Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2.
Document 1: UEA2 and UIA2 Specification
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>10th January 2006</td>
<td>Publication</td>
</tr>
<tr>
<td>V1.1</td>
<td>6th September 2006</td>
<td>No change to the algorithm specification at all, just removal of an unwanted page header</td>
</tr>
</tbody>
</table>
PREFACE

This specification has been prepared by the 3GPP Task Force, and gives a detailed specification of the 3GPP confidentiality algorithm \textit{UEA2} and the 3GPP integrity algorithm \textit{UIA2}.

This document is the first of four, which between them form the entire specification of 3GPP Confidentiality and Integrity Algorithms:

- Specification of the 3GPP Confidentiality and Integrity Algorithms \textit{UEA2} & \textit{UIA2}.
  Document 1: \textit{UEA2} and \textit{UIA2} Algorithm Specifications.

- Specification of the 3GPP Confidentiality and Integrity Algorithms \textit{UEA2} & \textit{UIA2}.

- Specification of the 3GPP Encryption and Confidentiality Algorithms \textit{UEA2} & \textit{UIA2}.
  Document 3: Implementors’ Test Data.

- Specification of the 3GPP Encryption and Confidentiality Algorithms \textit{UEA2} & \textit{UIA2}.
  Document 4: Design Conformance Test Data.

The normative part of the specification of the \textit{UEA2} (confidentiality) and \textit{UIA2} (integrity) algorithms is in the main body of this document. The annexes to this document are purely informative.

The informative section of this document includes four informative annexes: Annex 1 contains remarks about the mathematical background of some functions of \textit{UIA2}. Annex 2 contains implementation options for some functions of \textit{UIA2}. Annex 3 contains illustrations of functional elements of the algorithms, while Annex 4 contains an implementation program listing of the cryptographic algorithm specified in the main body of this document, written in the programming language C.

The normative section of the specification of the stream cipher (\textit{SNOW 3G}) on which they are based is in the main body of Document 2. The annexes to that document, and Documents 3 and 4 above, are purely informative.
# TABLE OF CONTENTS

1. OUTLINE OF THE NORMATIVE PART ................................................................. 8

2. INTRODUCTORY INFORMATION .................................................................. 8
   2.1. Introduction............................................................................................... 8
   2.2. Notation .................................................................................................... 8
   2.3. List of Variables ...................................................................................... 10

3. CONFIDENTIALITY ALGORITHM UEA2 ......................................................... 11
   3.1. Introduction............................................................................................... 11
   3.2. Inputs and Outputs .................................................................................. 11
   3.3. Components and Architecture ............................................................... 11
   3.4. Initialisation .............................................................................................. 11
   3.5. Keystream Generation ............................................................................. 12
   3.6. Encryption/Decryption ............................................................................ 12

4. INTEGRITY ALGORITHM UIA2 ...................................................................... 13
   4.1. Introduction............................................................................................... 13
   4.2. Inputs and Outputs .................................................................................. 13
   4.3. Components and Architecture ............................................................... 13
   4.4. Initialisation .............................................................................................. 14
   4.5. Calculation ............................................................................................... 15

ANNEX 1 Remarks about the mathematical background of some operations of the UIA2 Algorithm ................................................................. 17
   1.1. The function EVAL_M ............................................................................... 17
   1.2. The function MUL(V, P, c) ...................................................................... 17

ANNEX 2 Implementation options for some operations of the UIA2 Algorithm ................................................................. 18
   2.1. Procedure Pre_Mul_P ............................................................................... 18
   2.2. Function Mul_P ........................................................................................ 18

ANNEX 3 Figures of the UEA2 and UIA2 Algorithms ............................................ 20

ANNEX 4 Simulation Program Listing .................................................................. 23
   4.1. UEAII ....................................................................................................... 23
   4.2. UIAII ....................................................................................................... 24
REFERENCES


NORMATIVE SECTION

This part of the document contains the normative specification of the Confidentiality and Integrity algorithms.
1. OUTLINE OF THE NORMATIVE PART

Section 2 introduces the algorithm and describes the notation used in the subsequent sections.

Section 3 specifies the confidentiality algorithm UEA2.

Section 4 specifies the integrity algorithm UIA2.

2. INTRODUCTORY INFORMATION

2.1. Introduction

Within the security architecture of the 3GPP system there are standardised algorithms for confidentiality (f8) and integrity (f9). A first set of algorithms for f8 and f9 (UEA1 and UIA1) has already been specified [3]. A second set of algorithms for f8 and f9 (UEA2 and UIA2) are fully specified here: The second set of these algorithms is based on the SNOW 3G algorithm that is specified in a companion document [5].

The confidentiality algorithm UEA2 is a stream cipher that is used to encrypt/decrypt blocks of data under a confidentiality key CK. The block of data may be between 1 and 20000 bits long. The algorithm uses SNOW 3G as a keystream generator.

The integrity algorithm UIA2 computes a 32-bit MAC (Message Authentication Code) of a given input message using an integrity key IK. The approach adopted uses SNOW 3G.

2.2. Notation

2.2.1. Radix

We use the prefix 0x to indicate hexadecimal numbers.

2.2.2. Conventions

We use the assignment operator ‘=’, as used in several programming languages. When we write

<variable> = <expression>

we mean that <variable> assumes the value that <expression> had before the assignment took place. For instance,

x = x + y + 3

means

(new value of x) becomes (old value of x) + (old value of y) + 3.
2.2.3. Bit/Byte ordering

All data variables in this specification are presented with the most significant bit (or byte) on the left hand side and the least significant bit (or byte) on the right hand side. Where a variable is broken down into a number of sub-strings, the left most (most significant) sub-string is numbered 0, the next most significant is numbered 1 and so on through to the least significant.

For example an n-bit MESSAGE is subdivided into 64-bit substrings MB₀, MB₁, MB₂, ....

So if we have a message:

0x0123456789ABCDEFFEDCBA98765432108654381AB594FC28786404C50A37…

we have:

\[ MB₀ = 0x0123456789ABCDE \]
\[ MB₁ = 0xFEDCBA9876543210 \]
\[ MB₂ = 0x86545381AB594FC2 \]
\[ MB₃ = 0x8786404C50A37… \]

In binary this would be:

00000001001000110100010101100111100010011010101111011111111111111110

with \[ MB₀ = 00000001001000110100010101100111100010011010101111011111111111111 \]
\[ MB₁ = 1111111011011100101110101001100001110100101000011001000010000 \]
\[ MB₂ = 100001100101000101000111000001110101101101001000011001000010000 \]
\[ MB₃ = 100001111000011001110000001001100101000011111111100010 \]

2.2.4. List of Symbols

\[ = \] The assignment operator.
\[ ⊕ \] The bitwise exclusive-OR operation
\[ || \] The concatenation of the two operands.
\[ \lceil x \rceil \] The smallest integer greater than or equal to the real number \( x \).
\[ \&_n \] The bitwise AND operation in an \( n \)-bit register.
\[ <<_n \] \( t \)-bit left shift in an \( n \)-bit register.
\[ >>_n \] \( t \)-bit right shift in an \( n \)-bit register
2.3. List of Variables

BEARER the 5-bit input to the \textit{UEA2} function.

CK the 128-bit confidentiality key.

COUNT the 32-bit time variant input to the \textit{UEA2} and \textit{UIA2} functions (COUNT-C for \textit{UEA2} and COUNT-I for \textit{UIA2}).

DIRECTION the 1-bit input to both the \textit{UEA2} and \textit{UIA2} functions indicating the direction of transmission (uplink or downlink).

FRESH the 32-bit random input to the \textit{UIA2} function.

IBS the input bit stream to the \textit{UEA2} function.

IK the 128-bit integrity key.

KS\([i]\) the \(i\)th bit of keystream produced by the keystream generator.

LENGTH the input to the \textit{UEA2} and \textit{UIA2} functions which specifies the number of bits in the input bitstream (1-20000).

MAC-I the 32-bit message authentication code (MAC) produced by the integrity function \textit{UIA2}.

MESSAGE the input bitstream of LENGTH bits that is to be processed by the \textit{UIA2} function.

OBS the output bit stream from the \textit{UEA2} function.

\(z_1, z_2, \ldots\) the 32-bit words forming the keystream sequence of \textit{SNOW 3G}. The word produced first is \(z_1\), the next word \(z_2\) and so on.
3. CONFIDENTIALITY ALGORITHM UEA2

3.1. Introduction

The confidentiality algorithm UEA2 is a stream cipher that encrypts/decrypts blocks of data between 1 and 20000 bits in length.

3.2. Inputs and Outputs

The inputs to the algorithm are given in Table 1, the output in Table 2:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Size (bits)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT-C</td>
<td>32</td>
<td>Frame dependent input COUNT-C[0]…COUNT-C[31]</td>
</tr>
<tr>
<td>BEARER</td>
<td>5</td>
<td>Bearer identity BEARER[0]…BEARER[4]</td>
</tr>
<tr>
<td>DIRECTION</td>
<td>1</td>
<td>Direction of transmission DIRECTION[0]</td>
</tr>
<tr>
<td>CK</td>
<td>128</td>
<td>Confidentiality key CK[0]…CK[127]</td>
</tr>
<tr>
<td>LENGTH</td>
<td>16</td>
<td>The number of bits to be encrypted/decrypted</td>
</tr>
<tr>
<td>IBS</td>
<td>LENGTH</td>
<td>Input bit stream IBS[0]….IBS[LENGTH-1]</td>
</tr>
</tbody>
</table>

Table 1. UEA2 inputs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Size (bits)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBS</td>
<td>LENGTH</td>
<td>Output bit stream OBS[0]….OBS[LENGTH-1]</td>
</tr>
</tbody>
</table>

Table 2. UEA2 output

3.3. Components and Architecture

The keystream generator is based on SNOW 3G that is specified in [5]. SNOW 3G is a word oriented stream cipher and generates a keystream in multiples of 32-bits.

3.4. Initialisation

In this section we define how the keystream generator is initialised with the key variables before the generation of keystream bits.

All variables have length 32 and are presented with the most significant bit on the left hand side and the least significant bit on the right hand side.
\[ K_3 = CK[0] \parallel CK[1] \parallel CK[2] \parallel ... \parallel CK[31] \]
\[ K_2 = CK[32] \parallel CK[33] \parallel CK[34] \parallel ... \parallel CK[63] \]
\[ K_1 = CK[64] \parallel CK[65] \parallel CK[66] \parallel ... \parallel CK[95] \]
\[ K_0 = CK[96] \parallel CK[97] \parallel CK[98] \parallel ... \parallel CK[127] \]
\[ IV_3 = COUNT-C[0] \parallel COUNT-C[1] \parallel COUNT-C[2] \parallel ... \parallel COUNT-C[31] \]
\[ IV_2 = BEARER[0] \parallel BEARER[1] \parallel ... \parallel BEARER[4] \parallel DIRECTION[0] \parallel 0 \parallel ... \parallel 0 \]
\[ IV_1 = COUNT-C[0] \parallel COUNT-C[1] \parallel COUNT-C[2] \parallel ... \parallel COUNT-C[31] \]
\[ IV_0 = BEARER[0] \parallel BEARER[1] \parallel ... \parallel BEARER[4] \parallel DIRECTION[0] \parallel 0 \parallel ... \parallel 0 \]

SNOW 3G is initialised as described in document [5].

### 3.5. Keystream Generation

Set \[ L = \left\lfloor \frac{\text{LENGTH}}{32} \right\rfloor. \]

SNOW 3G is run as described in document [5] to produce the keystream consisting of the 32-bit words \( z_1 \) \( ... \) \( z_L \). The word produced first is \( z_1 \), the next word \( z_2 \) and so on.

The sequence of keystream bits is \( KS[0] \) \( ... \) \( KS[\text{LENGTH}-1] \), where \( KS[0] \) is the most significant bit and \( KS[31] \) is the least significant bit of \( z_1 \), \( KS[32] \) is the most significant bit of \( z_2 \) and so on.

### 3.6. Encryption/Decryption

Encryption/decryption operations are identical operations and are performed by the exclusive-OR of the input data (\( IBS \)) with the generated keystream (\( KS \)).

For each integer \( i \) with \( 0 \leq i \leq \text{LENGTH}-1 \) we define:

\[ OBS[i] = IBS[i] \oplus KS[i]. \]
4. INTEGRITY ALGORITHM UIA2

4.1. Introduction

The integrity algorithm UIA2 computes a Message Authentication Code (MAC) on an input message under an integrity key $IK$. The message may be between 1 and 20000 bits in length.

For ease of implementation the algorithm is based on the same stream cipher (SNOW 3G) as is used by the confidentiality algorithm UEA2.

4.2. Inputs and Outputs

The inputs to the algorithm are given in table 3, the output in table 4:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Size (bits)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT-I</td>
<td>32</td>
<td>Frame dependent input COUNT-I[0]…COUNT-I[31]</td>
</tr>
<tr>
<td>FRESH</td>
<td>32</td>
<td>Random number FRESH[0]…FRESH[31]</td>
</tr>
<tr>
<td>DIRECTION</td>
<td>1</td>
<td>Direction of transmission DIRECTION[0]</td>
</tr>
<tr>
<td>IK</td>
<td>128</td>
<td>Integrity key IK[0]…IK[127]</td>
</tr>
<tr>
<td>LENGTH</td>
<td>64</td>
<td>The number of bits to be ‘MAC’d</td>
</tr>
<tr>
<td>MESSAGE</td>
<td>LENGTH</td>
<td>Input bit stream</td>
</tr>
</tbody>
</table>

Table 3. UIA2 inputs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Size (bits)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC-I</td>
<td>32</td>
<td>Message authentication code MAC-I[0]…MAC-I[31]</td>
</tr>
</tbody>
</table>

Table 4. UIA2 output

4.3. Components and Architecture

4.3.1. SNOW 3G

The integrity function uses SNOW 3G that is specified in [5]. SNOW 3G is a word oriented stream cipher and generates from the key and an initialisation variable five 32-bit-words $z_1, z_2, z_3, z_4$ and $z_5$.

4.3.2. MULx

MULx maps 128 bits to 64 bits. Let $V$ and $c$ be 64-bit input values. Then MULx is defined: If the leftmost (i.e. the most significant) bit of $V$ equals 1, then
\[ MULx(V, c) = (V \ll_{64} 1) \oplus c, \]
else
\[ MULx(V, c) = V \ll_{64} 1. \]

### 4.3.3. MULxPOW

MULxPOW maps 128 bits and a positive integer \( i \) to 64 bit. Let \( V \) and \( c \) be 64-bit input values, then MULxPOW\((V, i, c)\) is recursively defined:
If \( i \) equals 0, then
\[ MULxPOW(V, i, c) = V, \]
else
\[ MULxPOW(V, i, c) = MULx(MULxPOW(V, i - 1, c), c). \]

### 4.3.4. MUL

MUL maps 192 bits to 64 bit. Let \( V, P \) and \( c \) be 64-bit input values.

Then the 64-bit output \( \text{result} \) of MUL\((V, P, c)\) is computed as follows:

- \( \text{result} = 0. \)
- for \( i = 0 \) to 63 inclusive
  - if \((P >>_{64} i) \&_{64} 0x01 \) equals 0x01, then
    \[ \text{result} = \text{result} \oplus MULxPOW(V, i, c). \]

### 4.4. Initialisation

In this section we define how the keystream generator is initialised with the key and initialisation variables before the generation of keystream bits.

All variables have length 32 bits and are presented with the most significant bit on the left hand side and the least significant bit on the right hand side.

\[
\begin{align*}
K_3 & = \text{IK}[0] \parallel \text{IK}[1] \parallel \text{IK}[2] \parallel \ldots \parallel \text{IK}[31] \\
K_2 & = \text{IK}[32] \parallel \text{IK}[33] \parallel \text{IK}[34] \parallel \ldots \parallel \text{IK}[63] \\
K_1 & = \text{IK}[64] \parallel \text{IK}[65] \parallel \text{IK}[66] \parallel \ldots \parallel \text{IK}[95] \\
K_0 & = \text{IK}[96] \parallel \text{IK}[97] \parallel \text{IK}[98] \parallel \ldots \parallel \text{IK}[127] \\
\end{align*}
\]

\[
\begin{align*}
IV_3 & = \text{COUNT-I}[0] \parallel \text{COUNT-I}[1] \parallel \text{COUNT-I}[2] \parallel \ldots \parallel \text{COUNT-I}[31] \\
IV_2 & = \text{FRESH}[0] \parallel \text{FRESH}[1] \parallel \text{FRESH}[2] \parallel \ldots \parallel \text{FRESH}[31] \\
IV_1 & = \text{DIRECTION}[0] \oplus \text{COUNT-I}[0] \parallel \text{COUNT-I}[1] \parallel \text{COUNT-I}[2] \parallel \ldots \parallel \text{COUNT-I}[31] \\
IV_0 & = \text{FRESH}[0] \parallel \text{FRESH}[1] \parallel \ldots \parallel \text{FRESH}[15] \parallel \text{FRESH}[16] \oplus \text{DIRECTION}[0] \parallel \text{FRESH}[17] \parallel \ldots \parallel \text{FRESH}[31] \\
\end{align*}
\]

SNOW 3G is initialised as described in document [5].
4.5.  Calculation

Set $D = \lceil \text{LENGTH} / 64 \rceil + 1$.

$\text{SNOW 3G}$ is run as described in document [5] in order to produce 5 keystream words $z_1, z_2, z_3, z_4, z_5$.

Set $P = z_1 \parallel z_2$

and $Q = z_3 \parallel z_4$.

Let $\text{OTP}[0], \text{OTP}[1], \text{OTP}[2], \ldots, \text{OTP}[31]$ be bit-variables such that

$$z_5 = \text{OTP}[0] \parallel \text{OTP}[1] \parallel \ldots \parallel \text{OTP}[31],$$

i.e. $\text{OTP}[0]$ is the most and $\text{OTP}[31]$ the least significant bit of $z_5$.

For $0 \leq i \leq D - 3$ set

$$M_i = \text{MESSAGE}[64i] \parallel \text{MESSAGE}[64i+1] \parallel \ldots \parallel \text{MESSAGE}[64i+63].$$

Set

$$M_{D-2} = \text{MESSAGE}[64(D-2)] \parallel \ldots \parallel \text{MESSAGE}[\text{LENGTH}-1] \parallel 0\ldots0.$$ 

Let $\text{LENGTH}[0], \text{LENGTH}[1], \ldots, \text{LENGTH}[63]$ be the bits of the 64-bit representation of $\text{LENGTH}$, where $\text{LENGTH}[0]$ is the most and $\text{LENGTH}[63]$ is the least significant bit.

Set $M_{D-1} = \text{LENGTH}[0] \parallel \text{LENGTH}[1] \parallel \ldots \parallel \text{LENGTH}[63]$.

Compute the function $\text{Eval}_M$:

- Set the 64-bit variable $\text{EVAL} = 0$.

- for $i = 0$ to $D - 2$ inclusive:
  - $\text{EVAL} = \text{Mul}(\text{EVAL} \oplus M_i, P, 0x000000000000001b)$.

Set $\text{EVAL} = \text{EVAL} \oplus M_{D-1}$

Now we multiply $\text{EVAL}$ by $Q$:

$$\text{EVAL} = \text{Mul}(\text{EVAL}, Q, 0x0000000000000001b).$$

Let $\text{EVAL} = e_0 \parallel e_1 \parallel \ldots \parallel e_{63}$ with $e_0$ the most and $e_{63}$ the least significant bit.

For $0 \leq i \leq 31$, set

$$\text{MAC-I}[i] = e_i \oplus \text{OTP}[i].$$

The bits $e_{32}, \ldots, e_{63}$ are discarded.
INFORMATIVE SECTION

This part of the document is purely informative and does not form part of the normative specification of the Confidentiality and Integrity algorithms.
ANNEX 1
Remarks about the mathematical background of some operations of the UIA2 Algorithm

1.1. The function EVAL_M

The first part (the function EVAL_M) of the calculations for the UIA2 algorithm corresponds to the evaluation of a polynomial at a secret point: From the bits and the length of MESSAGE a polynomial \( M \in GF(2^64)[X] \) is defined. This polynomial is evaluated at the point \( P \in GF(2^64) \) defined by \( z_1||z_2 \).

This can be seen as follows:

Consider the Galois Field \( GF(2^{64}) \) where elements of the field are represented as polynomials over \( GF(2) \) modulo the irreducible polynomial \( x^{64} + x^4 + x^3 + x + 1 \).

Variables consisting of 64 bits can be mapped to this field by interpreting the bits as the coefficients of the corresponding polynomial.

For example for \( 0 \leq i \leq D-3 \) the variable \( M_i = MESSAGE[64i] || MESSAGE[64i+1] ||...|| MESSAGE[64i+62] || MESSAGE[64i+63] \) is interpreted as \( MESSAGE[64i]x^{63} + MESSAGE[64i+1]x^{62} + ... + MESSAGE[64i+62]x + MESSAGE[64i+63] \).

Construct the polynomial \( M \) of degree \( D-1 \) in \( GF(2^{64})[X] \) as

\[
M(X) = M_0X^{D-1} + M_1X^{D-2} + ... + M_{D-2}X + M_{D-1}.
\]

Evaluate the polynomial \( M \) at the point \( P \), i.e. compute

\[
M(P) = M_0P^{D-1} + M_1P^{D-2} + ... + M_{D-2}P + M_{D-1} = (\ldots (M_2P + M_1P + M_2P + \ldots + M_{D-2}P)P + \ldots + M_1P + M_0P).
\]

This is done in the function Eval_M in 4.5.

1.2. The function MUL(V, P, c)

The function MUL(\( V, P, c \)) (see 4.3.4) corresponds to a multiplication of \( V \) by \( P \) in \( GF(2^{64}) \). Here \( GF(2^{64}) \) is described as \( GF(2)(\beta) \) where \( \beta \) is a root of the \( GF(2)[X] \) polynomial \( x^{64} + c_0X^{63} + ... + c_{62}X + c_{63} \) and \( c = c_0 || c_1 || ... || c_{63} \).

3GPP Confidentiality and Integrity Algorithms UEA2&UIA2  page 17 of 27
UEA2 and UIA2 Specification Version 1.1
ANNEX 2
Implementation options for some operations of the UIA2 Algorithm

The function MUL (see 4.3.4) can be implemented using table lookups. This might accelerate
evaluation of the function EVAL_M, as for the evaluation of the polynomial only
multiplication by a constant factor \( P \) is needed.

There are different possible sizes for the tables. Here we use 8 tables with 256 entries, but for example it is also possible to use 16 tables with 16 entries.

In order to execute MUL by table-lookups first Pre_Mul_P (see 2.1) is executed, which generates the tables. Then in MUL_P (see 2.2) the multiplication is performed by 8 table-lookups and an xor of the results.

Hence in 4.5 instead of \( \text{EVAL} = \text{Mul} (\text{EVAL} \oplus M_i, P, 0x1b) \) we can use \( \text{EVAL} = \text{Mul_P} (\text{EVAL} \oplus M_i) \).

2.1. Procedure Pre_Mul_P

In order to be able to compute Mul_P (see 2.2) the procedure Pre_Mul_P is executed once before the first call of Mul_P.
Pre_Mul_P computes from the 64-bit input \( P \) eight tables \( \text{PM}[0], \text{PM}[1], \ldots, \text{PM}[7] \). Each of these tables contains 256 entries \( \text{PM}[j][0], \text{PM}[j][1], \ldots, \text{PM}[j][255] \) with 64 bits.

For \( 0 \leq j \leq 7 \) and \( 0 \leq X \leq 255 \) the value \( \text{PM}[j][X] \) corresponds to \( X \cdot P \times 8^j \).

Let \( r \) be the 64-bit value \( 0x000000000000001b \).

- The tables are computed as follows: \( \text{PM}[0][0] = \text{PM}[1][0] = \text{PM}[2][0] = \text{PM}[3][0] = \text{PM}[4][0] = \text{PM}[5][0] = \text{PM}[6][0] = \text{PM}[7][0] = 0 \).
- \( \text{PM}[0][1] = P \).
- for \( i = 1 \) to 63 inclusive:
  - \( \text{PM}[i \ggg 3][1 \lll 8 ((i - 1) \& 8 \times 0x07)] = \text{PM}[(i - 1) \gg 3][1 \lll 8 ((i - 1) \& 8 \times 0x07)] \ll 64 \times 1 \).
  - if the leftmost bit of \( \text{PM}[(i - 1) \ggg 3][1 \lll (i - 1) \& 8 \times 0x07)] \) equals 1, then \( \text{PM}[i \ggg 3][1 \lll (i \& 8 \times 0x07)] = \text{PM}[i \gg 3][1 \lll (i \& 8 \times 0x07)] \oplus r \).
- for \( i = 0 \) to 7 inclusive
  - for \( j = 1 \) to 7 inclusive
    - for \( k = 1 \) to \( (1 \lll 8 j) - 1 \) inclusive
      - \( \text{PM}[i][(1 \lll 8 j) + k] = \text{PM}[i][1 \lll 8 j] \oplus \text{PM}[i][k] \).

2.2. Function Mul_P

The function Mul_P maps a 64-bit input \( X \) to a 64-bit output.
Let $X = X_0 \| X_1 \| X_2 \| X_3 \| X_4 \| X_5 \| X_6 \| X_7$, with $X_0$ the most and $X_7$ the least significant byte.

Compute $\text{Mul}_P(X)$ as

$$\text{Mul}_P(X) = \text{PM}[0][X_7] \oplus \text{PM}[1][X_6] \oplus \text{PM}[2][X_5] \oplus \text{PM}[3][X_4] \oplus \text{PM}[4][X_3] \oplus \text{PM}[5][X_2] \oplus \text{PM}[6][X_1] \oplus \text{PM}[7][X_0].$$
ANNEX 3
Figures of the UEA2 and UIA2 Algorithms

Figure 1: UEA2 Keystream Generator
Figure 2: UIA2 Integrity function, part 1
Figure 3: UIA2 Integrity function, part 2
ANNEX 4
Simulation Program Listing

4.1. UEAII

4.1.1 Header File

```c
/*---------------------------------------------------------
*     f8.h
*---------------------------------------------------------*/
#ifndef F8_H_
#define F8_H_

#include "SNOW_3G.h"

/* f8.
* Input key: 128 bit Confidentiality Key.
* Input count:32-bit Count, Frame dependent input.
* Input bearer: 5-bit Bearer identity (in the LSB side).
* Input dir:1 bit, direction of transmission.
* Input data: length number of bits, input bit stream.
* Input length: 16 bit Length, i.e., the number of bits to be encrypted or
*               decrypted.
* Output data: Output bit stream. Assumes data is suitably memory
*              allocated.
* Encrypts/decrypts blocks of data between 1 and 20000 bits in length as
* defined in Section 3.
*/

void f8( u8 *key, int count, int bearer, int dir, u8 *data, int length );
#endif
```

4.1.2 Code

```c
/*---------------------------------------------------------
*     f8.c
*---------------------------------------------------------*/
#include "f8.h"
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

/* f8.
* Input key: 128 bit Confidentiality Key.
* Input count:32-bit Count, Frame dependent input.
* Input bearer: 5-bit Bearer identity (in the LSB side).
* Input dir:1 bit, direction of transmission.
* Input data: length number of bits, input bit stream.
* Input length: 16 bit Length, i.e., the number of bits to be encrypted or
*               decrypted.
* Output data: Output bit stream. Assumes data is suitably memory
*              allocated.
* Encrypts/decrypts blocks of data between 1 and 20000 bits in length as
* defined in Section 3.
*/

void f8( u8 *key, int count, int bearer, int dir, u8 *data, int length )
{
    u32 K[4],IV[4];
    int n = ( length + 31 ) / 32;
    int i=0;
    u32 *KS;
```
/*Initialisation*/

/* Load the confidentiality key for SNOW 3G initialization as in section 3.4. */
memcpy(K+3,key+0,4);  /*K[3] = key[0]; we assume
K[3]=key[0]|key[1]|...|key[31] , with key[0] the
* most important bit of key*/
memcpy(K+2,key+4,4);  /*K[2] = key[1];*/
memcpy(K+1,key+8,4);  /*K[1] = key[2];*/
memcpy(K+0,key+12,4); /*K[0] = key[3]; we assume
K[0]=key[96]|key[97]|...|key[127] , with key[127] the
* least important bit of key*/

/* Prepare the initialization vector (IV) for SNOW 3G initialization as in
section 3.4. */
IV[3] = count;
IV[2] = (bearer << 27) | ({(dir & 0x1) << 26};
IV[1] = IV[3];
IV[0] = IV[2];

/* Run SNOW 3G algorithm to generate sequence of key stream bits KS*/
Initialize(K,IV);

KS = (u32 *)malloc(4*n);
GenerateKeystream(n,(u32*)KS);

/* Exclusive-OR the input data with keystream to generate the output bit
stream */
for (i=0;i<n*4;i++)
  data[i] ^= *(((u8*)KS)+i);

free(KS);
}

/* End of f8.c */

4.2. UIAII

4.2.1 Header File

/*-----------------------------------------------
 * f9.h
 *-----------------------------------------------*/
#ifndef F9_H_
#define F9_H_
#include "SNOW_3G.h"
#define F9_H_
#include "SNOW_3G.h"

/*9.*/
*/
* Input key: 128 bit Integrity Key.
* Input count: 32-bit Count, Frame dependent input.
* Input fresh: 32-bit Random number.
* Input dir: 1 bit, direction of transmission (in the LSB).
* Input data: length number of bits, input bit stream.
* Input length: 64 bit Length, i.e., the number of bits to be MAC'd.
* Output : 32 bit block used as MAC
* Generates 32-bit MAC using UIA2 algorithm as defined in Section 4.
*/

u8* f9(u8* key, int count, int fresh, int dir, u8 *data, u64 length);
#endif
4.2.2 Code

```c
/*---------------------------------------------------------
*     f9.c
*---------------------------------------------------------*/
#include "f9.h"
#include <stdio.h>
#include <math.h>
#include <string.h>

/* MUL64x.
* Input V: a 64-bit input.
* Input c: a 64-bit input.
* Output : a 64-bit output.
* A 64-bit memory is allocated which is to be freed by the calling
* function.
* See section 4.3.2 for details.
*/

u64 MUL64x(u64 V, u64 c)
{
    if ( V & 0x8000000000000000 )
        return (V << 1) ^ c;
    else
        return V << 1;
}

/* MUL64xPOW.
* Input V: a 64-bit input.
* Input i: a positive integer.
* Input c: a 64-bit input.
* Output : a 64-bit output.
* A 64-bit memory is allocated which is to be freed by the calling
* function.
* See section 4.3.3 for details.
*/

u64 MUL64xPOW(u64 V, u8 i, u64 c)
{
    if ( i == 0)
        return V;
    else
        return MUL64x( MUL64xPOW(V,i-1,c) , c);
}

/* MUL64.
* Input V: a 64-bit input.
* Input P: a 64-bit input.
* Input c: a 64-bit input.
* Output : a 64-bit output.
* A 64-bit memory is allocated which is to be freed by the calling
* function.
* See section 4.3.4 for details.
*/

u64 MUL64(u64 V, u64 P, u64 c)
{
    u64 result = 0;
    int i = 0;

    for ( i=0; i<64; i++)
    {
        if( ( P>>i ) & 0x1 )
            result ^= MUL64xPOW(V,i,c);
    }
```
return result;
}

/* mask32bit.
* Input n: an integer in 1-32.
* Output : a 32 bit mask.
* Prepares a 32 bit mask with required number of 1 bits on the MSB side.
*/

u32 mask32bit(int n)
{
    u32 mask=0x0;
    if ( n%32 == 0 )
        return 0xffffffff;

    while (n--)
        mask = (mask>>1) ^ 0x80000000;
    return mask;
}

/* f9.
* Input key: 128 bit Integrity Key.
* Input count:32-bit Count, Frame dependent input.
* Input fresh: 32-bit Random number.
* Input dir:1 bit, direction of transmission (in the LSB).
* Input data: length number of bits, input bit stream.
* Input length: 64 bit Length, i.e., the number of bits to be MAC'd.
* Output  : 32 bit block used as MAC
* Generates 32-bit MAC using UIA2 algorithm as defined in Section 4.
*/

u8* f9( u8* key, int count, int fresh, int dir, u8 *data, u64 length)
{
    u32 K[4],IV[4], z[5];
    int i=0,D;
    static u32 MAC_I = 0; /* static memory for the result */
    u64 EVAL;
    u64 V;
    u64 P;
    u64 Q;
    u64 c;

    u64 M_D_2;
    int rem_bits = 0;
    u32 mask = 0;
    u32 *message;

    message = (u32*)data; /* To operate 32 bit message internally. */

    /* Load the Integrity Key for SNOW3G initialization as in section 4.4. */
    memcpy(K+3,key+0,4);  /*K[3] = key[0]; we assume
    K[3]=key[0]||key[1]||...||key[31] , with key[0] the
    * most important bit of key*/
    memcpy(K+2,key+4,4);  /*K[2] = key[1];*/
    memcpy(K+1,key+8,4);  /*K[1] = key[2];*/
    memcpy(K+0,key+12,4); /*K[0] = key[3]; we assume
    K[0]=key[96]||key[97]||...||key[127] , with key[127] the
    * least important bit of key*/

    /* Prepare the Initialization Vector (IV) for SNOW3G initialization as in
    section 4.4. */
    IV[3] = count;
    IV[2] = fresh;
    IV[1] = count ^ ( dir << 31 );
    IV[0] = fresh ^ (dir << 15);


    /* Run SNOW 3G to produce 5 keystream words z_1, z_2, z_3, z_4 and z_5. */
Initialize(K,IV);
GenerateKeystream(5,z);

\[ P = (u64)z[0] \ll 32 \mid (u64)z[1] ; \]
\[ Q = (u64)z[2] \ll 32 \mid (u64)z[3] ; \]

/* Calculation */
\[ D = \text{ceil}(\text{length} / 64.0) + 1 ; \]
\[ \text{EVAL} = 0 ; \]
\[ c = 0x1b ; \]

/* for 0 \leq i \leq D-3 */
for (i=0;i<D-2;i++)
{
    \[ V = \text{EVAL} \wedge (u64)\text{message}[2*i] \ll 32 \mid (u64)\text{message}[2*i+1] ; \]
    \[ \text{EVAL} = \text{MUL64}(V,P,c) ; \]
}

/* for D-2 */
\[ \text{rem_bits} = \text{length} \% 64 ; \]
if (rem_bits == 0)
    \[ \text{rem_bits} = 64 ; \]
\[ \text{mask} = \text{mask32bit}(\text{rem_bits}\%32) ; \]
if (rem_bits > 32)
{
    \[ \text{M}_D_2 = (u64)\text{message}[2*(D-2)] \ll 32 \mid (u64)\text{message}[2*(D-2)+1] \& \text{mask} ; \]
} else
{
    \[ \text{M}_D_2 = (u64)\text{message}[2*(D-2)] \& \text{mask} \ll 32 ; \]
}
\[ V = \text{EVAL} \wedge \text{M}_D_2 ; \]
\[ \text{EVAL} = \text{MUL64}(V,P,c) ; \]

/* for D-1 */
\[ \text{EVAL} \wedge= \text{length} ; \]
/* Multiply by Q */
\[ \text{EVAL} = \text{MUL64}(\text{EVAL},Q,c) ; \]

\[ \text{MAC}_I = (u32)(\text{EVAL} >> 32) \wedge z[4] ; \]
\[ \text{return } (u8*) \& \text{MAC}_I ; \]

/* End of f9.c */

/*-----------------------------------------------*/