

中华人民共和国国家标准

GB/T 35276-2017

信息安全技术 SM2 密码算法使用规范

Information security technology—SM2 cryptographic algorithm usage specification

2017-12-29 发布 2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局 皮 布 国 国 家 标 准 化 管 理 委 员 会

目 次

引言 范围 2 规范性引用文件 3 术语和定义 4 缩略语 5 SM2 的密钥对 5.1 SM2 私钥 5.2 SM2 公钥 6 数据转换 6.1 位申到 8 位字节串的转换 6.2 8 位字节串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式 7.3 签名数据格式	··· 1
2 规范性引用文件	
3 术语和定义 4 缩略语 5 SM2 的密钥对 5.1 SM2 私钥 5.2 SM2 公钥 6 数据转换 6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.1 密钥数据格式 7.2 加密数据格式	_
4 缩略语 5 SM2 的密钥对 5.1 SM2 私钥 5.2 SM2 公钥 6 数据转换 6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式	··· 1
5 SM2 的密钥对 5.1 SM2 私钥 5.2 SM2 公钥 6 数据转换 6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式	1
5.1 SM2 私钥 5.2 SM2 公钥 6 数据转换 6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式	··· 1
5.2 SM2 公钥 6 数据转换 6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式	··· 1
6 数据转换 6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式 7.2 加密数据格式	··· 1
6.1 位串到 8 位字节串的转换 6.2 8 位字节串到位串的转换 6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式	2
6.2 8 位字节串到位串的转换 6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式	2
6.3 整数到 8 位字节串的转换 6.4 8 位字节串到整数的转换 7 数据格式 7.1 密钥数据格式 7.2 加密数据格式 7.2 加密数据格式	2
6.4 8 位字节串到整数的转换	2
7 数据格式 ····································	
7.1 密钥数据格式 ····································	
7.2 加密数据格式	
73	
8 预处理	4
8.1 预处理 1	4
-1- 000-1-	
9 计算过程 ······· 9.1 生成密钥 ······ ···· ··· ··· ··· ··· ··· ··· ·	4
	4
9.2 加密 ···································	E
9.4 数字签名	
9.5 签名验证	5
9.6 密钥协商	E
10 用户身份标识 ID 的默认值 ····································	7

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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京海泰方圆科技股份有限公司、卫士通信息产业股份有限公司、无锡江南信息 安全工程技术中心、兴唐通信科技股份有限公司、山东得安信息技术有限公司、上海格尔软件股份有限 公司。

本标准主要起草人:刘平、蒋红宇、柳增寿、李元正、徐强、谭武征、孔凡玉、王妮娜。

引 言

SM2 椭圆曲线公钥密码算法(以下简称 SM2)是由 GB/T 32918 给出的一组非对称算法,其中包括 SM2-1 椭圆曲线数字签名算法、SM2-2 椭圆曲线密钥协商协议、SM2-3 椭圆曲线加密算法。

本标准的目标是保证 SM2 使用的正确性,为 SM2 密码算法的使用制定统一的数据格式和使用方法。

本标准中涉及的 SM3 算法是指 GB/T 32905 给出的一种密码杂凑算法。

本标准仅从算法应用的角度给出 SM2 密码算法的使用说明,不涉及 SM2 密码算法的具体编制细节。

信息安全技术 SM2 密码算法使用规范

1 范围

本标准规定了 SM2 密码算法的使用方法,以及密钥、加密与签名等的数据格式。 本标准适用于 SM2 密码算法的使用,以及支持 SM2 密码算法的设备和系统的研发和检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法

GB/T 32918.1-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第1部分:总则

GB/T 32918.2-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第2部分:数字签名算法

GB/T 32918.3-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第3部分:密钥交换协议

GB/T 32918.4-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法

GB/T 32918.5-2017 信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分:参数定义

3 术语和定义

下列术语和定义适用于本文件。

3.1

算法标识 algorithm identifier

用于标明算法机制的数字化信息。

3.2

SM2 密码算法 SM2 cryptographic algorithm

由 GB/T 32918(所有部分)定义的一种算法。

3.3

SM3 密码算法 SM3 cryptographic algorithm

由 GB/T 32905-2016 定义的一种算法。

4 缩略语

下列缩略语适用于本文件。

ECB:电码本模式(Electronics Code Book)

ECC: 椭圆曲线密码算法(Elliptic Curve Cryptography)

5 SM2 的密钥对

5.1 SM2 私钥

SM2 私钥是大于 1 且小于 n-1 的整数(n 为 SM2 算法的阶,其值见 GB/T 32918.5—2017 的第 2