ICS 35.040
L 80
备案号:36824—2012

GM

# 中华人民共和国密码行业标准

GM/T 0001.3—2012

# 祖冲之序列密码算法
# 第3部分:基于祖冲之算法的完整性算法

**ZUC stream cipher algorithm—**
**Part 3:The ZUC-based integrity algorithm**

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　发布

# 目　次

# 前　言

GM/T 0001《祖冲之序列密码算法》包括三部分：

——第1部分：算法描述；

——第2部分：基于祖冲之算法的机密性算法；

——第3部分：基于祖冲之算法的完整性算法。

本部分为GM/T 0001的第3部分。

GM/T 0001的本部分依据GB/T 1.1—2009给出的规则起草。

本部分内容同3GPP LTE机密性和完整性算法标准128-EIA3规范(ETSI/SAGE TS 35.221)保持一致性。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分附录A为资料性附录。

本部分由国家密码管理局提出并归口。

本部分起草单位：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。

本部分主要起草人：冯登国、林东岱、冯秀涛、周春芳。

# 祖冲之序列密码算法
# 第3部分:基于祖冲之算法的完整性算法

## 1 范围

GM/T 0001的本部分描述了基于祖冲之算法的完整性算法。该完整性算法可适用于3GPP LTE通信中消息的完整性保护。本部分可用于指导基于祖冲之算法的完整性算法相关产品的研制、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。

GM/T 0001.1—2012 祖冲之序列密码算法 第1部分:算法描述

## 3 术语和约定

以下术语和约定适用于本文件。

3.1

**比特 bit**

二进制字符0和1称之为比特。

3.2

**字节 byte**

由8个比特组成的比特串称之为字节。

3.3

**字 word**

由2个以上(包含2个)比特组成的比特串称之为字。

本部分主要使用31比特字和32比特字。

3.4

**字表示 word representation**

本部分字默认采用十进制表示。当字采用其他进制表示时,总是在字的表示之前或之后添加指示符。例如,前缀0x指示该字采用十六进制表示,后缀下角标2指示该字采用二进制表示。

3.5

**高低位顺序 bit ordering**

本部分规定字的最高位总是位于字表示中的最左边,最低位总是位于字表示中的最右边。

## 4 符号和缩略语

### 4.1 符号

下列符号适用于本部分:

| | |
|---|---|
| $\oplus$ | 异或运算 |
| $a \| b$ | 字符串连接符 |
| $\lceil x \rceil$ | 不小于 $x$ 的最小整数 |
| $<<k$ | 左移 $k$ 位 |

## 4.2 缩略语

下列缩略语适用于本部分：

| | |
|---|---|
| IK | 基于祖冲之算法的完整性算法密钥 |
| KEY | 祖冲之算法的初始密钥 |
| IV | 祖冲之算法的初始向量 |
| MAC | 消息认证码 |

# 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 输入参数表

| 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 |

表 2 输出参数表

| 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 初始化

本算法的初始化主要是指根据完整性密钥 **IK** 和其他输入参数(见 5.1 的表 1)构造祖冲之算法的初始密钥 **KEY** 和初始向量 **IV**。

记完整性密钥

$$\mathbf{IK}=\mathbf{IK}[0] \| \mathbf{IK}[1] \| \mathbf{IK}[2] \| \cdots \| \mathbf{IK}[15]$$

和祖冲之算法的初始化密钥

$$\mathbf{KEY}=\mathbf{KEY}[0] \| \mathbf{KEY}[1] \| \mathbf{KEY}[2] \| \cdots \| \mathbf{KEY}[15],$$

其中 $\mathbf{IK}[i]$、$\mathbf{KEY}[i]$($0 \leqslant i \leqslant 15$)都是 8 比特的字节。则有：

$$\mathbf{KEY}[i]=\mathbf{IK}[i],i=0,1,2,\cdots,15。$$

记计数器

$$\mathbf{COUNT}=\mathbf{COUNT}[0]\|\mathbf{COUNT}[1]\|\mathbf{COUNT}[2]\|\mathbf{COUNT}[3],$$

其中 $\mathbf{COUNT}[i]$为 8 比特的字节，$i=0,1,2,3$。设祖冲之算法的初始向量 **IV** 为：

$$\mathbf{IV}=\mathbf{IV}[0]\|\mathbf{IV}[1]\|\mathbf{IV}[2]\|\cdots\|\mathbf{IV}[15],$$

其中 $\mathbf{IV}[i](0\leqslant i\leqslant 15)$为 8 比特的字节。则有：

$\mathbf{IV}[0]=\mathbf{COUNT}[0]$，$\mathbf{IV}[1]=\mathbf{COUNT}[1]$，

$\mathbf{IV}[2]=\mathbf{COUNT}[2]$，$\mathbf{IV}[3]=\mathbf{COUNT}[3]$，

$\mathbf{IV}[4]=\mathbf{BEARER}\|000_2$，$\mathbf{IV}[5]=00000000_2$，

$\mathbf{IV}[6]=00000000_2$，$\mathbf{IV}[7]=00000000_2$，

$\mathbf{IV}[8]=\mathbf{IV}[0]\oplus(\mathbf{DIRECTION}<<7)$，$\mathbf{IV}[9]=\mathbf{IV}[1]$，

$\mathbf{IV}[10]=\mathbf{IV}[2]$，$\mathbf{IV}[11]=\mathbf{IV}[3]$，

$\mathbf{IV}[12]=\mathbf{IV}[4]$，$\mathbf{IV}[13]=\mathbf{IV}[5]$，

$\mathbf{IV}[14]=\mathbf{IV}[6]\oplus(\mathbf{DIRECTION}<<7)$，$\mathbf{IV}[15]=\mathbf{IV}[7]$。

### 5.2.2 产生密钥流

利用 5.2.1 生成的初始密钥 **KEY** 和初始向量 **IV**，祖冲之算法产生 $L$ 个字的密钥流。将生成的密钥流用比特串表示为 $\mathbf{k}[0],\mathbf{k}[1],\cdots,\mathbf{k}[32*L-1]$，其中 $\mathbf{k}[0]$为祖冲之算法生成的第一个密钥字的最高位比特，$\mathbf{k}[31]$为最低位比特，其他依此类推。为了计算 **LENGTH** 比特消息的 **MAC** 值，$L$ 的取值为 $L=\lceil \mathbf{LENGTH}/32 \rceil+2$。

对于 $i=0,1,2,\cdots\cdots,32*(L-1)$，令

$$\mathbf{k}_i=\mathbf{k}[i]\|\mathbf{k}[i+1]\|\cdots\|\mathbf{k}[i+31],$$

则 $\mathbf{k}_i$ 为 32 比特字。

### 5.2.3 计算 MAC

设 **T** 为 32 比特字变量，置 $\mathbf{T}=0$。

对 $i=0,1,\cdots,\mathbf{LENGTH}-1$，如果 $\mathbf{M}[i]=1$，那么

$$\mathbf{T}=\mathbf{T}\oplus\mathbf{k}_i。$$

计算

$$\mathbf{T}=\mathbf{T}\oplus\mathbf{k}_{\mathbf{LENGTH}}。$$

最后计算

$$\mathbf{MAC}=\mathbf{T}\oplus\mathbf{k}_{32*(L-1)}。$$

# 附 录 A
## （资料性附录）
## 算法计算实例

以下为本算法的计算实例。数据采用16进制表示。

第一组实例：

**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

第二组实例：

**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

第三组实例：

**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 34c2cfdf 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.

中华人民共和国密码
行业标准
祖冲之序列密码算法
第3部分：基于祖冲之算法的完整性算法
GM/T 0001.3—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室：(010)64275323 发行中心：(010)51780235
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 14千字
2012年8月第一版 2012年8月第一次印刷
*
书号：155066·2-23746 定价 16.00 元



GM/T 0001.3-2012