ETSI TS 135 233 V15.0.0 (2018-07)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
LTE;
Specification of the TUAK algorithm set:
A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*;
Document 3: Design conformance test data
(3GPP TS 35.233 version 15.0.0 Release 15)

Reference

RTS/TSGS-0335233vf00

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) 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

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

The present document is third of three, which between them form the entire specification of the example algorithms, entitled:

- 3GPP TS 35.231: "Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation Functions f1, f1*, f2, f3, f4, f5 and f5*;
  Document 1: algorithm specification ".
- 3GPP TS 35.232: "Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation Functions f1, f1*, f2, f3, f4, f5 and f5*;
  Document 2: Implementers' test data".
- **3GPP TS 35.233: " Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*;
  Document 3: Design conformance test data".**

1 Scope

The present document and the other Technical Specifications in the series, TS 35.231 [4] and TS 35.232 [5], contain an example set of algorithms which could be used as the authentication and key generation functions ***f1***, ***f1****, ***f2***, ***f3***, ***f4***, ***f5*** and ***f5**** for 3GPP systems. The present document provides sets of input/output test data for 'black box' testing of physical realizations of all algorithms, and in particular:

- Test data for the Keccak permutation used within Tuak.
- Test data for the MILENAGE authentication and key generation algorithms *f1, f1*, f2, f3, f4, f5* and *f5**.

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] 3GPP TS 33.102: "3G Security; Security Architecture".

[2] 3GPP TS 35.206: "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 2: Algorithm specification".

[3] "The KECCAK Reference", version 3.0, 14 January 2011, G. Bertoni, J. Daemen, M. Peeters, G. van Aasche.

[4] 3GPP TS 35. 231: "Specification of the Tuak Algorithm Set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: algorithm specification ".

[5] 3GPP TS 35. 232: "Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Implementers' test data"

[6] 3GPP TS 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture".

3 Definitions

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Tuak: The name of this algorithm set is "Tuak". It should be pronounced like "too-ack".

3.2 Symbols

For the purposes of the present document, the following symbols apply:

AK	a 48-bit anonymity key that is the output of either of the functions f5 and f5*
AMF	a 16-bit authentication management field that is an input to the functions f1 and f1*

CK	a 128-bit or 256-bit confidentiality key that is the output of the function f3
IK	a 128-bit or 256-bit integrity key that is the output of the function f4
IN	a 1600-bit value that is used as the input to the permutation Π when computing the functions f1, f1*, f2, f3, f4, f5 and f5*
K	a 128-bit or 256-bit subscriber key that is an input to the functions f1, f1*, f2, f3, f4, f5 and f5*
MAC-A	a 64-bit, 128-bit or 256-bit network authentication code that is the output of the function f1
MAC-S	a 64-bit, 128-bit or 256-bit resynchronization authentication code that is the output of the function f1*
TOP	a 256-bit Operator Variant Algorithm Configuration Field that is a component of the functions f1, f1*, f2, f3, f4, f5 and f5*
TOPC	a 256-bit value derived from TOP and K and used within the computation of the functions
OUT	a 1600-bit value that is taken as the output of the permutation Π when computing the functions f1, f1*, f2, f3, f4, f5 and f5*
RAND	a 128-bit random challenge that is an input to the functions f1, f1*, f2, f3, f4, f5 and f5*
RES	a 32-bit, 64-bit, 128-bit or 256-bit signed response that is the output of the function f2
SQN	a 48-bit sequence number that is an input to either of the functions f1 and f1*. (For f1* this input is more precisely called SQNMS) See informative Annex C of [1] for methods of encoding sequence numbers.

3 Definitions

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Tuak: The name of this algorithm set is "Tuak". It should be pronounced like "too-ack".

3.2 Symbols

For the purposes of the present document, the following symbols apply:

AK	a 48-bit anonymity key that is the output of either of the functions f5 and f5*
AMF	a 16-bit authentication management field that is an input to the functions f1 and f1*
CK	a 128-bit or 256-bit confidentiality key that is the output of the function f3
IK	a 128-bit or 256-bit integrity key that is the output of the function f4
IN	a 1600-bit value that is used as the input to the permutation Π when computing the functions f1, f1*, f2, f3, f4, f5 and f5*
K	a 128-bit or 256-bit subscriber key that is an input to the functions f1, f1*, f2, f3, f4, f5 and f5*
MAC-A	a 64-bit, 128-bit or 256-bit network authentication code that is the output of the function f1
MAC-S	a 64-bit, 128-bit or 256-bit resynchronization authentication code that is the output of the function f1*
TOP	a 256-bit Operator Variant Algorithm Configuration Field that is a component of the functions f1, f1*, f2, f3, f4, f5 and f5*
TOPC	a 256-bit value derived from TOP and K and used within the computation of the functions
OUT	a 1600-bit value that is taken as the output of the permutation Π when computing the functions f1, f1*, f2, f3, f4, f5 and f5*
RAND	a 128-bit random challenge that is an input to the functions f1, f1*, f2, f3, f4, f5 and f5*
RES	a 32-bit, 64-bit, 128-bit or 256-bit signed response that is the output of the function f2
SQN	a 48-bit sequence number that is an input to either of the functions f1 and f1*. (For f1* this input is more precisely called SQNMS) See informative Annex C of [1] for methods of encoding sequence numbers.

4 Preliminary information

4.1 Introduction

Within the security architecture of the 3GPP system there are seven security functions ***f1***, ***f1****, ***f2***, ***f3***, ***f4***, ***f5*** and ***f5****. The operation of these functions falls within the domain of one operator, and the functions are therefore to be specified by each operator rather than being fully standardized. The algorithms specified in the present document are examples that may be used by an operator who does not wish to design his own.

The inputs and outputs of all seven algorithms are defined in clause 4.4.

4.2 Radix

Unless stated otherwise, all test data values presented in the present document are in hexadecimal.

4.3 Bit/Byte ordering for Tuak inputs and outputs

3GPP TS 33.102 [1] includes the following convention. (There is similar text in the specification of MILENAGE, as defined in 3GPP TS 35.206 [2]):

All data variables in the present document are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bit string. Where a variable is broken down into a number of substrings, the left-most (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

So, for example, RAND[0] is the most-significant bit of RAND and RAND[127] is the least significant bit of RAND.

This convention applies to all **inputs** and **outputs** to Tuak, as listed in tables 1-9 below.

However, when describing intermediate states of Tuak (e.g. inputs and outputs for the Keccak permutation), variables are simply treated as indexed bit strings. These bit strings will be presented in hexadecimal notation, using a display convention described in clause5.2 .

4.4 Tuak inputs and outputs

The inputs to Tuak are given in tables 1 and 2, the outputs in tables 3 to 9 below.

There are a few differences from the inputs and outputs to MILENAGE [2].

The key K may be 128 bits **or** 256 bits. MAC-A and MAC-S may be 64, 128 **or** 256 bits. RES may be 32, 64, 128 **or** 256 bits. CK and IK may be 128 **or** 256 bits. Existing 3GPP specification (see [1] and [7]) do not support all these possibilities, but they are included in Tuak for future flexibility in case future releases of these specifications support them.

NOTE 1: The 3G security architecture specification [1] calls the output of the f1 function 'MAC' while the present document and [2] call it 'MAC-A'.

Any sizes for the parameters K, MAC-A, MAC-S, RES, CK and IK mentioned in the present document shall not be supported nor used in entities defined in 3GPP specifications until these specifications explicitly allow their use.

In any particular implementation, the parameters shall have a fixed length, chosen in advance. For example an operator may fix K at length 256 bits, RES at length 64 bits, CK and IK at length 128 bits. As the lengths do not vary with input, they are not specified as formal input parameters.

Table 1: Inputs to *f1* and *f1**

Parameter	Size (bits)	Comment
K	128 or 256	Subscriber key K[0]…K[127] or K[0]…K[255]
RAND	128	Random challenge RAND[0]…RAND[127]
SQN	48	Sequence number SQN[0]…SQN[47] (for ***f1**** this input is more precisely called SQN_{MS})
AMF	16	Authentication management field AMF[0]…AMF[15]

Table 2: Inputs to *f2*, *f3*, *f4*, *f5* and *f5**

Parameter	Size (bits)	Comment
K	128 or 256	Subscriber key K[0]…K[127] or K[0]…K[255]
RAND	128	Random challenge RAND[0]…RAND[127]

Table 3: *f1* output

Parameter	Size (bits)	Comment
MAC-A	64, 128 or 256	Network authentication code MAC-A[0]…MAC-A[63] or MAC-A[0]…MAC-A[127] or MAC-A[0]…MAC-A[255]

Table 4: *f1 output**

Parameter	Size (bits)	Comment
MAC-S	64, 128 or 256	Resynch authentication code MAC-S[0]…MAC-S[63] or MAC-S[0]…MAC-S[127] or MAC-S[0]…MAC-S[255]

Table 5: *f2* output

Parameter	Size (bits)	Comment
RES	32, 64, 128 or 256	Response RES[0]…RES[31] or RES[0]…RES[63] or RES[0]…RES[127] or RES[0]…RES[255]

Table 6: *f3* output

Parameter	Size (bits)	Comment
CK	128 or 256	Confidentiality key CK[0]…CK[127] or CK[0]…CK[255]

Table 7: *f4* output

Parameter	Size (bits)	Comment
IK	128 or 256	Integrity key IK[0]…IK[127] or IK[0]…IK[255]

Table 8: *f5* output

Parameter	Size (bits)	Comment
AK	48	Anonymity key AK[0]…AK[47]

Table 9: *f5 output**

Parameter	Size (bits)	Comment
AK	48	Resynch anonymity key AK[0]…AK[47]

NOTE 2: Both f5 and f5* outputs are called AK according to [1]. In practice only one of them at a time will be calculated in any given call to the authentication and key agreement algorithms.

5 Conformance test data for KECCAK

5.1 Overview

The test data sets presented here are for the cryptographic permutation Keccak-f[1600], as it is specified in [3], and used within [4]. This permutation is abbreviated as Π, and use strings **IN**[0] .. **IN**[1599] and **OUT**[0] .. **OUT**[1599] to represent the input and output of Π.

The following test sets are the same as in [5].

5.2 Format

For brevity, the **IN** and **OUT** strings will be presented as lists of 200 bytes (octets), with each individual byte written separately in hexadecimal notation. The lists of bytes should be read from left to right, and then from top to bottom.

For **IN**, the first byte of the list will denote the bits **IN**[0] to **IN**[7], with **IN**[0] equal to the *least* significant bit of the corresponding hexadecimal number equal to and **IN**[7] equal to the *most* significant bit of the same hexadecimal number. The final byte of the list will denote **IN**[1592] to **IN**[1599], with **IN**[1592] equal to the *least* significant bit of the corresponding hexadecimal number, and **IN**[1599] equal to the *most* significant bit of the same number.

OUT strings will be presented in the same way.

As an example, in Test Set 1 below:

```
IN[0] = 0,  IN[1] = 0,  IN[2] = 1,  IN[3] = 0,  IN[4] = 0,  IN[5] = 1,  IN[6] = 0,  IN[7] = 0,
IN[8] = 0,  IN[9] = 1,  IN[10]=1,  IN[11]=0,  IN[12]=1,  IN[13]=1,  IN[14]=1,  IN[15]=0, … ,
IN[1584]=1, IN[1585]=1, IN[1586]=0, IN[1587]=1, IN[1588]=0, IN[1589]=0, IN[1590]=0, IN[1591]=0,
IN[1592]=0, IN[1593]=0, IN[1594]=0, IN[1595]=0, IN[1596]=1, IN[1597]=0, IN[1598]=1, IN[1599]=0.

OUT[0] = 1, OUT[1] = 1, OUT[2] = 1, OUT[3] = 1, OUT[4] = 0, OUT[5] = 1, OUT[6] = 0, OUT[7] = 0,
OUT[8] = 0, OUT[9] = 0, OUT[10]=1, OUT[11]=1, OUT[12]=1, OUT[13]=0, OUT[14]=1, OUT[15]=1, … ,
OUT[1584]=0, OUT[1585]=1, OUT[1586]=1, OUT[1587]=1, OUT[1588]=1,OUT[1589]=0,OUT[1590]=0,
OUT[1591]=0, OUT[1592]=1, OUT[1593]=1, OUT[1594]=1,OUT[1595]=0,OUT[1596]=0, OUT[1597]=1,
OUT[1598]=0, OUT[1599]=1.
```

5.3 Test set 1

```
IN:
24 76 d2 da c5 9e 2e 93 49 df 32 55 a9 da b1 b6 9e b5 c2 08 f1 51 c7 30 9e 8c 8f 17 db 45 6d 0b 5e
b0 af b6 c7 3e 37 ce 8c cc cf 20 b7 9d 8a 67 29 41 49 17 48 09 e4 29 70 93 30 c4 ad 23 1d 3e 52 11
ae 0b d8 05 20 c4 3a d4 b4 36 62 57 92 a7 6c 52 08 9d 0f 73 92 71 15 1a 37 59 4d f6 6d e4 42 9f 3c
97 0a 34 56 b6 ce 2c 78 cd 11 28 71 7f 4b db 73 1a 4c 97 db e5 eb 73 53 fe 81 e3 7c 33 ac 60 b8 21
22 ea c6 11 a9 8e 0e 74 42 b9 99 64 75 22 93 e4 f9 c6 96 ba 05 f0 7a 21 45 1f 90 73 0c 96 78 c6 45
ad 4b e4 4c 4d 2d 98 1a 34 12 08 1c 9c 6b 05 c9 93 ff 1c 56 1a 0d 24 2b 47 06 d5 01 c3 47 65 b3 7a
0b 50

OUT:
2f dc 58 d4 d9 4a 88 4c 1c b0 3a 8e 63 ac ab 83 75 e8 56 b5 61 ba 3a 06 25 e8 30 ac db 55 73 42 86
64 6f 87 18 9b 43 54 25 b5 d6 65 4e 22 82 28 b6 97 b8 1c be ad 65 5b 71 aa cc c2 5e 3d 7e 51 b5 cb
5a c2 27 f6 7f 2a d8 a0 62 97 67 82 b0 8a 7e c3 f1 b5 38 d6 00 8c 0b ab ef 83 da 64 36 6b 62 a5 3f
88 a3 dc 06 29 bd ed 79 5f 32 20 f3 c6 5c 76 bd d0 12 43 e8 8f 63 d6 91 2e 5f b5 cd a1 67 b7 1f 9b
aa a7 42 dc 19 3f f7 8c 17 67 a3 8a 1c 96 40 8c ce 16 92 39 b0 77 f2 90 3a 07 b8 c4 6a 04 8d 66 31
8e 59 5e a4 bb 92 99 2c 7c 2d 3d cd 38 19 75 b6 e0 5f 85 ba 18 15 20 96 cc 30 ed 22 14 0f f3 b6 71
1e a7
```

5.4 Test set 2

IN:

```
80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00
```

OUT:

```
44 e0 e5 8c a9 68 97 5c 4c 25 92 a1 57 f5 3f 21 24 51 9b 01 0b 89 e1 5e 30 1e f5 8f 76 50 1d b5 9c
de 06 7f 1f de 09 c0 a4 b5 c2 10 a6 a1 9f 06 ba 4c 8f 0c 6f c8 68 f0 fc 80 a6 3b 25 53 79 1e 41 c8
22 78 ad 11 5e fc 70 f7 1d 64 1f f0 77 4a a5 d5 47 b6 d9 91 49 14 02 2c 51 4c 45 fc ec a6 1c b6 6b
0f 03 13 e3 49 88 ae 0d 36 73 7e 2c 05 29 90 7f e6 53 fc 4e 18 5d 07 f3 96 1f 82 6b b8 80 31 af 84
4d 9e 7d 98 76 17 03 63 fd e7 67 86 c5 8c cb cf 5c 3a 01 bb 91 4c 1b 02 08 a2 7c 7b e3 bb bb bb 99
76 e0 40 31 7a fc 2a fb fa dc 7b a7 fc 23 72 35 c6 55 51 aa 31 39 64 1f a8 db 2e 64 83 f2 87 40 b3
1b 61
```

5.5 Test set 3

```
IN:
01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42
43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63
64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84
85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5
a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6
c7 c8

OUT:
5d d0 e3 dd 9e 46 db 21 87 a9 e1 a4 44 42 7d 7a 83 2f ef 29 91 39 90 e0 15 ea 8d 1f 3f 1f a6 41 3f
fb bc 58 6f 5a 4d 69 4d d6 06 68 fb f3 b4 bb da 49 45 c9 ea 0c be e2 11 73 5e bf a8 39 9b 61 3a ff
34 d1 dd 47 fa 39 8c 78 f4 8a 91 a6 65 7d 29 03 6c 87 f7 73 5f 43 e2 ab b7 6a 13 50 45 b7 0e 42 c5
9d 80 92 14 a4 cd 30 1f 18 57 30 0a 55 d0 1d 32 36 5b 6a bd a5 1e ad 75 41 db 7b ed dc 46 e4 85 72
7c 3b 2b 5d 83 b5 9e 5a 7a 62 e0 13 16 14 ba 0d 7b fa cd 4e ba 71 62 32 80 88 59 f0 03 85 5f 5c 47
01 0a 50 e1 26 2f 9e 9e 81 2e 6c b3 dd 52 d9 ad b7 be 19 10 42 76 34 02 52 31 96 8d e0 b4 3f a2 4b
4b 3e
```

5.6 Test set 4

```
IN:
ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab
ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab
ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab
ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab
ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab
ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab ab
ab ab

OUT:
00 52 f0 0e b4 09 b5 ce 5f 78 e9 53 20 ee 6a 71 5f 5b 1a 0a 7e 5b ed 03 43 d6 91 13 30 ab e2 fc 57
b6 6f b5 ba 9e f2 88 0b 05 75 ed 0a 98 70 c5 0c 66 57 83 8a 1d 32 f3 88 fd c3 a4 e7 32 46 dd d9 56
58 74 77 c4 c8 d4 1a d4 19 14 04 52 cc 17 13 23 ae 1f f0 91 0c e1 c3 27 8b 62 c6 48 75 91 2b 7f 7c
21 cf a0 52 e0 b0 40 21 4c 5f 3b 81 c3 20 75 87 92 ce a0 c8 d1 e4 2e 92 e1 ef 3c f0 66 be 16 c6 1e
e4 4d dd 69 db 72 9a 82 5d 4d bb fd 9f 97 da 46 c6 10 3d 5a 5f 8c 8d 21 bd 42 7d 58 af 4b 41 11 78
be de 5a 19 86 a0 c9 1d 38 c4 85 ee 2d 54 72 bd d0 a5 b9 fa ab f7 07 73 13 ca f9 f3 0a 1e 46 ac 8e
12 58
```

5.7 Test set 5

```
IN:
cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
cd cd

OUT:
c1 6c a0 6d ef 3a dd 45 b2 0c cf d6 7a a8 f9 12 15 c2 e8 75 1e dd 02 a5 10 3f 61 ba 6f 7b f3 bb b2
59 5f 41 1b af 6a ab 16 53 f1 7e 95 1e 2d c8 8d fb f7 68 67 94 0a 63 38 60 82 18 f8 df f1 41 7b db
3c 6f 45 22 64 87 a9 a6 07 8b 65 6a 37 ff 86 1d fa 79 30 77 c0 88 03 a8 b9 62 da 67 24 dd c8 6d 10
93 ff d0 05 88 a2 8e 6c 1b 80 1f 73 54 63 bc 05 58 1e d5 97 bd bf 37 a4 59 29 7f 65 05 39 98 9e fc
4a 7a 9c 8b 22 33 c0 20 de a3 00 34 c1 f2 c6 cf 5e 0c cc cc 53 55 40 87 18 03 ed 3d 20 b0 c5 10 13
a3 02 4a c5 6b 33 af 5a 26 11 23 3d 53 7d 11 80 4e f0 2e b5 59 78 ff d4 3d 9a 7e 48 84 42 64 de ce
8f a8
```

5.8 Test set 6

```
IN:
00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 04
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 03 00
00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 02 00 00
00 00 00 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
00 00 00 00 02 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00
00 00

OUT:
56 0d be 41 f6 a7 5a 7d 33 e1 5d 6b fe 0b dc 64 7d e5 54 34 1c e0 d0 61 bb bd f1 be 75 76 49 de e7
41 b1 fd 37 41 8d a6 f3 5a b7 0e 15 87 cc 36 8c 1b 89 ad cc ce 1d 07 ad 92 0d 4d 9d 08 a0 43 94 6c
2f 6f e1 a5 17 a2 49 ce 3c 8a 5f 83 4e ec fa 2f aa ad de e8 32 e6 db 24 d4 2a 2b 04 a7 84 63 a9 b2
df 6d 2f 02 fc 5c 29 73 2a 12 65 14 fb 15 eb 7a be 7f bf 57 18 91 66 91 c7 c2 f8 43 46 00 da 7e 2f
9b 76 65 a5 9c 61 41 11 55 05 c9 d9 e9 f8 05 af 6f 9e 6b c4 f1 9c 65 c6 0e a9 72 a6 e4 fa 01 85 7d
29 8a 09 26 83 90 d5 74 f6 3d 4f 76 fb 6d 6d fc d1 37 38 c4 98 48 ac d5 1e 4e d7 83 af a1 ba 52 0f
a3 37
```

6 Conformance test data for Tuak

6.1 Overview

The test data sets presented here are for the seven functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**. The test sets are the same as in [5].

6.2 Format

Each Test shows the various inputs to the algorithms. This is followed by the configuration field TOP and other operator configuration parameters: the length of the K, the length of the outputs MAC, CK, IK and RES, and the number of Keccak iterations. These are followed by the value of TOP_C and finally by the function outputs.

One of the test sets (set 4) is shown twice: once in hexadecimal format, and then again in binary format. This is to explicitly show the relationship between the binary data and the hexadecimal representation.

For brevity, the remainder of the test sets are presented in hexadecimal format only.

6.3 Test set 1

Input Parameters:

```
K:          abababababababababababababababab
RAND:       42424242424242424242424242424242
SQN:        111111111111
AMF:        ffff
```

Operator Configuration Parameters:

```
TOP:        5555555555555555555555555555555555555555555555555555555555555555
Klength = 128 bits, MAClength = 64 bits, CKlength = 128 bits,
IKlength = 128 bits, RESLength = 32 bits, KeccakIterations = 1
TOPc:       bd04d9530e87513c5d837ac2ad954623a8e2330c115305a73eb45d1f40cccbff
```

Output Parameters:

```
f1:         f9a54e6aeaa8618d
f1*:        e94b4dc6c7297df3
f2:         657acd64
f3:         d71a1e5c6caffe986a26f783e5c78be1
f4:         be849fa2564f869aecee6f62d4337e72
f5:         719f1e9b9054
f5*:        e7af6b3d0e38
```

6.4 Test set 2

Input Parameters:

```
K:          fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0efeeedecebeae9e8e7e6e5e4e3e2e1e0
RAND:       0123456789abcdef0123456789abcdef
SQN:        0123456789ab
AMF:        abcd
```

Operator Configuration Parameters:

```
TOP:        808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
Klength = 256 bits, MAClength = 128 bits, CKlength = 128 bits,
IKlength = 128 bits, RESLength = 64 bits, KeccakIterations = 1
TOPc:       305425427e18c503c8a4b294ea72c95d0c36c6c6b29d0c65de5974d5977f8524
```

Output Parameters:

```
f1:         c0b8c2d4148ec7aa5f1d78a97e4d1d58
f1*:        ef81af7290f7842c6ceafa537fa0745b
f2:         e9d749dc4eea0035
f3:         a4cb6f6529ab17f8337f27baa8234d47
f4:         2274155ccf4199d5e2abcbf621907f90
f5:         480a9345cc1e
f5*:        f84eb338848c
```

6.5 Test set 3

Input Parameters:

```
K:          fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0efeeedecebeae9e8e7e6e5e4e3e2e1e0
RAND:       0123456789abcdef0123456789abcdef
SQN:        0123456789ab
AMF:        abcd
```

Operator Configuration Parameters:

```
TOP:        808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
Klength = 256 bits, MAClength = 256 bits, CKlength = 128 bits,
IKlength = 256 bits, RESLength = 64 bits, KeccakIterations = 1
TOPc:       305425427e18c503c8a4b294ea72c95d0c36c6c6b29d0c65de5974d5977f8524
```

Output Parameters:

```
f1:         d97b75a1776065271b1e212bc3b1bf173f438b21e6c64a55a96c372e085e5cc5
f1*:        427bbf07c6e3a86c54f8c5216499f3909a6fd4a164c9fe235b1550258111b821
f2:         07021c73e7635c7d
f3:         4d59ac796834eb85d11fa148a5058c3c
f4:         126d47500136fdc5ddfd14f19ebf16749ce4b6435323fbb5715a3a796a6082bd
f5:         1d6622c4e59a
f5*:        f84eb338848c
```

6.6 Test set 4

Hexadecimal Format

Input Parameters:

```
K:          b8da837a50652d6ac7c97da14f6acc61
RAND:       6887e55425a966bd86c9661a5fa72be8
SQN:        0dea2ee2c5af
AMF:        df1e
```

Operator Configuration Parameters:

```
TOP:        0952be13556c32ebc58195d9dd930493e12a9003669988ffde5fa1f0fe35cc01
Klength = 128 bits, MAClength = 128 bits, CKlength = 128 bits,
IKlength = 128 bits, RESLength = 128 bits, KeccakIterations = 1
TOPc:       2bc16eb657a68e1f446f08f57c0efb1d493527a2e652ce281eb6ca0e4487760a
```

Output Parameters:

```
f1:         749214087958dd8f58bfcdf869d8ae3f
f1*:        619e865afe80e382aee13063f9dfb56d
f2:         4041ce438e3e38e8aa96562eed83ac43
f3:         3e3bc01bea0cd914c4c2c83ce2d92757
f4:         666a8e6f577b1aa77b7fd53cebb8a3d6
f5:         1f880d005119
f5*:        45e617d77fe5
```

Binary Format

```
K:  10111000 11011010 10000011 01111010 01010000 01100101 00101101 01101010 11000111 11001001
01111101 10100001 01001111 01101010 11001100 01100001

RAND:    01101000 10000111 11100101 01010100 00100101 10101001 01100110 10111101 10000110 11001001
01100110 00011010 01011111 10100111 00101011 11101000

SQN:     00001101 11101010 00101110 11100010 11000101 10101111

AMF:     11011111 00011110

TOP:     00001001 01010010 10111110 00010011 01010101 01101100 00110010 11101011 11000101 10000001
10010101 11011001 11011101 10010011 00000100 10010011 11100001 00101010 10010000 00000011 01100110
10011001 10001000 11111111 11011110 01011111 10100001 11110000 11111110 00110101 11001100 00000001

TOPc:    00101011 11000001 01101110 10110110 01010111 10100110 10001110 00011111 01000100 01101111
00001000 11110101 01111100 00001110 11111011 00011101 01001001 00110101 00100111 10100010 11100110
01010010 11001110 00101000 00011110 10110110 11001010 00001110 01000100 10000111 01110110 00001010

f1: 01110100 10010010 00010100 00001000 01111001 01011000 11011101 10001111 01011000 10111111
11001101 11111000 01101001 11011000 10101110 00111111

f1*:     01100001 10011110 10000110 01011010 11111110 10000000 11100011 10000010 10101110 11100001
00110000 01100011 11111001 11011111 10110101 01101101

f2: 01000000 01000001 11001110 01000011 10001110 00111110 00111000 11101000 10101010 10010110
01010110 00101110 11101101 10000011 10101100 01000011

f3: 00111110 00111011 11000000 00011011 11101010 00001100 11011001 00010100 11000100 11000010
11001000 00111100 11100010 11011001 00100111 01010111

f4: 01100110 01101010 10001110 01101111 01010111 01111011 00011010 10100111 01111011 01111111
11010101 00111100 11101011 10111000 10100011 11010110

f5: 00011111 10001000 00001101 00000000 01010001 00011001

f5*:     01000101 11100110 00010111 11010111 01111111 11100101
```

6.7 Test set 5

Input Parameters:

```
K:          1574ca56881d05c189c82880f789c9cd4244955f4426aa2b69c29f15770e5aa5
RAND:       c570aac68cde651fb1e3088322498bef
SQN:        c89bb71f3a41
```

```
AMF:        297d
```

Operator Configuration Parameters:

```
TOP:        e59f6eb10ea406813f4991b0b9e02f181edf4c7e17b480f66d34da35ee88c95e
Klength = 256 bits, MAClength = 64 bits, CKlength = 256 bits,
IKlength = 128 bits, RESLength = 256 bits, KeccakIterations = 1
TOPc:       3c6052e41532a28a47aa3cbb89f223e8f3aaa976aecd48bc3e7d6165a55eff62
```

Output Parameters:

```
f1:         d7340dad02b4cb01
f1*:        c6021e2e66accb15
f2:         84d89b41db1867ffd4c7ba1d82163f4d526a20fbae5418fbb526940b1eeb905c
f3:         d419676afe5ab58c1d8bee0d43523a4d2f52ef0b31a4676a0c334427a988fe65
f4:         205533e505661b61d05cc0eac87818f4
f5:         d7b3d2d4980a
f5*:        ca9655264986
```

6.8 Test set 6

Input Parameters:

```
K:          1574ca56881d05c189c82880f789c9cd4244955f4426aa2b69c29f15770e5aa5
RAND:       c570aac68cde651fb1e3088322498bef
SQN:        c89bb71f3a41
AMF:        297d
```

Operator Configuration Parameters:

```
TOP:        e59f6eb10ea406813f4991b0b9e02f181edf4c7e17b480f66d34da35ee88c95e
Klength = 256 bits, MAClength = 256 bits, CKlength = 256 bits,
IKlength = 256 bits, RESLength = 256 bits, KeccakIterations = 2
TOPc:       b04a66f26c62fcd6c82de22a179ab65506ecf47f56245cd149966cfa9cec7a51
```

Output Parameters:

```
f1:         90d2289ed1ca1c3dbc2247bb480d431ac71d2e4a7677f6e997cfddb0cbad88b7
f1*:        427355dbac30e825063aba61b556e87583abac638e3ab01c4c884ad9d458dc2f
f2:         d67e6e64590d22eecba7324afa4af4460c93f01b24506d6e12047d789a94c867
f3:         ede57edfc57cdffe1aae75066a1b7479bbc3837438e88d37a801cccc9f972b89
f4:         48ed9299126e5057402fe01f9201cf25249f9c5c0ed2afcf084755daff1d3999
f5:         6aae8d18c448
f5*:        8c5f33b61f4e
```

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Dec 2013					Version after approval	1.1.0	12.0.0
Dec 2013					Update of Introduction with spec numbers	12.0.0	12.0.1
June 2014	SP-64	SP-140316	001	2	Overall editorial modification to the Tuak specification TS 35.233	12.0.1	12.1.0
2016-01	-	-	-	-	Update to Rel-13 version (MCC)	12.1.0	**13.0.0**
2017-03	SA#75	-	-	-	Promotion to Release 14 without technical change	13.0.0	**14.0.0**
2018-06	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	**15.0.0**

History

Document history		
V15.0.0	July 2018	Publication