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。