GM/T 0001.2

ZUC Stream Cipher Algorithm

Part 2: Confidentiality Algorithm

Cryptography Standardization

Technical Committee of China

Issued on 2012-03-21 Translated on 2024-10-30

Contents

Foreword

GM/T 0001 " ZUC Stream Cipher Algorithm" consists of three parts:

Part 1: Algorithm Description;

Part 2: Confidentiality Algorithm;

Part 3: Integrity Algorithm.

This part is Part 2 of GM/T 0001.

1 Scope

This part of GM/T 0001 describes the confidentiality algorithm based on the ZUC stream cipher algorithm. It is applicable to the development, testing, and use of products related to the confidentiality algorithm based on the ZUC stream cipher algorithm.

2 Normative References

The following documents are essential for the application of this document. For dated references, only the dated version applies. For undated references, the latest version (including all amendments) applies.

- GM/T 0001.1 ZUC Stream Cipher Algorithm Part 1: Algorithm Description

3 Terms and Definitions

The terms and definitions defined in GM/T 0001.1 apply to this document.

4 Symbols and Abbreviations

4.1 Symbols

The following symbols apply to this document:

$\oplus$: Bitwise XOR operation

$\lceil x \rceil$: Smallest integer no less than x

|| : String concatenation operator

4.2 Abbreviations

The following abbreviations apply to this document:

- CK: Confidentiality Key
- IV: Initial Vector

- IBS: Input Bit Stream
- LTE: Long Term Evolution
- OBS: Output Bit Stream
- 3GPP: The 3rd Generation Partnership Project

5 Algorithm Description

5.1 Algorithm Input and Output

The input parameters of this algorithm are shown in Table 1, and the output parameters are shown in Table 2.

Table 1 The inputs

Parameter	Size(bits)	Remark
CK	128	Confidentiality Key
IV	128	Initialization Vector
LENGTH	32	Bit length of the plaintext message stream
IBS	LENGTH	Input bit stream with length LENGTH

Table 2 The output

Parameter	Size(bits)	Remark
OBS	LENGTH	Output bit stream with length LENGTH

5.2 Algorithm Workflow

5.2.1 Generating the Key Stream

Let $L = \lceil \text{LENGTH} / 32 \rceil$. Use the confidentiality key (CK), initialization vector (IV), and L as input parameters, and generate a key stream of L words using the method given in 5.6 of GM/T 0001.1. Represent the generated key stream as a bit string $K[0],K[1],\ldots,K[32\times L-1]$, where $K[0]$ is the most significant bit of the first key word, $K[31]$ is the least significant bit of the first key word, and so on.

In the 3GPP LTE application scenario, refer to Appendix A for the initialization method of the initialization vector (IV).

5.2.2 Encryption and Decryption

Let the input bit stream of length LENGTH be:

IBS=IBS[0] || IBS[1] || IBS[2] || … || IBS[LENGTH−1]

The corresponding output bit stream is:

OBS=OBS[0] || OBS[1] || OBS[2] || … || OBS[LENGTH−1]

Where both IBS[*i*] and OBS[*i*] are bits, *i*=0,1,2,…,LENGTH−1. Compute the output bit stream: OBS[*i*]=IBS[*i*] ⊕ K[*i*], *i*=0,1,2,…,LENGTH−1

For the 3GPP LTE application scenario, refer to Appendix B for algorithm calculation examples.

Appendix A
(Informative Appendix)
Parameter Initialization in 3GPP LTE

A.1 Input and Output Parameters

The assignment of input and output parameters in 3GPP LTE is specified in Table A.1 and Table A.2.

Table A.1 The inputs to 128-EEA3

Parameter	Size(bits)	Remark
COUNT	32	The counter
BEARER	5	The bearer identity
DIRECTION	1	The direction of transmission
CK	128	The Confidentiality key
LENGTH	32	The length of the input message
IBS	LENGTH	The input bit stream

Table A.2 The output of 128-EEA3

Parameter	Size(bits)	Remark
OBS	LENGTH	The output bit stream

A.2 Parameter Initialization

The initialization process constructs the initialization vector (IV) based on the counter (COUNT), bearer identifier (BEARER), and transmission direction identifier (DIRECTION) as shown in Table A.1.

The counter is defined as

COUNT=COUNT[0] || COUNT[1] || COUNT[2] || COUNT[3]

The initialization vector (IV) is defined as

IV=IV[0] || IV[1] || IV[2] || … || IV[15]

where COUNT[0],COUNT[1],COUNT[2],COUNT[3] and IV[0],IV[1],…,IV[15] are all 8-bit bytes.

The calculation is as follows:

IV[0] = COUNT[0], IV[1] = COUNT[1],
IV[2] = COUNT[2], IV[3] = COUNT[3],
IV[4] = BEARER || DIRECTION || 00_2,

IV[5] = IV[6] = IV[7] = 00000000_2,
IV[8] = IV[0], IV[9] = IV[1],
IV[10] = IV[2], IV[11] = IV[3],
IV[12] = IV[4],IV[13] = IV[5],
IV[14] = IV[6],IV[15] = IV[7].

Refer to Appendix B for 3GPP LTE algorithm calculation examples.

Appendix B

(Informative Appendix)
Algorithm Calculation Examples in 3GPP LTE

Below are calculation examples of this algorithm in 3GPP LTE. The data is represented in hexadecimal.

Example 1:

The First Set of Encryption Examples

CK = 17 3d 14 ba 50 03 73 1d 7a 60 04 94 70 f0 0a 29

COUNT = 66035492

BEARER = f

DIRECTION = 0

LENGTH = c1

IBS:

6cf65340 735552ab 0c9752fa 6f9025fe 0bd675d9 005875b2 00000000

OBS:

a6c85fc6 6afb8533 aafc2518 dfe78494 0ee1e4b0 30238cc8 00000000

Example 2:

The Second Set of Encryption Examples

CK = e5 bd 3e a0 eb 55 ad e8 66 c6 ac 58 bd 54 30 2a

COUNT = 56823

BEARER = 18

DIRECTION = 1

LENGTH = 320

IBS:

14a8ef69 3d678507 bbe7270a 7f67ff50 06c3525b 9807e467 c4e56000 ba338f5d 42955903 67518222 46c80d3b 38f07f4b e2d8ff58 05f51322 29bde93b bbdcaf38 2bf1ee97 2fbf9977 bada8945 847a2a6c 9ad34a66 7554e04d 1f7fa2c3 3241bd8f 01ba220d

OBS:

131d43e0 dea1be5c 5a1bfd97 1d852cbf 712d7b4f 57961fea 3208afa8 bca433f4 56ad09c7 417e58bc 69cf8866 d1353f74 865e8078 1d202dfb 3ecff7fc bc3b190f e82a204e d0e350fc 0f6f2613 b2f2bca6 df5a473a 57a4a00d 985ebad8 80d6f238 64a07b01

Example 3:

The Third Set of Encryption Examples

CK = e1 3f ed 21 b4 6e 4e 7e c3 12 53 b2 bb 17 b3 e0

COUNT = 2738cdaa

BEARER = 1a

DIRECTION = 0

LENGTH = FB3

IBS:

8d74e20d 54894e06 d3cb13cb 3933065e 8674be62 adb1c72b 3a646965 ab63cb7b 7854dfdc 27e84929 f49c64b8 72a490b1 3f957b64 827e71f4 1fbd4269 a42c97f8 24537027 f86e9f4a d82d1df4 51690fdd 98b6d03f 3a0ebe3a 312d6b84 0ba5a182 0b2a2c97 09c090d2 45ed267c f845ae41 fa975d33 33ac3009 fd40eba9 eb5b8857 14b768b6 97138baf 21380eca 49f644d4 8689e421 5760b906 739f0d2b 3f091133 ca15d981 cbe401ba f72d05ac e05cccb2 d297f4ef 6a5f58d9 1246cfa7 7215b892 ab441d52 78452795 ccb7f5d7 9057a1c4 f77f80d4 6db2033c b79bedf8 e60551ce 10c667f6 2a97abaf abbcd677 2018df96 a282ea73 7ce2cb33 1211f60d 5354ce78 f9918d9c 206ca042 c9b62387 dd709604 a50af16d 8d35a890 6be484cf 2e74a928 99403643 53249b27 b4c9ae29 eddfc7da 6418791a 4e7baa06 60fa6451 1f2d685c c3a5ff70 e0d2b742 92e3b8a0 cd6b04b1 c790b8ea d2703708 540dea2f c09c3da7 70f65449 e84d817a 4f551055 e19ab850 18a0028b 71a144d9 6791e9a3 57793350 4eee0060 340c69d2 74e1bf9d 805dcbcc 1a6faa97 6800b6ff 2b671dc4 63652fa8 a33ee509 74c1c21b e01eabb2 16743026 9d72ee51 1c9dde30 797c9a25 d86ce74f 5b961be5 fdfb6807 814039e7 137636bd 1d7fa9e0 9efd2007 505906a5 ac45dfde ed7757bb ee745749 c2963335 0bee0ea6 f409df45 80160000

OBS：

94eaa4aa 30a57137 ddf09b97 b25618a2 0a13e2f1 0fa5bf81 61a879cc 2ae797a6 b4cf2d9d f31debb9 905ccfec 97de605d 21c61ab8 531b7f3c 9da5f039 31f8a064 2de48211 f5f52ffe a10f392a 04766998 5da454a2 8f080961 a6c2b62d aa17f33c d60a4971 f48d2d90 9394a55f 48117ace 43d708e6 b77d3dc4 6d8bc017 d4d1abb7 7b7428c0 42b06f2f 99d8d07c 9879d996 00127a31 985f1099 bbd7d6c1 519ede8f 5eeb4a61 0b349ac0 1ea23506 91756bd1 05c974a5 3eddb35d 1d4100b0 12e522ab 41f4c5f2 fde76b59 cb8b96d8 85cfe408 0d1328a0 d636cc0e dc05800b 76acca8f ef672084 d1f52a8b bd8e0993 320992c7 ffbae17c 408441e0 ee883fc8 a8b05e22 f5ff7f8d 1b48c74c 468c467a 028f09fd 7ce91109 a570a2d5 c4d5f4fa 18c5dd3e 4562afe2 4ef77190 1f59af64 5898acef 088abae0 7e92d52e b2de5504 5bb1b7c4 164ef2d7 a6cac15e eb926d7e a2f08b66 e1f759f3 aee44614 725aa3c7 482b3084 4c143ff8 5b53f1e5 83c50125 7dddd096 b81268da a303f172 34c23335 41f0bb8e 190648c5 807c866d 71932286 09adb948 686f7de2 94a802cc 38f7fe52 08f5ea31 96d0167b 9bdd02f0 d2a5221c a508f893 af5c4b4b b9f4f520 fd84289b 3dbe7e61 497a7e2a 584037ea 637b6981 127174af 57b471df 4b2768fd 79c1540f b3edf2ea 22cb69be c0cf8d93 3d9c6fdd 645e8505 91cca3d6 2c0cc000

References

[1] ETSI/SAGE TS 35.221. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 Specification.

[2] ETSI/SAGE TS 35.222. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification.

[3] ETSI/SAGE TS 35.223. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 3: Implementor's Test Data.

[4] ETSI/SAGE TR 35.924. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4: Design and Evaluation Report.