ICS 35.040
L 80
备案号:36825—2012

GM

中华人民共和国密码行业标准

GM/T 0002—2012

SM4 分组密码算法

SM4 block cipher algorithm

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发 布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

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。

本标准的附录 A 为资料性附录。

本标准由国家密码管理局提出并归口。

本标准起草单位：中国科学院数据与通信保护研究教育中心、国家密码管理局商用密码检测中心。

本标准主要起草人：吕述望、李大为、张超、张众、董芳、毛颖颖、刘振华。

SM4 分组密码算法

1 范围

本标准规定了 SM4 分组密码算法的算法结构和算法描述，并给出了运算示例。

本标准适用于密码应用中使用分组密码的需求。

2 术语和定义

下列术语和定义适用于本文件。

2.1

分组长度 block length

一个信息分组的比特位数。

2.2

密钥长度 key length

密钥的比特位数。

2.3

密钥扩展算法 key expansion algorithm

将密钥变换为轮密钥的运算单元。

2.4

轮数 rounds

轮函数的迭代次数。

2.5

字 word

长度为 32 比特的组(串)。

2.6

S 盒 S-box

S 盒为固定的 8 比特输入 8 比特输出的置换，记为 Sbox(.)。

3 符号和缩略语

下列符号和缩略语适用于本文件：

$\oplus$　　32 位异或

$<<<i$　　32 位循环左移 i 位

4 算法结构

SM4 密码算法是一个分组算法。该算法的分组长度为 128 比特，密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。数据解密和数据加密的算法结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。