ICS 35.040
L 80
备案号:36823—2012

GM

中华人民共和国密码行业标准

GM/T 0001.2—2012

祖冲之序列密码算法
第2部分:基于祖冲之算法的机密性算法

ZUC stream cipher algorithm—
Part 2:The ZUC-based confidentiality 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2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-EEA3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2部分:基于祖冲之算法的机密性算法

1 范围

GM/T 0001的本部分描述了基于祖冲之算法的机密性算法。该机密性算法可适用于3GPP LTE通信中的加密和解密。本部分可用于指导基于祖冲之算法的机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。

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:

⊕	按比特位逐位异或运算
$a \| b$	字符串连接符
$\lceil x \rceil$	不小于 x 的最小整数

4.2 缩略语

下列缩略语适用于本部分：

CK	基于祖冲之算法的机密性算法密钥
KEY	祖冲之算法的初始密钥
IV	祖冲之算法的初始向量
IBS	输入比特流
OBS	输出比特流

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
CK	128	机密性密钥
LENGTH	32	明文消息流的比特长度
IBS	**LENGTH**	输入比特流

表 2 输出参数表

输出参数	比特长度	备注
OBS	**LENGTH**	输出比特流

5.2 算法工作流程

5.2.1 初始化

本算法的初始化是指根据机密性密钥 **CK** 以及其他输入参数(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**。

记机密性密钥

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

和祖冲之算法的初始密钥

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

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

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

记计数器

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

和祖冲之算法的初始向量

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

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。则有：

$$\mathbf{IV}[0]-\mathbf{COUNT}[0],\mathbf{IV}[1]-\mathbf{COUNT}[1],$$
$$\mathbf{IV}[2]-\mathbf{COUNT}[2],\mathbf{IV}[3]-\mathbf{COUNT}[3],$$

$$\mathbf{IV}[4]-\mathbf{BEARER}\|\mathbf{DIRECTION}\|00_2,$$

$$\mathbf{IV}[5]-\mathbf{IV}[6]-\mathbf{IV}[7]-00000000_2,$$
$$\mathbf{IV}[8]-\mathbf{IV}[0],\mathbf{IV}[9]-\mathbf{IV}[1],$$
$$\mathbf{IV}[10]-\mathbf{IV}[2],\mathbf{IV}[11]-\mathbf{IV}[3],$$
$$\mathbf{IV}[12]-\mathbf{IV}[4],\mathbf{IV}[13]-\mathbf{IV}[5],$$
$$\mathbf{IV}[14]-\mathbf{IV}[6],\mathbf{IV}[15]-\mathbf{IV}[7]。$$

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 **k**[0],**k**[1],…,**k**[32 * L − 1]，其中 **k**[0]为祖冲之算法生成的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。为了处理 **LENGTH** 比特的输入比特流，L 的取值为 $L-\lceil \mathbf{LENGTH}/32\rceil$。

5.2.3 加解密

设长度为 **LENGTH** 的输入比特流为：

$$\mathbf{IBS}-\mathbf{IBS}[0]\|\mathbf{IBS}[1]\|\mathbf{IBS}[2]\|\cdots\|\mathbf{IBS}[\mathbf{LENGTH}-1],$$

对应的输出比特流为：

$$\mathbf{OBS}-\mathbf{OBS}[0]\|\mathbf{OBS}[1]\|\mathbf{OBS}[2]\|\cdots\|\mathbf{OBS}[\mathbf{LENGTH}-1],$$

其中 **IBS**[i]和 **OBS**[i]均为比特，$i-0,1,2,\cdots,$LENGTII-1。则有：

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

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

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

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
c3a5fff70 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 a6cacl5e 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.

中华人民共和国密码
行业标准
祖冲之序列密码算法
第2部分：基于祖冲之算法的机密性算法
GM/T 0001.2 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：155066·2-23745 定价 16.00 元

GM/T 0001.2-2012