ICS 35.040
L 80
备案号：36822—2012

GM

中华人民共和国密码行业标准

GM/T 0001.1—2012

祖冲之序列密码算法
第1部分：算法描述

ZUC stream cipher algorithm—
Part 1：Description of the 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1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ZUC规范(ETSI/SAGE TS 35.222)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为规范性附录，附录B和附录C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1部分:算法描述

1 范围

GM/T 0001的本部分描述了祖冲之序列密码算法,可用于指导祖冲之算法相关产品的研制、检测和使用。

2 术语和约定

以下术语和约定适用于本文件。

2.1

比特 bit

二进制字符0和1称之为比特。

2.2

字节 byte

由8个比特组成的比特串称之为字节。

2.3

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。

2.4

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。

2.5

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。

3 符号和缩略语

3.1 运算符

$+$	算术加法运算
mod	整数取余运算
$\oplus$	按比特位逐位异或运算
$\boxplus$	模2^{32}加法运算
$\|\|$	字符串连接符
$\cdot_H$	取字的最高16比特
$\cdot_L$	取字的最低16比特
$<<<k$	32比特字左循环移k位
$>>k$	32比特字右移k位