



中华人民共和国国家标准

GB/T 33133.3—2021

信息安全技术 祖冲之序列密码算法 第3部分：完整性算法

Information security technology—
ZUC stream cipher algorithm—Part 3: Integrity algorithm

2021-10-11 发布

2022-05-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 I

引言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 符号和缩略语 1

 4.1 符号 1

 4.2 缩略语 1

5 算法描述 1

 5.1 算法输入与输出 1

 5.2 算法工作流程 2

附录 A (资料性附录) 3GPP LTE 中参数初始化 3

附录 B (资料性附录) 3GPP LTE 中算法计算实例 5

参考文献..... 7



前 言

GB/T 33133《信息安全技术 祖冲之序列密码算法》分为 3 个部分：

- 第 1 部分：算法描述；
- 第 2 部分：保密性算法；
- 第 3 部分：完整性算法。

本部分为 GB/T 33133 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：北京信息科学技术研究院、中国科学院软件研究所、中国科学院数据与通信保护研究教育中心、北京创原天地科技有限公司、国家密码管理局商用密码检测中心。

本部分主要起草人：冯登国、林东岱、冯秀涛、周春芳、刘辛越、肖青海、吕春梅。

引 言

本文件的发布机构提请注意,声明符合本文件时,可能涉及到 5.2 与《一种序列密码实现方法和装置》(专利号:ZL200910086409.9)和《一种完整性认证方法》(专利号:ZL200910243440.9)相关专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利的持有人已向本文件的发布机构保证,他愿意同任何申请人在合理且无歧视的条款和条件下,就专利授权许可进行谈判。该专利的持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得:

专利持有人:中国科学院数据与通信保护研究教育中心、中国科学院软件研究所

地址:北京市海淀区闵庄路甲 89 号 邮编:100093、北京市中关村南四街 4 号 邮编:100190

请注意除上述专利外,本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。



信息安全技术 祖冲之序列密码算法

第3部分:完整性算法

1 范围

GB/T 33133 的本部分描述了基于祖冲之序列密码算法的完整性算法。

本部分适用于基于祖冲之序列密码算法的完整性算法的相关产品的研制、检测和使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 33133.1—2016 信息安全技术 祖冲之序列密码算法 第1部分:算法描述

3 术语和定义

GB/T 33133.1—2016 界定的术语和定义适用于本文件。

4 符号和缩略语

4.1 符号

下列符号适用于本文件。

\oplus 按比特位逐位异或运算

\parallel 字符串或字节串连接符

$\lceil x \rceil$ 不小于 x 的最小整数

$\ll k$ 左移 k 位

4.2 缩略语

下列缩略语适用于本文件。

IK:完整性算法密钥(Integral Key)

IV:初始向量(Initial Vector)

LTE:长期演进(Long Term Evolution)

MAC:消息认证码(Message Authentication Code)

3GPP:第三代合作伙伴计划(the 3rd Generation Partnership Project)

5 算法描述

5.1 算法输入与输出

本算法的输入参数见表1,输出参数见表2。

表 1 输入参数

输入参数	比特长度	备注
IK	128	完整性密钥
IV	128	初始向量
LENGTH	32	输入消息流的比特长度
M	LENGTH	输入消息流,其长度为 LENGTH

表 2 输出参数

输出参数	比特长度	备注
MAC	32	消息认证码

5.2 算法工作流程

5.2.1 产生密钥流

设 $L = \lceil \text{LENGTH}/32 \rceil + 2$ 。利用完整性密钥 IK 和初始向量 IV,将 IK、IV、 L 作为输入参数,按 GB/T 33133.1—2016 中 5.6 给出的方法产生 L 个字的密钥流。将生成的密钥流用比特串表示为: $k[0], k[1], \dots, k[32 \times L - 1]$,其中 $k[0]$ 为第一个密钥字的最高位比特, $k[31]$ 为最低位比特,其他依此类推。

对于 $i = 0, 1, 2, \dots, 32 \times (L - 1)$, 令

$$k_i = k[i] \parallel k[i+1] \parallel \dots \parallel k[i+31]$$

其中, k_i 为 32 比特字。

在 3GPP LTE 应用场景中,初始向量 IV 的初始化方法参见附录 A。

5.2.2 计算 MAC

设 T 为 32 比特字变量。置 $T = 0$ 。

对 $i = 0, 1, \dots, \text{LENGTH}-1$, 如果 $M[i] = 1$, 则

$$T = T \oplus k_i$$

计算

$$T = T \oplus k_{\text{LENGTH}}$$

计算 MAC

$$\text{MAC} = T \oplus k_{32 \times (L - 1)}$$

在 3GPP LTE 应用场景中,算法计算实例参见附录 B。

附录 A
(资料性附录)
3GPP LTE 中参数初始化


A.1 输入与输出参数

在 3GPP LTE 中输入参数与输出参数赋值规定参见表 A.1、表 A.2。

表 A.1 输入参数

输入参数	比特长度	备注
COUNT	32	计数器
BEARER	5	承载层标识
DIRECTION	1	传输方向标识
IK	128	完整性密钥
LENGTH	32	输入消息流的比特长度
M	LENGTH	输入消息流,其长度为 LENGTH

表 A.2 输出参数

 输出参数	比特长度	备注
MAC	32	消息认证码

A.2 参数初始化

初始化流程根据计数器 COUNT、承载层标识 BEARER、传输方向标识 DIRECTION(见表 A.1)构造初始向量 IV。

设计数为：

$$\text{COUNT} = \text{COUNT}[0] \parallel \text{COUNT}[1] \parallel \text{COUNT}[2] \parallel \text{COUNT}[3]$$

其中,COUNT[i]为 8 比特的字节,i=0,1,2,3。设初始向量 IV 为：

$$\text{IV} = \text{IV}[0] \parallel \text{IV}[1] \parallel \text{IV}[2] \parallel \cdots \parallel \text{IV}[15]$$

其中,IV[i](0≤i≤15)为 8 比特的字节。

计算：

$$\begin{aligned} \text{IV}[0] &= \text{COUNT}[0], \text{IV}[1] = \text{COUNT}[1], \\ \text{IV}[2] &= \text{COUNT}[2], \text{IV}[3] = \text{COUNT}[3], \\ \text{IV}[4] &= \text{BEARER} \parallel 000_2, \text{IV}[5] = 00000000_2, \\ \text{IV}[6] &= 00000000_2, \text{IV}[7] = 00000000_2, \\ \text{IV}[8] &= \text{IV}[0] \oplus (\text{DIRECTION} \ll 7), \text{IV}[9] = \text{IV}[1], \end{aligned}$$

$$IV[10]=IV[2], IV[11]=IV[3],$$

$$IV[12]=IV[4], IV[13]=IV[5],$$

$$IV[14]=IV[6]\oplus(DIRECTION \ll 7), IV[15]=IV[7].$$

3GPP LTE 算法计算实例参见附录 B。



附 录 B
(资料性附录)
3GPP LTE 中算法计算实例

以下为本算法在 3GPP LTE 中的计算实例。数据采用 16 进制表示。

示例 1:

第一组计算实例:	
IK	=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
COUNT	=0
BEARER	=0
DIRECTION	=0
LENGTH	=1
M	00000000
MAC	c8a9595e

示例 2:

第二组计算实例:	
IK	=c9 e6 ce c4 60 7c 72 db 00 0a ef a8 83 85 ab 0a
COUNT	=a94059da
BEARER	=a
DIRECTION	=1
LENGTH	=241
M	983b41d4 7d780c9e 1ad11d7e b70391b1 de0b35da 2dc62f83 e7b78d63 06ca0ea0 7e941b7b e91348f9 fcb170e2 217fecd9 7f9f68ad b16e5d7d 21e569d2 80ed775c ebde3f40 93c53881 00000000
MAC	fae8ff0b

示例 3:

第三组计算实例:	
IK	=6b 8b 08 ee 79 e0 b5 98 2d 6d 12 8e a9 f2 20 cb
COUNT	=561eb2dd
BEARER	=1c
DIRECTION	=0
LENGTH	=1626
M	5bad7247 10ba1c56 d5a315f8 d40f6e09 3780be8e 8de07b69 92432018 e08ed96a 5734af8b ad8a575d 3a1f162f 85045cc7 70925571 d9f5b94e 454a77c1 6e72936b f016ae15 7499f054 3b5d52ca a6dbeab6 97d2bb73 e41b8075 dce79b4b 86044f66 1d4485a5 43dd7860 6e0419e8 059859d3 cb2b67ce 0977603f 81ff839e 33185954 4cfbc8d0 0fef1a4c 8510fb54 7d6b06c6 11ef44f1 bce107cf a45a06aa b360152b 28dc1ebe 6f7fe09b 0516f9a5 b02a1bd8 4bb0181e 2e89e19b d8125930 d178682f 3862dc51 b636f04e 720c47c3 ce51ad70 d94b9b22 55fbae90 6549f499 f8c6d399 47ed5e5d f8e2def1 13253e7b 08d0a76b 6bfc68c8 12f375c7 9b8fe5fd 85976aa6 d46b4a23 39d8ae51 47f680fb e70f978b 38effd7b 2f7866a2 2554e193 a94e98a6 8b74bd25 bb2b3f5f b0a5fd59 887f9ab6 8159b717 8d5b7b67 7cb546bf 41eadca2 16fc1085 0128f8bd ef5c8d89 f96afa4f a8b54885 565ed838 a950fee5 f1c3b0a4 f6fb71e5 4dfd169e

82cecc72 66c850e6 7c5ef0ba 960f5214 060e71eb 172a75fc 1486835c bea65344 65b055c9
6a72e410 52241823 25d83041 4b40214d aa8091d2 e0fb010a e15c6de9 0850973b df1e423b
e148a237 b87a0c9f 34d4b476 05b803d7 43a86a90 399a4af3 96d3a120 0a62f3d9 507962e8
e5bee6d3 da2bb3f7 237664ac 7a292823 900bc635 03b29e80 d63f6067 bf8e1716 ac25beba
350deb62 a99fe031 85eb4f69 937ecd38 7941fda5 44ba67db 09117749 38b01827 bcc69c92
b3f772a9 d2859ef0 03398b1f 6bbad7b5 74f7989a 1d10b2df 798e0dbf 30d65874 64d24878
cd00c0ea ee8a1a0c c753a279 79e11b41 db1de3d5 038afaf4 9f5c682c 3748d8a3 a9ec54e6
a371275f 1683510f 8e4f9093 8f9ab6e1 34c2cdf 4841cba8 8e0cff2b 0bcc8e6a dcb71109
b5198fec f1bb7e5c 531aca50 a56a8a3b 6de59862 d41fa113 d9cd9578 08f08571 d9a4bb79
2af271f6 cc6dbb8d c7ec36e3 6be1ed30 8164c31c 7c0afc54 1c000000

MAC:0ca12792

参 考 文 献

- [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

