ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32907—2016

信息安全技术　SM4 分组密码算法

Information security technology—SM4 block cipher algorithm

2016-08-29 发布　　2017-03-01 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 …… Ⅰ
1　范围 …… 1
2　术语和定义 …… 1
3　符号和缩略语 …… 1
4　算法结构 …… 2
5　密钥及密钥参量 …… 2
6　轮函数　F …… 2
6.1　轮函数结构 …… 2
6.2　合成置换　T …… 2
7　算法描述 …… 3
7.1　加密算法 …… 3
7.2　解密算法 …… 3
7.3　密钥扩展算法 …… 3
附录A（资料性附录）　运算示例 …… 5
A.1　示例1 …… 5
A.2　示例2 …… 6

前　言

本标准按照 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。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)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、北京信息科学技术研究院。

本标准主要起草人:吕述望、李大为、邓开勇、张超、罗鹏、张众、董芳、毛颖颖、刘振华。

信息安全技术　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。

本标准适用于商用密码产品中分组密码算法的实现、检测和应用。

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

轮密钥　round key

又称子密钥，在迭代分组密码中每一轮使用的密钥，根据输入密钥用密钥编排算法推导得出。

2.6

字　word

长度为 32 比特的组(串)。

2.7

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
Z_2^n	比特长度为 n 的二进制序列集合