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。