



# 中华人民共和国国家标准

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

Information security technology—ZUC stream cipher algorithm—  
Part 1: Algorithm description

2016-10-13 发布

2017-05-01 实施

---

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

## 目 次

前言 .....	III
引言 .....	IV
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 .....	2
4.1 运算符 .....	2
4.2 符号 .....	2
4.3 缩略语 .....	2
5 算法流程 .....	2
5.1 算法结构 .....	2
5.2 线性反馈移位寄存器 LFSR .....	3
5.3 比特重组 BR .....	4
5.4 非线性函数 $F$ .....	4
5.5 密钥装入 .....	4
5.6 算法运行 .....	5
附录 A (规范性附录) S 盒 .....	6
附录 B (资料性附录) 模 $2^{31}-1$ 乘法和模 $2^{31}-1$ 加法的实现 .....	8
附录 C (资料性附录) 算法计算实例 .....	9
参考文献 .....	13

## 前 言

GB/T 33133《信息安全技术 祖冲之序列密码算法》分为以下 3 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 1 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由国家密码管理局提出。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)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。

本部分主要起草人：冯登国、林东岱、冯秀涛、周春芳、刘辛越。

## 引 言

本部分的目标是保证祖冲之序列密码算法使用的正确性,为国内企业正确研发使用祖冲之算法的相关设备提供指导。

本部分修改采用如下国际标准:

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.

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

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

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

本文件的发布机构请注意,声明符合本文件时,可能涉及《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,就该专利授权许可进行谈判。该专利的持有人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:

专利持有人姓名: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 1 部分:算法描述

### 1 范围

GB/T 33133 的本部分给出了祖冲之序列密码算法的一般结构,基于该结构可实现本标准其他各部分所规定的密码机制。

本部分适用于祖冲之序列密码算法相关产品的研制、检测和使用,可应用于涉及非国家秘密范畴的商业应用领域。

### 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 25069—2010 信息安全技术术语

### 3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

#### 3.1

##### 祖冲之序列密码算法 ZUC Stream Cipher

祖冲之序列密码算法是中国自主研发的流密码算法,是运用于下一代移动通信 4G 网络中的国际标准密码算法,该算法包括祖冲之算法、保密性算法和完整性算法三个部分。

#### 3.2

##### 位 bit

二进制数字 binary digit

二进制计数制中使用的数字 0 或 1。

#### 3.3

##### 字节 byte

一种由若干位组成的串,视作一个单位,通常代表一个字符或字符的一部分。

注 1: 对一个给定的数据处理系统,一个字节中的位数是固定的。

注 2: 一个字节通常是 8 位。

#### 3.4

##### 字 word

由 2 个以上(包含 2 个)比特组成的比特串。

本部分主要使用 31 比特字和 32 比特字。

#### 3.5

##### 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。