**3GPP TSG SA 3 Meeting #15**
**Washington, 12-14 September 2000**

***Document S3-000622***
*e.g. for 3GPP use the format TP-99xxx*
*or for SMG, use the format P-99-xxx*

# CHANGE REQUEST

*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

**33.909** **CR** **0xx** Current Version: 3.0.0

*GSM (AA.BB) or 3G (AA.BBB) specification number ↑* *↑ CR number as allocated by MCC support team*

| | | | | | |
|---|---|---|---|---|---|
| For submission to: | SA#9 | for approval | X | strategic | |
| *list expected approval meeting # here ↑* | | for information | | non-strategic | |

*(for SMG use only)*

*Form: CR cover sheet, version 2 for 3GPP and SMG* *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

**Proposed change affects:** (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [ ]
*(at least one should be marked with an X)*

**Source:** Vodafone

**Date:** 13 September 2000

**Subject:** Addition of information on an improved theoretical result on the resilience of the f9 function

**Work item:** Security

**Category:**
*(only one category shall be marked with an X)*

| | | |
|---|---|---|
| F | Correction | |
| A | Corresponds to a correction in an earlier release | |
| B | Addition of feature | |
| C | Functional modification of feature | |
| D | Editorial modification | X |

**Release:**

| | |
|---|---|
| Phase 2 | |
| Release 96 | |
| Release 97 | |
| Release 98 | |
| Release 99 | X |
| Release 00 | |

**Reason for change:** After the completion of the SAGE work for the UMTS Confidentiality (f8) and Integrity (f9) functions, two scientists obtained an improved theoretical research result on the resilience of the f9 function. Though the result does not affect the practical security of f9, some minor changes are made to the public evaluation report to deal with the result.

**Clauses affected:**

**Other specs Affected:**

| | | |
|---|---|---|
| Other 3G core specifications | | → List of CRs: |
| Other GSM core specifications | | → List of CRs: |
| MS test specifications | | → List of CRs: |
| BSS test specifications | | → List of CRs: |
| O&M specifications | | → List of CRs: |

**Other comments:**

help.doc

<--------- double-click here for help and instructions on how to create a CR.

# Foreword

This Report has been produced by ETSI SAGE Task Force for the design of the Standard 3GPP Confidentiality and Integrity Algorithms (SAGE TF 3GPP).

The work described in this report was undertaken in response to a request made by 3GPP.

Version 1 of this report was submitted to the 3GPP SA3 group in December 1999.

In August 2000 a version 1.1 was issued. This addressed a new result on the evaluation of the f9 mode (see section 9.4.2. of this report) and also showed the correct use of the Direction bit in the f9 mode.

## On the Construction of f9

If a regular CBC-MAC mode had been chosen for the f9 algorithm, the internal state fed forward from block to block would have been only 64 bits long. In this case a $2^{33}$-message birthday attack would be likely to yield an internal state coincidence. Having identified a pair ($m_i$, $m_j$) for which such a coincidence occur, you can always be sure that $m_i||x$ and $m_j||x$ have the same MAC for any extension $x$. In other words, if you can obtain the MAC for $m_i||x$, then you can forge the MAC for $m_j||x$.

This attack would be unrealistic in the 3GPP context, but nevertheless the current f9 construction has been chosen over the regular CBC-MAC mode because it provides a 128-bit internal state at almost no extra cost. The f9 construction prevents the $2^{33}$-message birthday attack, seemingly without introducing any other weaknesses. The straightforward birthday attack on this construction requires ~~$2^{65}$ chosen-~~2^65 chosen-texts, which is completely out of reach. A variation on the birthday attack found by Knudsen and Mitchell [14a] requires approximately $2^{48}$ chosen-texts, which is still considerably more than for the regular CBC-MAC mode.

The following observations can be made on f9; none of these seem to present any security weakness.

- A change in a single block will no longer change the MAC with probability one (except for the last block), This property is satisfied by standard CBC-MAC, but not by f9.
- For every value of the $x$ of the chaining variable, there exists an input block $y$ such that the output again is $x$. Note that both $x$ and $y$ are completely unknown, and both values depend on the value of the integrity key. Then inserting the block $y$ an even number of times will not affect the MAC value.
- As a special case of the previous fact, if $x$ = 0, which is an event with probability $2^{-64}$ (that cannot be detected easily by an opponent), inserting $y$ (which again is hard to find) an arbitrary number of times will not affect the MAC value.

# Annex A - External references


[1] 3G TS 25.321 V3.0.0: 3rd Generation Partnership Project; Technical Specification Group (TSG) RAN; Working Group 2 (WG2); MAC protocol specification.

[2] 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.

[3] 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.

[4] 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

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

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

{14a] L. Knudsen, C Mitchell, *An analysis of the 3gpp-MAC scheme, private communication*, May 25, 2000

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

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

[9] 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.

[10] 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.

[11] 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.

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

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

[14] Kaisa Nyberg, *Differential uniform mappings for cryptography*, EUROCRYPT' 93.

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

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

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

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

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

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

[21] 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.

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

[23] D. Wagner, *The Boomerang Attack*, FSE '99, to appear.

[24] Wassenaar Arrangement, December 1998.