ETSI TS 135 232 V16.0.0 (2020-08)

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 2: Implementers' test data
(3GPP TS 35.232 version 16.0.0 Release 16)

Reference
RTS/TSGS-0335232vg00

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

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.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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 second 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 35.233 [6], 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. In particular, the present document defines the test data:

- for the Keccak permutation used within Tuak,
- for the authentication algorithms *f1* and *f1**,
- for the algorithms *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, (available at http://keccak.noekeon.org/Keccak-reference-3.0.pdf).

[4] 3GPP TS 35. 231: "Specification of the Tuaka lgorithm 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 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture".

[6] 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".

[7] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [7] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [7].

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

3.2 Symbols

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 this 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 clause4.4 .

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 presentdocument 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 to 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 clause 5.2.

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 specifications (see [1] and [5]) 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 KECCAK test data

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.

5.2 Format

For brevity, the **IN** and **OUT** strings are 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 Authentication algorithms *f1* and *f1**

6.1 Overview

The test data sets presented here are for the authentication algorithms *f1, f1**. Inputs and outputs to the permutation Π are also presented here to assist with the implementation.

6.2 Format

Each test starts by showing the various inputs (K, RAND, SQN, AMF) to the functions. Next are shown the operator configuration field TOP, and other operator configuration parameters: the length of the K, the length of the output MAC, and the number of Keccak iterations.

These are followed by the value of TOP_C and then the output values of *f1* and *f1** are shown. The value TOP_C should not be computed on but off the UICC. In the example code TOP_C is computed inside the functions, so it was included in the test data.

All the input, output and configuration parameters are presented using the bit/byte ordering convention described in clause 4.3. Intermediate inputs and outputs to the permutation Π are also shown, as lists of 200 bytes, using the convention described in clause 5.2.

6.3 Test set 1

Input Parameters:

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

Operator Configuration Parameters:

```
TOP:       55555555555555555555555555555555555555555555555555555555555555555555555555555555
Klength = 128 bits, MAClength = 64 bits, KeccakIterations = 1
TOPc:   bd04d9530e87513c5d837ac2ad954623a8e2330c115305a73eb45d1f40cccbff
```

Output Parameters:

```
f1:     f9a54e6aeaa8618d
f1*:       e94b4dc6c7297df3
```

Intermediate Values:

```
IN when computing TOPc:
55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 00
30 2e 31 4b 41 55 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ab ab
ab ab ab ab ab ab ab ab ab ab ab ab 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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

OUT when computing TOPc:
ff cb cc 40 1f 5d b4 3e a7 05 53 11 0c 33 e2 a8 23 46 95 ad c2 7a 83 5d 3c 51 87 0e 53 d9 04 bd de
03 f9 ad b1 49 08 91 49 1c 23 5c 3d 41 31 eb 8f 9a 84 b5 fe b1 84 d6 13 c1 c4 db 07 6d 19 ea ac df
d0 24 e8 8e e9 53 a0 6c 3d 13 31 ad 61 14 00 4f 62 b3 bc da 77 fd 10 58 05 50 06 40 9a 40 6d 84 ac
a3 b2 62 dd 7b c8 76 b7 36 43 df 2c 55 a3 f1 af 11 63 ba 79 da aa 4f ce 02 fc fe 7f d4 d8 b6 06 f1
eb 71 e8 9f 92 46 4c 4a 24 e8 6a 29 72 78 6c 81 53 b4 ca 21 46 35 49 da 3a b3 e0 b7 19 5b be e4 e7
7f 77 d1 29 05 0a 99 5f 61 bd 0b 2f 72 e0 8a ae 75 aa fe b4 1e ee b0 4f 8c 51 ff f1 91 27 a7 9b 2c
99 b7

IN when computing f1:
ff cb cc 40 1f 5d b4 3e a7 05 53 11 0c 33 e2 a8 23 46 95 ad c2 7a 83 5d 3c 51 87 0e 53 d9 04 bd 08
30 2e 31 4b 41 55 54 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 ff ff 11 11 11 11 11 11 ab ab
```

```
ab ab ab ab ab ab ab ab ab ab ab ab ab 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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
```

OUT when computing f1:

```
8d 61 a8 ea 6a 4e a5 f9 61 5f 1e f1 ee 2b 9e 22 f6 f3 3b b0 c6 59 1c b2 ef ed f4 6b fe 15 b3 bf a4
93 5c 6d 5d 52 af 2c 27 81 c7 6f 16 10 ee 84 8e 81 86 59 e8 c3 45 8f 78 bb a4 a5 a9 66 11 6c ef 4a
1a 9e f1 e4 56 16 2e ef 18 c5 51 fd 9e 52 99 72 ca 01 f1 67 0e 3f 04 c0 f7 08 ab 30 a9 be 52 31 26
ad 2d 8d b2 43 9a 41 29 3e d9 27 4b fc 7e 30 e7 73 69 25 61 16 6c d3 e0 16 23 6a 61 5e 2d de df ff
92 36 3d 2a 38 f0 e1 12 d7 31 f5 14 ec 84 5c 26 c7 f9 a9 1f 17 a4 27 f5 e4 30 ec 28 19 94 b9 b4 4a
50 79 e4 08 52 ca 0b 66 67 a6 55 71 8e c3 34 8b 81 2e 83 f5 8b de 28 23 f3 b5 de 18 89 21 00 8f 1e
93 03
```

IN when computing f1*:

```
ff cb cc 40 1f 5d b4 3e a7 05 53 11 0c 33 e2 a8 23 46 95 ad c2 7a 83 5d 3c 51 87 0e 53 d9 04 bd 88
30 2e 31 4b 41 55 54 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 ff ff 11 11 11 11 11 11 ab ab
ab ab ab ab ab ab ab ab ab ab ab ab 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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
```

OUT when computing f1*:

```
f3 7d 29 c7 c6 4d 4b e9 08 40 73 fe c7 69 e9 b0 ca 72 71 ef e7 7b 16 1c 8e 9d 81 4d 4e 19 77 c0 8d
f0 52 cd 65 a7 1e 21 b2 6c 31 72 ae 3c c4 ea 93 a1 4f 98 17 18 3d 3a 22 6e ce f0 a9 f1 a6 9d ca 75
2d fd ee 32 98 ce 01 55 ac 90 a6 df 92 51 c1 95 b6 1a 78 25 f0 48 ca de ee 77 5e e0 9b cb 14 4b f9
58 bb cf de 3f da b2 7e 1a 1e 19 5c a3 19 02 de 39 94 24 d6 1b eb 57 17 df 4b d2 c7 f9 f4 57 84 7c
43 7e bb 4e 73 ca c1 18 61 8c 98 87 0a b9 60 40 3d 40 b4 40 61 ab db 81 1e 44 1c 62 0f 03 95 0f da
e3 c3 84 4c 08 b1 51 56 5a fe 60 0b ce ad 14 ca 09 b6 8a e2 d3 a5 f4 0c a4 d0 7e db 90 d4 c1 8a f7
00 9f
```

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, KeccakIterations = 1
TOPc:   305425427e18c503c8a4b294ea72c95d0c36c6c6b29d0c65de5974d5977f8524
```

Output Parameters:

```
f1:     c0b8c2d4148ec7aa5f1d78a97e4d1d58
f1*:        ef81af7290f7842c6ceafa537fa0745b
```

Intermediate Values:

IN when computing TOPc:

```
9f 9e 9d 9c 9b 9a 99 98 97 96 95 94 93 92 91 90 8f 8e 8d 8c 8b 8a 89 88 87 86 85 84 83 82 81 80 01
30 2e 31 4b 41 55 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing TOPc:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 90
db 97 25 30 c0 28 ed 2d 29 7e a9 37 bb 65 75 b6 06 03 b5 3d 24 25 bf 21 85 91 4c 29 83 a0 c0 22 7b
8c 8e 29 1e 56 23 b9 87 fd e7 9c eb 91 82 38 96 7c e0 51 0e 15 dc 83 cd 84 20 b2 45 2a b8 5f b6 f5
2f af 79 d2 df 63 ac f1 bb e2 4a 7d 71 a3 4b 48 ca 88 28 1a 55 f5 e6 6f 61 0f 08 a0 b7 05 11 b8 1f
1c fb 47 97 c0 48 d0 36 08 c0 10 10 0f 02 dd 81 95 06 b9 8e 0a 1f 28 14 a2 54 36 d2 0a 7f 27 82 24
13 f4 b7 2d 31 76 5a d2 19 4f 42 27 70 2c e1 98 50 4e 21 d3 15 8f a6 f1 9e e0 3a 87 90 f0 a2 9c 30
8c b5
```

IN when computing f1:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 11
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 cd ab ab 89 67 45 23 01 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing f1:

```
58 1d 4d 7e a9 78 1d 5f aa c7 8e 14 d4 c2 b8 c0 11 fe 0e 69 e9 d9 72 c8 9a e9 c0 99 88 b6 2c 37 ea
3f c3 e5 7f 18 63 d3 62 f9 fc 91 f9 92 b8 50 48 54 19 ed bf ee 23 79 4d 15 09 57 82 72 78 1a 1d 54
3d a6 ac 45 16 59 2c 0f b3 f5 ec 99 f1 5b 94 dc bc 7a 63 bc da 40 36 5f 9e a8 d6 e2 3a b2 9d b5 b7
1f 26 4e c3 61 95 b6 12 79 84 66 4f 3e 74 ba e0 9e b6 ce b0 66 94 22 14 8e e8 c9 12 dd dc bf f9 f9
30 e2 b3 8b 5c 8b 6b d8 90 b6 14 1c 02 7f 23 9c bf f4 f2 e2 3c 2d c4 89 f3 7a 61 38 18 cd 64 7a 27
56 05 5a 4e de 7e c4 66 74 37 24 6d 90 be 59 b6 ed f9 35 19 50 68 e6 d2 f1 82 60 80 3d 07 bd b7 ae
59 4c
```

IN when computing f1*:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 91
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 cd ab ab 89 67 45 23 01 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing f1*:

```
5b 74 a0 7f 53 fa ea 6c 2c 84 f7 90 72 af 81 ef 3c 41 02 e7 94 ab e0 40 1b ce a6 44 c2 c8 13 1f 54
7d 3d 57 fc ac c4 9c 07 9d fd e2 ec ac e8 56 43 78 70 87 44 63 f5 6f 92 94 12 b1 6b 67 6d 67 d3 3a
f9 cc 1e bc 4f 8b 99 4c 3f 64 6a a5 f5 38 dc 83 64 16 bf 7d 32 e6 cf 72 41 46 63 2b df 11 a5 2a 96
65 1e ef 55 3d b3 b0 0d f3 93 c2 d8 a4 29 cb 4c d4 b6 e9 3f 11 e1 f4 95 a4 a1 5f dd 50 e6 e9 67 6e
ab ba 56 49 24 e4 2b 89 fe 6a cd f8 23 c8 29 15 ad a3 39 37 c5 f2 c6 7a f3 c0 27 0f d8 49 1d 1d 22
bc c3 ff a1 0e 8d 25 df c5 1d 72 ab 86 0a 8a e6 cc 43 e2 5e f7 0c 14 82 8c c9 3d e0 a7 26 ba f6 f4
4b eb
```

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, KeccakIterations = 1
TOPc:       305425427e18c503c8a4b294ea72c95d0c36c6c6b29d0c65de5974d5977f8524
```

Output Parameters:

```
f1:         d97b75a1776065271b1e212bc3b1bf173f438b21e6c64a55a96c372e085e5cc5
f1*:        427bbf07c6e3a86c54f8c5216499f3909a6fd4a164c9fe235b1550258111b821
```

Intermediate Values:

As for Test Set 2 in clause6 .4, when computing TOPc.

IN when computing f1:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 21
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 cd ab ab 89 67 45 23 01 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing f1:

```
c5 5c 5e 08 2e 37 6c a9 55 4a c6 e6 21 8b 43 3f 17 bf b1 c3 2b 21 1e 1b 27 65 60 77 a1 75 7b d9 75
4e b1 85 f6 20 a8 57 a8 55 ce 33 ce b3 98 40 b3 06 ca 9c 15 6d 87 36 0d 3d e0 13 b0 41 c8 00 68 80
90 da 63 7c 2d 0a 80 79 02 a7 a3 b1 fd ce 8b f2 ac 0a 0f 17 04 e3 3c 28 37 ed c6 df 01 88 b9 5b b6
49 10 99 d1 62 e3 dd 92 03 fa bb f9 99 df 76 ca c8 4e d6 fb 8a da dd 1e cf 07 be 52 9e 74 6e 17 c9
22 a0 e5 4e e4 30 a1 76 5b bc bb cc b0 6d b0 b9 c3 95 26 4f 3b 4e b9 d7 6f d6 fc bc f9 4c 0e 4f 13
c4 69 23 70 70 50 4f 9e 0a 16 b2 22 5b ad 56 58 ff 19 26 93 39 73 37 7a 5c 96 75 7f 38 eb a2 c0 8e
00 1d
```

IN when computing f1*:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 a1
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 cd ab ab 89 67 45 23 01 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing f1*:

```
21 b8 11 81 25 50 15 5b 23 fe c9 64 a1 d4 6f 9a 90 f3 99 64 21 c5 f8 54 6c a8 e3 c6 07 bf 7b 42 d9
20 f9 d5 1e 28 2a a6 4f a7 ed 58 9b 93 f2 37 b9 0d d5 6f c7 fa 6d 05 a4 c9 b7 5d b4 28 1c 19 5b d7
fb 1d 5f 56 98 4a a3 ec fe ef a6 7a 05 90 67 5a 67 5b 95 03 fb 05 59 6d a7 7b a7 0c 17 aa d6 2e c2
1d 24 5e 25 82 b1 b7 d2 bd 0a 38 6f 51 93 a6 b4 a3 b2 00 42 ab be 68 ad 2b 58 da 9d ac 7c 9b d5 82
8a fb 15 ad 25 e5 b0 49 14 54 ba 3a 32 bd f8 7d 14 f0 3d 24 61 a8 65 f1 5f 51 62 41 ec 3d 54 d5 4f
b4 16 4f dd db f4 c9 9e a3 74 40 96 32 ec 8d bd 00 1f c6 71 f3 31 ae 5e fd 3d 90 bb a5 7b 62 fb a6
46 d2
```

6.6 Test set 4

Input Parameters:

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

Operator Configuration Parameters:

```
TOP:        0952be13556c32ebc58195d9dd930493e12a9003669988ffde5fa1f0fe35cc01
```

```
Klength = 128 bits, MAClength = 128 bits, KeccakIterations = 1
TOPc:       2bc16eb657a68e1f446f08f57c0efb1d493527a2e652ce281eb6ca0e4487760a
```

Output Parameters:

```
f1:         749214087958dd8f58bfcdf869d8ae3f
f1*:        619e865afe80e382aee13063f9dfb56d
```

Intermediate Values:

IN when computing TOPc:

```
01 cc 35 fe f0 a1 5f de ff 88 99 66 03 90 2a e1 93 04 93 dd d9 95 81 c5 eb 32 6c 55 13 be 52 09 00
30 2e 31 4b 41 55 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 61 cc
6a 4f a1 7d c9 c7 6a 2d 65 50 7a 83 da b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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
```

OUT when computing TOPc:

```
0a 76 87 44 0e ca b6 1e 28 ce 52 e6 a2 27 35 49 1d fb 0e 7c f5 08 6f 44 1f 8e a6 57 b6 6e c1 2b 6a
1d 66 b7 67 81 62 b7 4d 5a 55 3e 82 41 ec 7a e5 dd 89 25 12 a9 44 90 1a b6 e0 cb c9 ee a3 bd 86 ad
43 7f ae d3 2b 85 e1 38 af 04 03 66 1c 68 87 d9 e6 84 c7 ec 20 78 27 ea bd a3 63 22 2d f1 e6 f3 bb
5f 19 35 fc eb 75 2c 8e 86 30 68 1c fd 80 86 46 cd 31 dd 5a 65 8e de d4 68 40 d2 d7 7e 3d 6f 67 7b
14 e6 0d c1 43 ab 18 02 ee 4c 54 46 e5 a9 15 af 75 10 f5 b6 e4 03 c5 84 d3 d9 f5 9c 83 07 96 86 62
0d 1a 1d 9c 48 f7 89 a4 6d 00 04 ef a7 f3 1c 7e 08 a1 d4 85 ae e1 4c 15 fa 3a 09 ac 62 00 5d c7 8e
13 42
```

IN when computing f1:
0a 76 87 44 0e ca b6 1e 28 ce 52 e6 a2 27 35 49 1d fb 0e 7c f5 08 6f 44 1f 8e a6 57 b6 6e c1 2b 10
30 2e 31 4b 41 55 54 e8 2b a7 5f 1a 66 c9 86 bd 66 a9 25 54 e5 87 68 1e df af c5 e2 2e ea 0d 61 cc
6a 4f a1 7d c9 c7 6a 2d 65 50 7a 83 da b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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

OUT when computing f1:
3f ae d8 69 f8 cd bf 58 8f dd 58 79 08 14 92 74 cf f4 d0 cd c5 0f e0 23 26 0d 55 74 cf c5 a3 83 6a
58 31 c8 61 39 47 b8 65 77 5b 59 92 a5 6e 74 37 0e 9b eb fb 24 57 5a 04 ab 80 11 96 c3 9a de 74 62
2c dc c3 e5 1d 00 e2 45 1c e2 cd 54 ea 44 d2 6b b9 c3 db 0b 3e da 55 d6 02 7e 87 63 4d 3a 7d 83 93
07 ff da 7a 49 0d 3e c1 91 6d 5f aa 8c a9 92 43 d1 99 3f 72 ad 47 e2 a6 fa bb 68 1e c4 17 54 53 fe
54 fc 6f 31 45 1e 3c ed a3 39 17 44 87 a2 6e 6a 1d 58 77 76 86 8a e5 c9 02 d6 7c 07 ce 5b 79 e3 9e
8d cf 2e 29 fd 8c 6a 8d dd c8 07 a5 c5 e3 90 b7 09 38 df 54 ae a7 1e c9 9a 6c 34 5c 6a ae e8 04 5d
4a 13
IN when computing f1*:
0a 76 87 44 0e ca b6 1e 28 ce 52 e6 a2 27 35 49 1d fb 0e 7c f5 08 6f 44 1f 8e a6 57 b6 6e c1 2b 90
30 2e 31 4b 41 55 54 e8 2b a7 5f 1a 66 c9 86 bd 66 a9 25 54 e5 87 68 1e df af c5 e2 2e ea 0d 61 cc
6a 4f a1 7d c9 c7 6a 2d 65 50 7a 83 da b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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

OUT when computing f1*:
6d b5 df f9 63 30 e1 ae 82 e3 80 fe 5a 86 9e 61 38 ad 67 63 c4 95 c9 d9 a6 36 e6 cb 97 a9 0b 9e 39
a7 ea 5f bc b4 76 48 96 e8 07 e6 32 05 16 0d e8 ee f8 2e ed bb 95 c0 09 60 8c f7 ee ba 0c 08 b4 9c
76 31 3c ba dc fb 2b 18 b4 94 fb a4 e2 0a 68 7a 35 73 41 bf d9 81 a9 69 18 0b 26 7d 11 fc be de 7a
04 85 a7 b3 05 b3 38 83 53 0e 9c c3 de 4b a5 c2 c7 1e 35 03 cc 19 0e 69 22 18 f7 b4 42 e4 be a7 06
41 96 71 8a 8e 90 63 6b 03 60 30 80 95 93 12 4b df a7 22 6f ca 04 c8 64 77 e7 6e 12 51 88 0e 6e d9
01 86 af b5 37 99 54 fc 19 18 55 09 85 73 c7 e9 22 60 c0 bd 07 e3 23 04 66 dd 3d 95 af 93 13 14 bf
5c b3

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, KeccakIterations = 1
TOPc:   3c6052e41532a28a47aa3cbb89f223e8f3aaa976aecd48bc3e7d6165a55eff62
```

Output Parameters:

```
f1:         d7340dad02b4cb01
f1*:        c6021e2e66accb15
```

Intermediate Values:

IN when computing TOPc:

```
5e c9 88 ee 35 da 34 6d f6 80 b4 17 7e 4c df 1e 18 2f e0 b9 b0 91 49 3f 81 06 a4 0e b1 6e 9f e5 01
30 2e 31 4b 41 55 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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
```

OUT when computing TOPc:

```
62 ff 5e a5 65 61 7d 3e bc 48 cd ae 76 a9 aa f3 e8 23 f2 89 bb 3c aa 47 8a a2 32 15 e4 52 60 3c 43
f5 71 a5 ba 6c 9d 75 07 6f 91 9a b5 a5 4c d7 78 70 f9 b7 8d 11 f2 61 41 78 05 1e d8 ba a8 cd 6e 09
df 81 0a 0a b1 1f 3d 73 47 e5 77 d9 b3 fc 93 75 6e ef 30 fd 3d 8a 38 9a 80 ad 11 97 2f 07 a8 fe f8
22 43 46 74 bd 13 f2 ef 33 54 45 2f 2e c9 b0 91 b3 1b 51 e3 11 29 ab 2a 70 54 96 ff c9 ce ee e8 7e
08 ea 5a 75 44 fd ce 57 08 ea 7b 2d a1 c2 a9 15 bc 2a 48 cd a1 58 2d 05 6e 6e 25 c7 48 24 7a 6e 95
66 6d e3 24 de 09 24 72 4d 20 ae 2a ce d6 e0 5b ea 53 22 91 27 96 3f b9 4f 72 28 85 02 cb a6 94 95
1c 0f
```

IN when computing f1:

```
62 ff 5e a5 65 61 7d 3e bc 48 cd ae 76 a9 aa f3 e8 23 f2 89 bb 3c aa 47 8a a2 32 15 e4 52 60 3c 09
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 7d 29 41 3a 1f b7 9b c8 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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
```

OUT when computing f1:

```
01 cb b4 02 ad 0d 34 d7 dd 3d 1c 29 35 6f 0c 34 05 fb f6 00 94 91 47 ff 38 52 13 d1 10 a7 f5 4d 4e
ae 0c f2 e9 24 4b e1 37 2f 4d 42 18 ff e0 4e b0 4c 8d 83 3f 5b 5f 0a c6 b2 13 d5 7b 5f 1c b5 18 dc
4d 34 4b 60 b2 1c a6 84 ba 97 d3 4c 17 88 92 cd 8d 92 44 64 37 c1 0f 54 af d1 54 b3 20 c1 06 0a de
a3 0f b0 97 33 53 70 f0 57 7a 4c cd f3 7f b5 2d 06 d6 5d a8 0e de 90 6c f5 a8 d9 0c cf 40 db c0 38
d7 f8 22 52 05 97 76 b6 f2 65 90 cd b6 ae 5b 34 c8 08 86 ee da a4 18 e9 d6 60 1f 59 24 df 16 71 99
02 c7 e2 d4 56 4e 32 f7 57 8f cb 55 75 18 9a 97 44 2c 9a 36 cf 58 d9 e6 c8 66 cf a1 28 98 b0 46 f7
83 2c
```

IN when computing f1*:

```
62 ff 5e a5 65 61 7d 3e bc 48 cd ae 76 a9 aa f3 e8 23 f2 89 bb 3c aa 47 8a a2 32 15 e4 52 60 3c 89
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 7d 29 41 3a 1f b7 9b c8 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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
```

OUT when computing f1*:

```
15 cb ac 66 2e 1e 02 c6 a0 8d 88 13 f1 23 34 c7 bb f6 0e 14 55 9b d3 d6 73 a5 ea 4d c5 98 e9 63 dd
ec bf 5e c0 fb 55 7f 5f bd 41 ca 30 2b f7 31 0c 9b 35 64 ae 7b 48 86 69 fd 3a d8 5d 86 e4 e7 46 07
05 e3 8e 7d 0c 75 56 4a 6a 5f ce 85 7b 1d 68 11 98 ab ca ed 76 72 e5 b6 4d 1b 3e 0b 36 51 73 d9 dc
24 10 72 f5 a5 fb fa 49 1b 07 a8 3e d8 1f 8b b6 22 3d 29 d2 71 ce 91 01 e5 0c 34 0c e4 9e 65 ea 5f
ad d6 38 05 ba ba c3 e5 4c b4 34 46 93 6b 1e 17 3f c6 a9 f5 bc 38 5d 37 68 90 b8 6b 8c 2f 4a 66 a1
75 8f 17 a0 9c 2e d8 8d 79 0d 59 9a 03 15 27 6e 66 17 33 cf 33 7c d4 8d 22 b1 09 50 46 eb f0 73 a4
82 24
```

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, KeccakIterations = 2
TOPc:       b04a66f26c62fcd6c82de22a179ab65506ecf47f56245cd149966cfa9cec7a51
```

Output Parameters:

```
f1:         90d2289ed1ca1c3dbc2247bb480d431ac71d2e4a7677f6e997cfddb0cbad88b7
f1*:        427355dbac30e825063aba61b556e87583abac638e3ab01c4c884ad9d458dc2f
```

Intermediate Values:

IN when computing TOPc:

```
5e c9 88 ee 35 da 34 6d f6 80 b4 17 7e 4c df 1e 18 2f e0 b9 b0 91 49 3f 81 06 a4 0e b1 6e 9f e5 01
30 2e 31 4b 41 55 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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
```

OUT/IN after one Keccak iteration, when computing TOPc:

```
62 ff 5e a5 65 61 7d 3e bc 48 cd ae 76 a9 aa f3 e8 23 f2 89 bb 3c aa 47 8a a2 32 15 e4 52 60 3c 43
f5 71 a5 ba 6c 9d 75 07 6f 91 9a b5 a5 4c d7 78 70 f9 b7 8d 11 f2 61 41 78 05 1e d8 ba a8 cd 6e 09
df 81 0a 0a b1 1f 3d 73 47 e5 77 d9 b3 fc 93 75 6e ef 30 fd 3d 8a 38 9a 80 ad 11 97 2f 07 a8 fe f8
22 43 46 74 bd 13 f2 ef 33 54 45 2f 2e c9 b0 91 b3 1b 51 e3 11 29 ab 2a 70 54 96 ff c9 ce ee e8 7e
08 ea 5a 75 44 fd ce 57 08 ea 7b 2d a1 c2 a9 15 bc 2a 48 cd a1 58 2d 05 6e 6e 25 c7 48 24 7a 6e 95
66 6d e3 24 de 09 24 72 4d 20 ae 2a ce d6 e0 5b ea 53 22 91 27 96 3f b9 4f 72 28 85 02 cb a6 94 95
1c 0f
```

OUT after second Keccak iteration, when computing TOPc:

```
51 7a ec 9c fa 6c 96 49 d1 5c 24 56 7f f4 ec 06 55 b6 9a 17 2a e2 2d c8 d6 fc 62 6c f2 66 4a b0 5f
93 fc cc 52 f0 45 26 53 4e 5f 33 9f ec 28 68 9d 6b 24 10 d4 ef 31 27 6d f1 28 30 88 bc 84 4d e3 18
44 5b dc c3 f1 07 43 37 b8 b5 fd c5 e0 dd dd 91 04 aa 78 b3 38 64 72 7d 46 13 78 3b 35 fa 09 61 77
d8 db 1c 3b c3 4b 96 e9 23 ed 3f af 4a ec fc cf 8e f4 e0 a1 52 90 44 40 40 07 e4 1b 2d 53 47 11 e4
79 c6 bd a0 1a 35 96 0f 03 a3 78 17 bf a6 85 ad 3a 43 d1 46 45 98 da b6 9a 54 e4 56 5d 0b 5b 71 3a
c8 f8 7c e7 d7 b6 2d a8 db 9c 87 72 e8 2c 07 12 2c 95 61 6c ee 1b 03 3f 2b 77 20 c1 2c 65 a7 4d 45
67 ac
```

IN when computing f1:

```
51 7a ec 9c fa 6c 96 49 d1 5c 24 56 7f f4 ec 06 55 b6 9a 17 2a e2 2d c8 d6 fc 62 6c f2 66 4a b0 21
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 7d 29 41 3a 1f b7 9b c8 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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
```

OUT/IN after one Keccak iteration, when computing f1:
26 52 3f 89 99 46 a9 85 f3 76 19 e7 38 9b 7e 42 e7 ab ff ff 8c 82 cb 1b 0f 22 5f 1d 64 29 a3 36 e2
22 63 bb 8b ee 5a c0 b4 b6 04 9d 77 54 69 a3 5c 21 42 a5 0d d6 28 4d 83 be 05 57 50 3c 5f 55 0d 18
30 26 ef e3 4b c9 d7 c9 2f 62 8c 25 95 e3 00 61 3d c1 df db a7 1c 18 87 22 18 12 e4 53 27 1d 98 20
eb a0 cb 01 34 59 18 58 b0 db ed 7f 54 f1 4f 5f 43 78 6c 44 38 9d a8 26 b6 34 41 1e 28 98 6f a6 7d
16 6d f2 84 90 b4 29 e9 06 b0 9f 3d 09 dc d6 d9 9f 8f 3d a8 b7 14 40 4e 7e 07 e9 dc d4 fd 36 a9 fa
76 4e bc a7 0f cd 6f 12 46 fe 82 67 23 ab 3f 17 94 e1 56 82 b9 48 b9 08 00 2c cc c1 7b ef 4d c9 70
57 e9

OUT after second Keccak iteration, when computing f1:
b7 88 ad cb b0 dd cf 97 e9 f6 77 76 4a 2e 1d c7 1a 43 0d 48 bb 47 22 bc 3d 1c ca d1 9e 28 d2 90 f3
69 1a f6 7f 10 1f 51 d8 d6 91 9c 19 55 1d 80 28 97 a8 e1 d6 11 68 70 01 39 24 28 7e b8 b8 c4 54 0f
2e 02 c7 08 cd 6d 56 5a 2a 7f 42 77 c7 7b c5 dd cb 2d 8f f5 a2 02 76 d1 0b da 13 f0 ac 06 76 05 14
fc 7a d5 b7 30 a7 76 22 6b d5 b0 e6 e5 b7 47 d5 03 af b3 a1 64 f9 b1 f0 b5 aa 13 99 8c fd a4 69 b0
7a a6 0c 0c 1c 25 ed b1 d1 bb bb 15 40 3a bf fc 83 b5 c3 87 7a 2f 65 82 1f 41 97 06 8f 13 f1 7f fb
fa 92 72 3d 47 63 86 45 6c 61 4c c9 30 93 1c f7 73 52 24 7c 20 96 f8 95 aa 1c b1 63 44 74 db f4 0c
a1 47

IN when computing f1*:
51 7a ec 9c fa 6c 96 49 d1 5c 24 56 7f f4 ec 06 55 b6 9a 17 2a e2 2d c8 d6 fc 62 6c f2 66 4a b0 a1
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 7d 29 41 3a 1f b7 9b c8 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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

OUT/IN after one Keccak iteration, when computing f1*:
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 after second Keccak iteration, when computing f1*:
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

Note that this final iteration corresponds to Test Set 1 for Keccak inclause 5.3.

7 Algorithms f2, f3, f4, f5 and f5*

7.1 Overview

The test data sets presented here are for the algorithms *f2, f3, f4, f5, f5**. Inputs and outputs to the permutation Π are also presented here to assist with the implementation.

7.2 Format

Each test starts by showing the inputs K and RAND to the functions. Next are shown the operator configuration field TOP, and other operator configuration parameters: the length of the K, the length of the outputs CK, IK and RES, and the number of Keccak iterations.

These are followed by the value of TOP_C and then the output values of *f2-f5* and *f5** are shown. The value TOP_C should not be computed on but off the UICC. In the example code TOP_C is computed inside the functions, so it was included in the test data.

All the input, output and configuration parameters are presented using the bit/byte ordering convention described in clause 4.3. Intermediate inputs and outputs to the permutation Π are also shown, as lists of 200 bytes, using the convention described in clause 5.2.

7.3 Test set 1

Input Parameters:

```
K:          abababababababababababababab
RAND:       42424242424242424242424242424242
```

Operator Configuration Parameters:

```
TOP:        55555555555555555555555555555555555555555555555555555555555555555555
Klength = 128 bits, CKlength = 128 bits, IKlength = 128 bits,
RESLength = 32 bits, KeccakIterations = 1
TOPc:       bd04d9530e87513c5d837ac2ad954623a8e2330c115305a73eb45d1f40cccbff
```

Output Parameters:

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

Intermediate Values:

As for Test Set 1 in clause 6.3, when computing TOPc.

IN when computing f2-f5:

```
ff cb cc 40 1f 5d b4 3e a7 05 53 11 0c 33 e2 a8 23 46 95 ad c2 7a 83 5d 3c 51 87 0e 53 d9 04 bd 40
30 2e 31 4b 41 55 54 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 00 00 00 00 00 00 00 00 ab ab
ab ab ab ab ab ab ab ab ab ab ab ab 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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
```

OUT when computing f2-f5:
64 cd 7a 65 43 ac 5e 7a a6 f8 d1 82 ec 01 84 d9 16 97 5e 5e fc 3b 0b c7 87 80 f7 f0 94 db 05 1a e1
8b c7 e5 83 f7 26 6a 98 fe af 6c 5c 1e 1a d7 13 32 e5 90 c7 72 8f 04 0e db e9 a9 8a 52 1c e2 72 7e
33 d4 62 6f ee ec 9a 86 4f 56 a2 9f 84 be f6 7b f6 1a 31 a8 cd 73 76 a5 40 02 bd ae f1 f0 54 90 9b
1e 9f 71 33 52 f1 8b e8 b5 f0 37 71 57 45 62 92 1a 4d 74 b5 76 12 8c d9 b3 53 ee 4b 9a 16 ff 6a aa
e8 09 5d 35 57 da cd ee 0b ad c1 99 b4 c5 ff 80 7f 77 61 5f b4 4a ce 33 d2 5e de 8e 19 44 39 f2 e5
37 88 6c ad 0a cd 41 02 1e a0 61 7c 2c 6a 78 ff 46 b5 c9 68 28 0c bb 6a 29 52 2e 53 c2 99 16 9a 61
73 8b

IN when computing f5*:
ff cb cc 40 1f 5d b4 3e a7 05 53 11 0c 33 e2 a8 23 46 95 ad c2 7a 83 5d 3c 51 87 0e 53 d9 04 bd c0
30 2e 31 4b 41 55 54 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 00 00 00 00 00 00 00 00 ab ab
ab ab ab ab ab ab ab ab ab ab ab ab 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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

OUT when computing f5*:
46 6b 1d bd 30 d3 3e 41 a9 65 b0 17 b1 63 d5 aa 3f 75 7f 65 ec 81 5b e0 e1 f1 97 5b c9 a0 70 61 64
00 8c 8c 02 08 71 70 e0 52 e8 bf ab d5 cf 67 b0 dc d0 cb 94 e7 a7 08 20 7d 40 f7 ef 2e 86 bf 81 99
e2 8f 0e bd 1f a1 b8 48 97 e5 24 31 72 61 bf 4c 2c 69 18 b2 66 76 78 92 e2 87 13 c1 9e 82 38 0e 3d
6b af e7 fb 66 1a 2e 97 4a bf f0 6d 7f 94 a5 ec 1b 8e ef 46 3e 11 b6 e0 59 77 19 ae 7d 27 f5 f9 5e
6b 38 5d 68 c2 2d 8a 60 32 2b de 04 0d 82 46 6e 39 cf ec ac 6c b7 cc cc 1e 8d fd 1b 87 9a ff 29 72
67 b1 70 11 b7 44 9b eb 28 99 e9 7e 36 9f a6 17 13 a9 1f c7 d4 1e 91 fe 4a 46 a0 a3 e9 b9 38 5b c8
56 9b

7.4 Test set 2

Input Parameters:

```
K:          fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0efeeedecebeae9e8e7e6e5e4e3e2e1e0
RAND:       0123456789abcdef0123456789abcdef
```

Operator Configuration Parameters:

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

Output Parameters:

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

Intermediate Values:

As for Test Set 2 in clause 6.4, when computing TOPc.

IN when computing f2-f5:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 49
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 00 00 00 00 00 00 00 00 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing f2-f5:

```
35 00 ea 4e dc 49 d7 e9 ec 66 ca 43 7c c7 37 70 f9 06 35 f0 2c f3 99 02 fa a5 f7 4d 38 c5 7f 84 47
4d 23 a8 ba 27 7f 33 f8 17 ab 29 65 6f cb a4 41 fd a2 ba f5 a3 45 0b b0 c5 0f 29 2b 3b ca 35 90 7f
90 21 f6 cb ab e2 d5 99 41 cf 5c 15 74 22 5f 68 0a 9d 4e a5 e1 20 e5 8c 28 a2 fa ad 50 34 1e cc 45
93 0a 48 1b 99 ad 40 f6 06 d7 f4 12 47 88 d6 b6 fe 66 da 8c 9d 53 8a 21 ad 08 f7 c0 cc 61 34 1d 4c
60 ff 16 af 27 d4 b3 89 ec b5 5c 0e 7e 1e 7f ed e7 b8 0b 37 e0 17 8f 86 8c eb b9 12 63 bc c1 72 6e
8e 66 25 e4 5e 83 1e 79 35 9b f4 b8 c2 8e 88 26 f1 fb 5b 8b b4 82 1a 5e 76 13 fb 48 32 11 87 80 5a
40 31
```

IN when computing f5*:

```
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 c1
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 00 00 00 00 00 00 00 00 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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
```

OUT when computing f5*:

```
2b 8b b3 71 5f 6f 3d a7 0a 69 56 67 60 93 cd 86 85 2f b8 d1 69 c8 34 65 1d 0c 76 cd 31 7c de 24 be
03 de e6 a0 0e 01 56 32 7c 8c 71 f4 e3 88 8d f6 a3 77 c8 00 aa 33 c5 29 5c bb e5 81 62 10 23 26 bd
89 79 9c 69 96 3f ab e6 d0 76 16 06 0e 36 d1 09 9d a1 b7 69 c2 7e cd e5 7d 87 d6 a7 1f 01 8c 84 38
b3 4e f8 e4 ad cd 1a a9 fe 7a 61 3c e6 ba 5e 0b 79 d7 0d 22 7f 33 9e 6a 3d fb 3d f5 fa 94 5e 98 10
36 b0 91 13 6f 96 90 e2 d4 79 d4 6d 31 d3 9b f4 10 75 08 e4 b5 8a 9b e6 e5 d0 0a 48 e4 c0 67 51 93
06 b7 3f 5b a3 dd 23 50 76 ac 1d 55 42 5e 6e f9 e3 f7 20 3c 47 0a 98 32 18 b1 2a c9 f4 d6 b9 05 9a
02 5e
```

7.5 Test set 3

Input Parameters:

```
K:          fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0efeeedecebeae9e8e7e6e5e4e3e2e1e0
RAND:       0123456789abcdef0123456789abcdef
```

Operator Configuration Parameters:

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

TOPc: 305425427e18c503c8a4b294ea72c95d0c36c6c6b29d0c65de5974d5977f8524

Output Parameters:

f2: 07021c73e7635c7d
f3: 4d59ac796834eb85d11fa148a5058c3c
f4: 126d47500136fdc5ddfd14f19ebf16749ce4b6435323fbb5715a3a796a6082bd
f5: 1d6622c4e59a
*f5**: f84eb338848c

Intermediate Values:

As for Test Set 2 in clause6.4, when computing TOPc.

IN when computing f2-f5:
24 85 7f 97 d5 74 59 de 65 0c 9d b2 c6 c6 36 0c 5d c9 72 ea 94 b2 a4 c8 03 c5 18 7e 42 25 54 30 4b
30 2e 31 4b 41 55 54 ef cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 00 00 00 00 00 00 00 00 e0 e1
e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 1f 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 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

OUT when computing f2-f5:
7d 5c 63 e7 73 1c 02 07 12 5c 5e fe bf 31 b4 c9 22 52 ed 1e 96 2a 98 3f 87 bf 79 3b 1a d0 93 43 3c
8c 05 a5 48 a1 1f d1 85 eb 34 68 79 ac 59 4d ac 21 e8 b7 cd 87 d5 57 a0 b4 19 c4 67 2c 74 ef bd 82
60 6a 79 3a 5a 71 b5 fb 23 53 43 b6 e4 9c 74 16 bf 9e f1 14 fd dd c5 fd 36 01 50 47 6d 12 9a e5 c4
22 66 1d 2c 03 c8 d4 c3 e9 59 a9 6e a8 cb d2 8a 81 4a 18 8b 2f a6 c1 c6 f1 44 2f 96 5e af ab 93 11
03 74 83 39 1f 3c 39 2f 3a 05 a9 43 3c 11 de 27 eb 6f 67 4d 98 7a 90 ad f1 74 8c 26 f3 65 fc 69 75
e3 b8 8b d2 33 48 f2 20 3b 60 f7 f6 82 78 e6 7a 35 d2 e7 28 fb 2f 7d 52 08 ce 11 9e 40 44 30 6e e7
24 3e
As for Test Set 2 in clause7.4, when computing f5*.

7.6 Test set 4

Input Parameters:

```
K:          b8da837a50652d6ac7c97da14f6acc61
RAND:       6887e55425a966bd86c9661a5fa72be8
```

Operator Configuration Parameters:

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

Output Parameters:

```
f2:         4041ce438e3e38e8aa96562eed83ac43
f3:         3e3bc01bea0cd914c4c2c83ce2d92757
f4:         666a8e6f577b1aa77b7fd53cebb8a3d6
f5:         1f880d005119
f5*:        45e617d77fe5
```

Intermediate Values:

```
As for Test Set 4 in clause6.6, when computing TOPc.

IN when computing f2-f5:
0a 76 87 44 0e ca b6 1e 28 ce 52 e6 a2 27 35 49 1d fb 0e 7c f5 08 6f 44 1f 8e a6 57 b6 6e c1 2b 50
30 2e 31 4b 41 55 54 e8 2b a7 5f 1a 66 c9 86 bd 66 a9 25 54 e5 87 68 00 00 00 00 00 00 00 00 61 cc
6a 4f a1 7d c9 c7 6a 2d 65 50 7a 83 da b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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

OUT when computing f2-f5:
43 ac 83 ed 2e 56 96 aa e8 38 3e 8e 43 ce 41 40 33 d3 16 49 0b ac 6f 15 ad 56 87 1e b8 d4 7b 3d 57
27 d9 e2 3c c8 c2 c4 14 d9 0c ea 1b c0 3b 3e ee 84 85 d7 7f a4 c8 a2 c6 9b c1 37 79 b4 26 19 d6 a3
b8 eb 3c d5 7f 7b a7 1a 7b 57 6f 8e 6a 66 5c 4c 99 c0 ad 5c 93 b3 ad d9 8f 5f 62 e6 eb 74 19 51 00
0d 88 1f ed ff 87 53 22 88 56 a3 e5 3d 8b 03 5c a1 06 78 c8 9a 69 24 05 3a a9 87 67 72 19 a0 5f b3
55 9a 72 66 b0 47 17 9d 7e 45 1a 78 a3 cf ed b7 4f 43 21 66 49 63 c4 62 ba c6 c3 61 78 88 c9 00 86
e0 46 fb 17 f6 2f 8e 6d 97 09 2d f6 8e 93 a4 a0 d2 f4 c3 2b 8a 3d 73 d1 13 94 27 4b 2b 16 ae db db
bc 8d

IN when computing f5*:
0a 76 87 44 0e ca b6 1e 28 ce 52 e6 a2 27 35 49 1d fb 0e 7c f5 08 6f 44 1f 8e a6 57 b6 6e c1 2b c0
30 2e 31 4b 41 55 54 e8 2b a7 5f 1a 66 c9 86 bd 66 a9 25 54 e5 87 68 00 00 00 00 00 00 00 00 61 cc
6a 4f a1 7d c9 c7 6a 2d 65 50 7a 83 da b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 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 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

OUT when computing f5*:
d1 72 29 2f 8e 08 be 5b 00 a2 ac d3 7f 51 00 0c e5 8d ad a9 84 9b 7f 76 94 0c 10 40 88 8b 64 d8 05
7d 45 2e 0a e7 f8 0f 93 3a 79 13 f3 72 23 13 fc 24 b5 63 27 29 b9 b1 10 59 bf 17 e7 b9 38 ed cc bc
67 26 cd ea 48 3d 8a 69 01 49 1a b6 b3 c4 f0 a7 59 e6 fb ac e5 55 4b f9 ad 9e 8e 91 59 34 e5 7f d7
17 e6 45 47 b6 2d fb 8c c6 af ac 46 76 2e 07 95 ba 5b c2 aa 9f bd 48 e2 e8 14 cb 7a 17 99 58 d3 ed
97 74 e9 ea be 89 82 83 c1 06 6d 34 d7 fc ee 51 75 66 4c aa 21 f1 16 d3 24 69 b2 3d 6c e1 7c f5 34
9b 66 ac dd 64 ae 6c 25 1f 6a c6 a9 23 60 93 bd 59 97 1c 25 9f 87 1b 88 6a a1 b8 07 94 e2 a7 3f f2
0b 21
```

7.7 Test set 5

Input Parameters:

```
K:          1574ca56881d05c189c82880f789c9cd4244955f4426aa2b69c29f15770e5aa5
RAND:       c570aac68cde651fb1e3088322498bef
```

Operator Configuration Parameters:

```
TOP:        e59f6eb10ea406813f4991b0b9e02f181edf4c7e17b480f66d34da35ee88c95e
Klength = 256 bits, CKlength = 256 bits, IKlength = 128 bits,
RESLength = 256 bits, KeccakIterations = 1
```

```
TOPc:       3c6052e41532a28a47aa3cbb89f223e8f3aaa976aecd48bc3e7d6165a55eff62
```

Output Parameters:

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

Intermediate Values:

```
As for Test Set 5 in clause 6.7, when computing TOPc.

IN when computing f2-f5:
62 ff 5e a5 65 61 7d 3e bc 48 cd ae 76 a9 aa f3 e8 23 f2 89 bb 3c aa 47 8a a2 32 15 e4 52 60 3c 65
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 00 00 00 00 00 00 00 00 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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

OUT when computing f2-f5:
5c 90 eb 1e 0b 94 26 b5 fb 18 54 ae fb 20 6a 52 4d 3f 16 82 1d ba c7 d4 ff 67 18 db 41 9b d8 84 65
fe 88 a9 27 44 33 0c 6a 67 a4 31 0b ef 52 2f 4d 3a 52 43 0d ee 8b 1d 8c b5 5a fe 6a 67 19 d4 f4 18
78 c8 ea c0 5c d0 61 1b 66 05 e5 33 55 20 77 dc 33 69 95 08 62 22 b2 11 98 a1 ed d9 50 7c 0a 98 d4
d2 b3 d7 c0 31 b7 ce 7e 47 3c 45 8b 01 ed 35 bf 2a 3f 33 2f 94 e6 e0 46 7b 48 5e 51 e5 e5 d6 9b 28
62 dc a1 2f ac 4a 9a e3 e8 81 13 f1 d2 6e bd df b6 6f ae 2c 61 ca ca 17 0d a3 58 02 32 b4 e0 02 ba
4a fe f8 42 f8 05 8b 2a eb 60 f0 74 52 92 13 2c b2 42 a0 c5 96 da c0 5f 68 d9 8f b0 f5 32 ee d5 eb
5c a3

IN when computing f5*:
62 ff 5e a5 65 61 7d 3e bc 48 cd ae 76 a9 aa f3 e8 23 f2 89 bb 3c aa 47 8a a2 32 15 e4 52 60 3c c1
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 00 00 00 00 00 00 00 00 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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

OUT when computing f5*:
b1 ef 6c a0 a5 a4 8b 08 fc c2 f1 84 39 77 3b f2 ee e8 f4 b8 95 25 8b 14 ce 08 2f cf 16 06 2b 76 09
8d 73 9e c2 68 3e c1 94 1d 61 bc 58 7c 8d f2 c2 b6 86 ef 05 d9 a3 8c d2 a2 6c fc e6 4e 81 3d cf e4
05 a5 5b 51 0c a8 a1 89 9f 63 4b c6 a3 89 a4 64 1a 93 9b 16 30 2e 17 06 86 02 6e a3 09 0a 86 49 26
55 96 ca 5f 7f e1 89 a7 06 c0 12 4d ae 0a 24 73 fc f3 d4 61 92 5a b4 a2 28 f4 22 ec b4 7c 24 5d b0
68 14 08 15 ba 72 96 de 53 07 cb f2 51 a5 34 80 bc c8 ae f5 1a 99 73 e6 75 51 bc 79 8f 78 1f f1 71
1d 65 01 6f e9 b3 6f 04 99 e5 cc 4c 86 fe a1 a8 bd 21 b9 fe 22 92 31 f4 18 8e fd fb 0f f4 04 18 0a
88 f4
```

7.8 Test set 6

Input Parameters:

```
K:          1574ca56881d05c189c82880f789c9cd4244955f4426aa2b69c29f15770e5aa5
RAND:       c570aac68cde651fb1e3088322498bef
```

Operator Configuration Parameters:

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

Output Parameters:

```
f2:         d67e6e64590d22eecba7324afa4af4460c93f01b24506d6e12047d789a94c867
f3:         ede57edfc57cdffe1aae75066a1b7479bbc3837438e88d37a801cccc9f972b89
f4:         48ed9299126e5057402fe01f9201cf25249f9c5c0ed2afcf084755daff1d3999
f5:         6aae8d18c448
f5*:        8c5f33b61f4e
```

Intermediate Values:

```
As for Test Set 6 in clause 6.8, when computing TOPc.
```

IN when computing f2-f5:
51 7a ec 9c fa 6c 96 49 d1 5c 24 56 7f f4 ec 06 55 b6 9a 17 2a e2 2d c8 d6 fc 62 6c f2 66 4a b0 67
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 00 00 00 00 00 00 00 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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

OUT/IN after one Keccak iteration, when computing f2-f5:
45 de 3d d1 50 4d 7c 3b b7 32 1a a8 2e c4 5a bc ed 2b b0 6d 4c 56 ef 84 7f 53 c3 95 2b 76 75 e9 6b
d8 d6 a6 f1 0f 25 83 65 cb c7 2d 71 f1 bf ae 8f 9f 1a b8 04 92 fb 03 50 db 45 d4 4c 16 c9 f3 4d 38
d8 fa c1 3c 8a 92 4a bd 97 d1 79 fa 28 b6 04 1a ca 29 6b 86 03 bb af f8 ac a2 d5 4c fd f5 a9 80 b1
7b 93 6f fe 6c 63 80 5a 8a c8 5f 07 e2 ba 9c 76 df 61 65 3c 1f ec 15 55 93 cd eb 05 61 73 7c ca b3
86 d0 c0 5b 5a 2e b9 29 c9 d4 d3 9e fc 63 38 83 77 06 f4 8a ab ab a2 69 a1 d9 ff 42 d2 f3 ef 01 bd
7f 27 15 2c a2 a7 32 54 02 3b 99 d1 cb b6 6b 88 eb 6e 2a 36 93 fd 56 48 e1 3d 81 9b 5f 2a 00 65 ca
8b 13

OUT after second Keccak iteration, when computing f2-f5:
67 c8 94 9a 78 7d 04 12 6e 6d 50 24 1b f0 93 0c 46 f4 4a fa 4a 32 a7 cb ee 22 0d 59 64 6e 7e d6 89
2b 97 9f cc cc 01 a8 37 8d e8 38 74 83 c3 bb 79 74 1b 6a 06 75 ae 1a fe df 7c c5 df 7e e5 ed 99 39
1d ff da 55 47 08 cf af d2 0e 5c 9c 9f 24 25 cf 01 92 1f e0 2f 40 57 50 6e 12 99 92 ed 48 48 c4 18
8d ae 6a ae 10 c1 1d 8d 25 00 c7 d0 95 53 8b 9e dc 42 6b 7b 0b ba 58 d4 15 a2 01 62 d6 41 42 b9 eb
9e af 5b 40 0f 17 bd a3 3f a3 da f8 a2 b3 bf a3 a1 b4 b7 54 53 69 83 2e 0b 94 da 31 93 81 d1 26 9a
c1 3c 26 a1 fe d0 dd 0a 66 0f f8 96 31 29 04 7e 2f 63 cd 4a 94 81 79 38 2e 4e db 4d 52 35 90 c7 87
46 28

IN when computing f5*:
51 7a ec 9c fa 6c 96 49 d1 5c 24 56 7f f4 ec 06 55 b6 9a 17 2a e2 2d c8 d6 fc 62 6c f2 66 4a b0 c1
30 2e 31 4b 41 55 54 ef 8b 49 22 83 08 e3 b1 1f 65 de 8c c6 aa 70 c5 00 00 00 00 00 00 00 a5 5a
0e 77 15 9f c2 69 2b aa 26 44 5f 95 44 42 cd c9 89 f7 80 28 c8 89 c1 05 1d 88 56 ca 74 15 1f 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 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

OUT/IN after one Keccak iteration, when computing f5*:
bf 66 e2 27 5d d6 6e 1c 15 82 da 5b ab b8 d6 dd 33 46 ff ca e0 c5 95 d9 08 22 7d f9 ec 75 2a ac c2
d5 ef c8 70 11 12 7c 72 32 d6 82 83 20 39 df e3 a9 8b 4f 63 2f 5f e4 6b af 34 4f 21 7f e8 68 be 5e
61 d3 41 be e4 05 12 e6 0f d3 c1 70 0b 5a 34 47 47 7d 5b b5 b5 f5 ba 5e e4 c0 2b f6 f8 38 8f 8c cc
35 bf 79 fb c0 31 db 27 b8 0f c1 b1 43 14 d7 99 f5 0e 01 28 e4 23 fa db 72 cd de c2 a8 ee 1c 74 69
53 cc d6 5f 94 19 24 62 b2 fb d6 91 e2 e5 5c 35 b3 e5 d1 59 a4 04 20 de d5 16 12 c0 96 64 f4 9b ea
aa ba 4e 1d 57 a5 ec 8c 0f 30 e3 59 2e b7 38 56 2b f7 e3 f9 0f a0 41 dc b1 4e d1 5d 0b 6c 5d 34 05
94 98

OUT after second Keccak iteration, when computing f5*:
3f cb 12 cc 5c aa aa 1f ea 8e 1c 14 8e 67 4a 6f ee e5 fc 38 88 9a a1 7a b4 d8 85 68 14 02 d0 9a 55
62 72 a7 99 99 4b 3b 9d 21 de b6 c5 5a 14 14 e1 a3 27 4d 75 c2 81 f6 15 7a 19 a4 d0 07 14 0d 52 35
3c 38 a5 89 27 39 24 5e 64 fa 6b 00 01 1b ec 63 10 b2 3f 3c 3f 02 0a cd b5 df fb af 92 7d 4e 1f b6
33 5f 8c 4a ef e0 d6 30 0a 8f f0 f9 34 68 0d a7 cf 7e 53 90 4b af f9 e8 1f 09 fa 0a 1f c6 2f 39 d3
7d da 64 b3 d1 c3 10 fe d3 fe 08 1b ad 8e 09 ef a6 c1 e2 7f 1b 11 3c 8a fd bc be b2 14 4f 31 4e 2c
09 1c d9 e5 27 92 07 90 0e 33 43 86 ed e9 79 4a 38 ec f9 ae 90 5f 72 e0 9b 76 84 79 24 78 b4 1a db
e6 25

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 35.232	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**
2020-07	-	-	-	-	Update to Rel-16 version (MCC)	15.0.0	**16.0.0**

History

Document history		
V16.0.0	August 2020	Publication