ETSI TR 135 909 V13.0.0 (2016-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
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
(3GPP TR 35.909 version 13.0.0 Release 13)

Reference
RTR/TSGS-0335909vd00

Keywords
LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Abbreviations 7
4 Structure of this report 8
5 Background to the design and evaluation work 8
6 Summary of algorithm requirements 9
6.1 General requirements for 3GPP cryptographic functions and algorithms 9
6.2 Authentication and key agreement functions 9
6.2.1 Implementation and operational considerations 9
6.2.2 Type of algorithm 9
6.2.2.1 f1 9
6.2.2.2 f1* 10
6.2.2.3 f2 10
6.2.2.4 f3 10
6.2.2.5 f4 10
6.2.2.6 f5 10
6.2.2.7 f5* 10
7 Design criteria 11
7.1 Cryptographic Criteria 11
7.2 Implementation Criteria 11
7.3 The need for an Operator Variant Algorithm Configuration Field 11
7.4 Criteria for the cryptographic kernel 11
7.4.1 Implementation and operational considerations 12
7.4.2 Functional requirements 12
7.4.3 Types and parameters for the kernel 12
8 The 3GPP MILENAGE algorithms 13
9 Rationale for the chosen design 13
9.1 Block ciphers vs. hash functions 13
9.2 The choice of Rijndael 14
9.3 The MILENAGE architecture 15
9.3.1 Use of OP 15
9.3.2 Rotations and constants 15
9.3.3 Protection against side-channel attacks 15
9.3.4 The number of kernel operations 15
9.3.5 Mode of operation 15
10 Evaluation 16
10.1 Evaluation criteria 16
10.2 Operational Context 17
10.3 Analysis 17
10.3.1 A formal proof of the soundness of the f2-f5* construction 17
10.3.2 On the f1-f1* construction and its separation from f2-f5* 19
10.3.2.1 Soundness of the f1-f1* construction 19
10.3.2.2 Separation between f1-f1* and f2-f5* 19

10.3.3 Investigation of forgery or distinguishing attacks with 2^{64} queries 20
10.3.3.1 An internal collision attack against f1 (or f1*) 20
10.3.3.2 Forgery or distinguishing attacks against combinations of several modes 20
10.3.3.2.1 Attacks against combinations of f2-f5 21
10.3.3.2.2 Attacks against combinations of f1-f1* and f2-f5* 21
10.3.3.3 Conclusion about the identified forgery or distinguishing attacks 21
10.4 Statistical evaluation 22
10.5 Published attacks on Rijndael 22
10.6 Complexity evaluation 23
10.6.1 Complexity of draft Rijndael implementation 23
10.6.2 Estimate complexity of modes 23
10.6.3 Estimate of total MILENAGE 23
10.6.4 SPA/DPA, Timing attack countermeasures 23
10.6.5 Conclusion on algorithm complexity 24
10.7 External complexity evaluations 24
10.8 Evaluation of side channel attacks 25
10.8.1 Evaluation of the kernel algorithm 25
10.8.1.1 Timing Attacks 25
10.8.1.2 Simple Power Analysis 25
10.8.1.3 Differential Power Analysis 25
10.8.1.4 Other side channels 26
10.8.2 Evaluation of the f1-f5 modes 26
10.8.2.1 Operator Constants (OP or OPc) 26
10.8.2.2 Rotations and constants 26
10.8.3 Conclusion on side channel attacks 26

11 Conclusions 27

Annex A (informative): Change history 28

History 29

Foreword

This Technical Report (TR) 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 172 on the design of an example set for 3GPP Authentication and Key Generation Algorithms.

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

SAGE Version 1.0 of this report was submitted to the 3GPP SA WG3 group in December 2000. Version 1.1 (with updated C-code in Annex 4) was approved by TSG SA#10 in December 2000.

1 Scope

This report contains a detailed summary of the work performed during the design and evaluation of the 3GPP Authentication Functions denoted as the MILENAGE algorithm set. It contains all results and findings from this work and should be read as a supplement to the specifications of the algorithms in ref. [3] and the general project report, ref. [4].

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] 3G TS 33. 102 V 3.5.0 (2000-07) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture.

[2] 3G TS 33. 105 V 3.4.0 (2000-07) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements. (Release 1999)

[3] ETSI/SAGE Specification. 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 1: Algorithm Specification. Version: 1.0; Date: 22nd November 2000.

[4] ETSI/SAGE Report. Report on the Design and Evaluation of the 3GPP Authentication and Key generation Functions; Version: 1.0; Date: 22nd November 2000.

[5] Wassenaar Arrangement, December 1998. http://www.wassenaar.org.

[6] P. C. Kocher, 'Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems', *CRYPTO'96, LNCS 1109*, Springer-Verlag, 1996, pp. 104-113.

[7] J. Kelsey, B. Schneier, D. Wagner, C. Hall, Side Channel Cryptanalysis of Product Ciphers', *ESORICS'98, LNCS 1485*, Springer-Verlag, 1998, pp. 97-110.

[8] L. Goubin, J. Patarin, 'DES and differential power analysis', *CHES'99, LNCS 1717*, Springer-Verlag, 1999, pp. 158-172

[9] P. Kocher, J. Jaffe, B. Jun, 'Differential Power Analysis', *CRYPTO'99, LNCS 1666*, Springer-Verlag, 1999, pp. 388-397.

[10] T. S. Messerges, 'Securing the AES finalists against Power Analysis Attacks', *FSE'00, LNCS*, Springer-Verlag, to appear.

[11] L. Goubin, J.-S. Coron, 'On boolean and arithmetic masking against differential power analysis,' *CHES'00, LNCS*, Springer-Verlag, to appear.

[12] Nechvatal, Barker, Bassham, Burr, Dworkin, Foti and Roback, 'Report on the Development of the Advanced Encryption Standard (AES)', NIST, October 2, 2000.

[13] F. Sano, M. Koike, S. Kawamura and M. Shiba, 'Performance evaluation of AES Finalists on the High-End Smart Card', The Third AES Candidate Conference, New York, April 2000.