of Denmark, 1999.

[16] L. Knudsen, *Truncated and Higher Order Differentials*, Fast Software Encryption - Second International Workshop, Leuven, Belgium, LNCS 1008, Springer Verlag, 1995, pp. 196-211.

[17] Donald E. Knuth, *The Art of Computer Programming, Volume 2, Seminumerical Algorithms*, Addision-Wesley, Third Edition, 1998

[18] A.G. Konheim, Cryptography, a primer , NY, John Wiley & Sons, 1981.

[19] X. Lai. *Higher order derivatives and differential cryptanalysis*, In Proc. "Symposium on Communication, Coding and Cryptography" in honour of James L. Masseyon the occasion of his 60'th birthday, Feb. 10-13, 1994, Monte – Verita, Ascona, Switzerland, 1994.

[20] S. K. Langford and M. E. Hellman, *Differential – Linear Cryptanalysis*, Advances in Cryptology – CRYPTO '94, in Lecture Notes in Computer Science 839, Springer, pp. 17-25.

[21] Mitsuru Matsui: *New Block Encryption Algorithm MISTY*, Proceedings of Fast Software Encryption '97 conference, in Lecture Notes in Computer Science 1267, Springer, pp. 54-68.

[22] Willi Meier, Othmar Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, EUROCRYPT' 89

[23] A. Menezes, P.C. van Oorschot, S.A Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[24] Kaisa Nyberg, *Differential uniform mappings for cryptography*, EUROCRYPT' 93. Lecture Notes in Computer Science 765, Springer Verlag, 1993

[25] K.Nyberg and L. Knudsen, *Provable Security Against a Differential Attack*, Journal of Cryptology Vol 8 Nr 1, 1995

[26] S. Luck, *On the Security of the 128-Bit Block Cipher DEAL*, http://th.informatik.uni-mannheim.de/m/lucks/papers/deal.ps.gz

[27] Rainer A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer, 1986

[28] SSLeay source, ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL (1999), see also http://www.cryptsoft.com/ssleay/faq.html (1999)

[29] M. Sudan, *Decoding of Reed-Solomon codes beyond the error-correction bound*, Journal of Complexity, Vol. 13, 1997, pp 180-193.

[30] M. Sugita: *Higher Order Differential Attack on Block Cipher MISTY1*, 2". Technical Report of IEICE, ISEC98-4, May 1998.

[31] Hidema Tanaka, Kazuyuki Hisamatsu and Toshinobu Kaneko*: "Strength of MISTY1 without FL function for Higher Order Differential attack*". The 3rd World Multiconference on Systemic Cybernetics and Informatics and the International Conference on Information Systems Analysis and Synthesis SCI'99/ISAS'99, Orlando, USA, August 1999.

[32] TSG SA WG3#5: Liaison Statement to SA3 on Ciphering Algorithm Requirements by RAN WG2

[33] D. Wagner, *The Boomerang Attack*, FSE '99, Lecture Notes in Computer Science 1636, Springer Verlag, 1999

[34] Wassenaar Arrangement, December 1998.

Annex B:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2002-05	-	-	-	-	ETSI SAGE first publication		SAGE V1.0
2002-07	-	-	-	-	Agreed at SA WG3 #24 for presentation to TSG SA #17 for approval. Converted into 3GPP TR format (TR 55.919) (Technically equivalent to SAGE V1.0)	SAGE V1.0	1.0.0
2002-09	SP-17	SP-020506	-	-	Approved for Release 6 - version 6.0.0	1.0.0	6.0.0