ICS 35.040

L 80



中华人民共和国密码行业标准

GM/T 0009—2012

|  |
| --- |
|  |

SM2密码算法使用规范

SM2 cryptography algorithm application specification

2012-11-22 发布

2012-11-22 实施

国家密码管理局

目 次

[前言  1](#_Toc292199338)

[1. 范围 1](#_Toc961769657)

[2. 规范性引用文件 1](#_Toc223853431)

[3. 术语和定义 1](#_Toc608861178)

[4. 引言 1](#_Toc981092435)

[5. 符号和缩略语 1](#_Toc676956911)

[6. SM2的密钥对 1](#_Toc112014064)

[6.1. SM2私钥 1](#_Toc442843180)

[6.2. SM2公钥 1](#_Toc21153975)

[7. 数据转换 1](#_Toc54965107)

[7.1. 位串到8位字节串的转换 1](#_Toc911497688)

[7.2. 8位字节串到位串的转换 1](#_Toc314863574)

[7.3. 整数到8位字节串的转换 1](#_Toc907386750)

[7.4. 8位字节串到整数的转换 1](#_Toc942438272)

[8. 数据格式 1](#_Toc766675314)

[8.1. 密钥数据格式 1](#_Toc616091904)

[8.2. 加密数据格式 1](#_Toc167289727)

[8.3. 签名数据格式 1](#_Toc970022949)

[8.4. 密钥对保护数据格式 1](#_Toc996219019)

[9. 预处理 1](#_Toc642722186)

[9.1. 预处理1 1](#_Toc56627101)

[9.2. 预处理2 1](#_Toc437618971)

[10. 计算过程 1](#_Toc794429274)

[10.1. 生成密钥 1](#_Toc669614104)

[10.2. 加密 1](#_Toc713439808)

[10.3. 解密 1](#_Toc989957583)

[10.4. 数字签名 1](#_Toc77038895)

[10.5. 签名验证 1](#_Toc298614832)

[10.6. 密钥协商 1](#_Toc993393261)

[11. 用户身份标识 ID 的默认值 1](#_Toc459063808)

[参考文献 1](#_Toc792007804)

前言

本标准按照GB/T 1.1 2009的规则编写。

本标准由国家密码管理局提出并归口。

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。

本标准起草单位：北京海泰方圆科技有限公司、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。

SM2密码算法使用规范

# 1. 范围

本标准定义了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。

GM/T 0003,

GM/T 0004,

# 3. 术语和定义

下列术语和定义适用于本文件。

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 algorithm

一种椭圆曲线密码算法，密钥长度为256比特。

3.3

SM3算法 SM3 algorithm

一种杂凑算法，输出长度为256比特。

# 4. 引言

SM2椭圆曲线密码算法（以下简称SM2）是国家密码管理局批准的一组算法， 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算法是指国家密码管理局批准的SM3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。

# 5. 符号和缩略语

下列缩略语适用于本文件：

|  |  |
| --- | --- |
| EC | 电码本模式（Electronics Code Book） |
| ECC | 椭圆曲线密码算法（Elliptic Curve Cryptography） |
| ID | 用户身份标识（Identity） |

# 6. SM2的密钥对

## 6.1. SM2私钥

SM2私钥是一个大于等于 1 且小于 n-1 的整数（ n 为SM2算法的阶，其值参见 [GM/T 0003](#GMT0003)），简记为 k ，长度为256位。

## 6.2. SM2公钥

SM2公钥是SM2曲线上的一个点，由横坐标和纵坐标两个分量来表示，记为 （x，y）， 简记为 Q ，每个分量的长度为256位。

# 7. 数据转换

在SM2算法的使用中将涉及8位字节串(Octet String)和位串(Bit String)之间的转换， 主要包括以下四种形式。

## 7.1. 位串到8位字节串的转换

位串长度若不是8的整数倍，需先在它的左边补 0 ，以保证它的长度为8的倍数， 然后构造8位字节串，转换过程如下：

输入: 一个长度为的位串。

输出: 一个长度为的字节串M，其中的取值为 的整数部分。

动作：将位串 转换到8位字节串 采用如下方法：

从 ，设置：

(1)

对于 ，最左边位设置为0，右边设置为 。

输出M。

## 7.2. 8位字节串到位串的转换

8位字节串到位串转换过程如下：

输入: 一个长度为的8位字节串。

输出: 一个长度为的位串。

动作：将8位字节串 转换到位串 采用如下方法：

从，设置：

(2)

输出B。

## 7.3. 整数到8位字节串的转换

一个整数转换为8位字节串，基本方法是将其先使用二进制表达， 然后把结果位串再转换为8位字节串。以下是转换流程：

输入: 一个非负整数，期望的8位字节串长度。基本限制为：

输出: 一个长度为的8位字节串。

动作: 将基于的值 转换为一个8位字节串 采用如下方法：

从，设置：

(3)

输出。

## 7.4. 8位字节串到整数的转换

可以简单地把8位字节串看成以256为基表示的整数，转换过程如下：

输入：一个长度的8位字节串。

输出：一个整数x。

动作：将一个8位字节串转换为整数方法如下：

将看作]中的一个整数

(4)

输出。

# 8. 数据格式

## 8.1. 密钥数据格式

SM2算法私钥数据格式的ASN.1定义为：

SM2PrivateKey ::= INTEGER

SM2算法公钥数据格式的ASN.1定义为：

SM2PublicKey ::= BIT STRING

SM2PublicKey 为 BIT STRING 类型，内容为 04 | X | Y， 其中， X 和 Y 分别标识公钥的 x 分量和 y 分量， 其长度各为256位。

## 8.2. 加密数据格式

SM2算法加密后的数据格式的ASN.1定义为：

SM2Cipher ::= SEQENCE{  
  XCoordinate     INTEGER,                -- x 分量  
  YCoordinate     INTEGER,                -- y 分量  
  HASH            OCTET STRING SIZE(32),  -- 杂凑值  
  CipherText      OCTET STRING            -- 密文  
}

其中，`HASH`为使用SM3算法对明文数据运算得到的杂凑值，其长度固定为256位。 `CipherText`是与明文等长的密文。

## 8.3. 签名数据格式

SM2算法签名数据格式的ASN.1定义为：

SM2Signature ::= SEQUENCE{  
  R   INTEGER,  -- 签名值的第一部分  
  S   INTEGER   -- 签名值的第二部分  
}

R 和 S 的长度各为256位。

## 8.4. 密钥对保护数据格式

在SM2密钥对传递时，需要对SM2密钥对进行加密保护。具体的保护方法为：

1. 产生一个对称密钥；
2. 按对称密码算法标识指定的算法对SM2私钥进行加密，得到私钥的密文。 若对称算法为分组算法，则其运算模式为ECB；
3. 使用外部SM2公钥加密对称密钥得到对称密钥密文；
4. 将私钥密文、对称密钥密文封装到密钥对保护数据中。

SM2密钥对的保护数据格式的ASN.1定义为：

SM2EnvelopedKey ::=  SEQUENCE{  
  symAlgID                AlgorithmIdentifier,  -- 对称密码算法标识  
  symEncryptedKey         SM2Cipher,            -- 对称密钥密文  
  Sm2PublicKey            SM2PublicKey,         -- SM2公钥  
  Sm2EncryptedPrivateKey  BIT STRING            -- SM2私钥密文  
}

# 9. 预处理

## 9.1. 预处理1

预处理1是指使用签名方的用户身份标识和签名方公钥，通过运算得到 Z 值的过程。 Z 值用于预处理2，也用于SM2密钥协商协议。

输入:

1. ID ： 字节串。 用户身份标识。
2. Q ： SM2PublicKey 。用户的公钥。

输出:

1. Z: 字节串。 预处理1的输出。

计算公式为：

Z = SM3(ENTL|ID|a|b|xG|yG|xA|yA)

其中：

1. ENTL 为由2个字节表示的ID的比特长度；
2. ID 为用户身份标识；
3. a, b 为系统曲线参数；
4. xG, yG 为基点；
5. xA, yA 为用户的公钥。

详细的计算过程参见 [GM/T 0003](#GMT0003) 和 [GM/T 0004](#GMT0004)。

## 9.2. 预处理2

预处理2是指使用 Z 值和待签名消息，通过SM3运算得到杂凑值 H 的过程。 杂凑值 H 用于SM2数字签名。

输入:

1. Z: 字节串。预处理2的输入。
2. M: 字节串。待签名消息。

输出:

1. H: 字节串。杂凑值。

计算公式为：

H = SM3(Z|M)

详细的计算过程参见 [GM/T 0003](#GMT0003) 和[GM/T 0004](#GMT0004)。

# 10. 计算过程

## 10.1. 生成密钥

SM2密钥生成是指生成SM2算法的密钥对的过程，该密钥对包括私钥和与之对应的公钥。 其中，私钥的长度为256位，公钥的长度为512位。

输入:

1. 无

输出:

1. k: SM2PrivateKey 。 SM2私钥。
2. Q: SM2PublicKey 。 SM2公钥。

详细的计算过程参见[GM/T 0003](#GMT0003)。

## 10.2. 加密

SM2加密是指使用指定公开密钥对明文进行特定的加密计算，生成相应密文的过程。 该密文只能由该指定公开密钥对应的私钥解密。

输入:

1. Q: SM2PublicKey。 SM2公钥。
2. m: Byte 字节串。 待加密的明文数据。

输出:

1. c: SM2Cipher. 密文.

其中：

1. 输出参数 c 的格式由本规范7.2中定义；
2. 输出参数 c 的 XCoordinate 、 YCoordinate 为随机产生的公钥的x分量和y分量；
3. 输出参数 c 中的 HASH 的计算公式为： HASH = SM3( x | m | y ) 其中，x，y为Q的x分量和y分量；

输出参数 c 中 CipherText 为加密密文，其长度等于明文的长度。

详细的计算过程参见 [GM/T 0003](#GMT0003) 和 [GM/T 0004](#GMT0004)。

## 10.3. 解密

SM2解密是指使用指定私钥对密文进行解密计算，还原对应明文的过程。

输入:

1. d: SM2PrivateKey。 SM2私钥。
2. c: SM2Cipher。 密文。

输出:

1. m: 字节串。 与密文对应的明文。

m 为 SM2Cipher 经过解密运算得到的明文， 该明文的长度与输入参数 c 中 CipherText 的长度相同。

详细的计算过程参见[GM/T 0003](#GMT0003)。

## 10.4. 数字签名

SM2签名是指使用预处理2的结果和签名者私钥，通过签名计算得到签名结果的过程。

输入:

1. d: SM2PrivateKey。 签名者私钥。
2. H: 字节串。 预处理2的结果。

输出:

1. sign: SM2Signature。 签名值。

详细的计算过程参见 [GM/T 0003](#GMT0003)。

## 10.5. 签名验证

SM2签名验证是指使用预处理2的结果、签名值和签名者的公钥， 通过验签计算确定签名是否通过验证的过程。

输入:

1. H: 字节串. 预处理2的结果
2. sign: SM2Signature. 签名值
3. Q: PublicKey. 签名者的公钥.

输出:

1. 为 真 表示"`验证通过`"，为 假 表示"`验证不通过`"。

详细的计算过程参见 [GM/T 0003](#GMT0003)。

## 10.6. 密钥协商

密钥协商是在两个用户之间建立一个共享秘密密钥的协商过程， 通过这种方式能够确定一个共享秘密密钥的值。

设密钥协商双方为、，其密钥对分别为 和， 双方需要获得的密钥数据的比特长度为。 密钥协商协议分为两个阶段。

第一阶段：产生临时密钥对

用户：

1. 调用生成密钥算法产生临时密钥对，将和用户的用户身份标识发送给用户。

用户：

1. 调用生成密钥算法产生临时密钥对，将和 用户的用户身份标识发送给用户。

第二阶段：计算共享秘密密钥

用户 ：

1. 输入参数：

* + : SM2PublicKey。 用户 的公钥

* + : SM2PublicKey。 用户 的公钥

* + : SM2PublicKey。 用户 的临时公钥
  + : OCTET STRING。 用户 的用户身份标识

* + : SM2PublicKey。 用户 的临时公钥
  + : OCTET STRING。 用户 的用户身份标识

* + : SM2PrivateKey。 用户 的私钥

* + : SM2PrivateKey。 用户 的临时私钥
  + : INTEGER。 需要输出的密钥数据的比特长度

1. 输出参数：
   * : OCTET STRING. 位长为 的密钥数据
2. 步骤：
   1. 用 和 作为输入参数，调用预处理1得到 ;
   2. 用 和 作为输入参数，调用预处理1得到 ;
   3. 以 , , , , , , , 为输入参数，进行运算得到 .

用户 :

1. 输入参数：

* + : SM2PublicKey。 用户 的公钥

* + : SM2PublicKey。 用户 的公钥

* + : SM2PublicKey。 用户 的临时公钥
  + : OCTET STRING。 用户 的用户身份标识

* + : SM2PublicKey。 用户 的临时公钥
  + : OCTET STRING。 用户 的用户身份标识

* + : SM2PrivateKey。 用户 的私钥

* + : SM2PrivateKey。 用户 的临时私钥
  + : INTEGER。 需要输出的密钥数据的比特长度

1. 输出参数：
   * : OCTET STRING. 位长为 的密钥数据
2. 步骤：
   1. 用 和 作为输入参数，调用预处理1得到 ;
   2. 用 和 作为输入参数，调用预处理1得到 ;
   3. 以 , , , , , , , 为输入参数，进行运算得到 .

详细的计算过程参见 [GM/T 0003](#GMT0003) 和 [GM/T 0004](#GMT0004)。

# 11. 用户身份标识 ID 的默认值

无特殊约定的情况下，用户身份标识ID的长度为16字节，其默认值从左至右依次为：

0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38

# 参考文献