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 …… Ⅲ
1　范围 …… 1
2　术语和定义 …… 1
3　符号和缩略语 …… 1
4　算法结构 …… 1
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 …… 4
A.1　示例 1 …… 4
A.2　示例 2 …… 5

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。