ICS 35.030
L 80

中华人民共和国国家标准

GB/T 33133.2—2021

信息安全技术　祖冲之序列密码算法　第2部分：保密性算法

Information security technology—ZUC stream cipher algorithm—Part 2：Confidentiality algorithm

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

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2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2部分:保密性算法

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保密性算法。

本部分适用于基于祖冲之序列密码算法的保密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

$\lceil x \rceil$　不小于x的最小整数

$\|$　　字节串连接符

4.2　缩略语

下列缩略语适用于本文件。

CK:保密性算法密钥(Confidential Key)

IV:初始向量(Initialization Vector)

IBS:输入比特流 (Input Bit Stream)

LTE:长期演进(Long Term Evolution)

OBS:输出比特流(Output Bit Stream)

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
CK	128	保密性密钥
IV	128	初始向量
LENGTH	32	明文消息流的比特长度
IBS	LENGTH	输入比特流，其长度为 LENGTH

表 2　输出参数

输出参数	比特长度	备注
OBS	LENGTH	输出比特流，其长度为 LENGTH

5.2　算法工作流程

5.2.1　产生密钥流

设 $L=\lceil \text{LENGTH}/32 \rceil$。将保密性密钥 CK、初始向量 IV 和 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 $K[0],K[1],\cdots,K[32\times L-1]$，其中 $K[0]$为第一个密钥字的最高位比特，$K[31]$为第一个密钥字的最低位比特，其他依此类推。

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　加解密

设长度为 LENGTH 的输入比特流为：

$$\text{IBS}=\text{IBS}[0]\parallel\text{IBS}[1]\parallel\text{IBS}[2]\parallel\cdots\parallel\text{IBS}[\text{LENGTH-1}]$$

对应的输出比特流为：

$$\text{OBS}=\text{OBS}[0]\parallel\text{OBS}[1]\parallel\text{OBS}[2]\parallel\cdots\parallel\text{OBS}[\text{LENGTH-1}]$$

其中，IBS[i]和 OBS[i]均为比特，$i=0,1,2,\cdots\cdots,\text{LENGTH-1}$。计算输出比特流：

$$\text{OBS}[i]=\text{IBS}[i]\oplus\text{k}[i],i=0,1,2,\cdots,\text{LENGTH-1}$$

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如表 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
CK	128	保密性密钥
LENGTH	32	明文消息流的比特长度
IBS	LENGTH	输入比特流，其长度为 LENGTH

表 A.2 输出参数

输出参数	比特长度	备注
OBS	LENGTH	输出比特流，其长度为 LENGTH

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。

设计数器为：

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

设初始向量为：

$$IV = IV[0] \| IV[1] \| IV[2] \| \cdots \| IV[15]$$

其中，COUNT[0]、COUNT[1]、COUNT[2]、COUNT[3]和 IV[0]、IV[1]、…、IV[15]都是 8 比特的字节。

计算：

$IV[0] = COUNT[0]$，$IV[1] = COUNT[1]$，

$IV[2] = COUNT[2]$，$IV[3] = COUNT[3]$，

$IV[4] = BEARER \| DIRECTION \| 00_2$，

$IV[5] = IV[6] = IV[7] = 00000000_2$，

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]。

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：

第一组加密实例

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

示例 2：

第二组加密实例

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

示例 3：

第三组加密实例

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

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