ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0080—2020

SM9 密码算法使用规范

SM9 cryptographic algorithm application specification

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：上海信息安全工程技术研究中心、北京国脉信安科技有限公司、深圳奥联信息安全技术有限公司、无锡华正天网信息安全系统有限公司。

本文件主要起草人：袁峰、王晓春、封维端、张立圆、王学进、药乐、蒋楠、程朝辉、蔡先勇、王一曲。

引　言

本文件是IBC(Identity-Based Cryptography)基于标识的密码技术系列标准之一，及依托于GB/T 38635.2《信息安全技术　SM9标识密码算法　第2部分：算法》。

本文件的目标是保证SM9密码算法使用的正确性，为SM9密码算法的使用制定统一的数据格式和使用方法。

本文件从算法应用的角度给出SM9密码算法的使用说明。

SM9 密码算法使用规范

1 范围

本文件定义了 SM9 密码算法的使用方法，以及密钥、加密与签名等的数据格式。

本文件适用于 SM9 密码算法的使用，以及支持 SM9 密码算法的设备和系统的研发和检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 38635.1—2020 信息安全技术 SM9 标识密码算法 第 1 部分：总则

GB/T 38635.2—2020 信息安全技术 SM9 标识密码算法 第 2 部分：算法

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

SM9 密码算法 SM9 algorithm

一种采用双线性对的椭圆曲线公钥密码算法。

3.3

签名主密钥 signature master key

密钥管理基础设施的根签名密钥对，包括签名主私钥和签名主公钥，用于进行数字签名、验签和为用户生成用户签名密钥。

3.4

加密主密钥 encryption master key

密钥管理基础设施的根加密密钥对，包括加密主私钥和加密主公钥，用于进行数字加密、解密和为用户生成用户加密密钥。

3.5

用户签名密钥 signature key

其中私钥由密钥管理基础设施产生并下发给用户。该类密钥包括用户签名私钥和签名公钥，用于数字签名和验签。

3.6

用户加密密钥　encryption key

其中私钥由密钥管理基础设施产生并下发给用户。该类密钥包括用户加密私钥和加密公钥，用于加密、解密和密钥协商。

3.7

公开参数服务　public parameter service

用于发布基于标识的密码技术中公开参数、私钥生成策略、用户标识信息和状态等数据的应用服务。

4　缩略语

下列缩略语适用于本文件。

ECB：电子密码本方式(Electronic Cipher Book)

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

IBC：基于标识的密码技术(Identity-Based Cryptography)

ID：用户身份标识(Identity)

KGC：密钥生成中心(Key Generating Center)

PPS：公开参数服务(Public Parameter Service)

5　SM9 的密钥对

5.1　生成元

G_1上的生成元 P_1点，记为(x_{p1}，y_{P1})，数据格式的 ASN.1 定义为 SM9P1::=BIT STRING，类型为 BIT STRING，其内容是：

04 ‖ X_1 ‖ Y_1，其中，X_1和 Y_1分别标识点的 x 分量和 y 分量，每个分量长度为 256 bit。

G_2上的生成元 P_2点，记为(x_{p2}，y_{P2})，数据格式的 ASN.1 定义为 SM9P2::=BIT STRING，类型为 BIT STRING，其内容是：

04 ‖ X_1 ‖ X_2 ‖ Y_1 ‖ Y_2，其中，X_1、X_2和 Y_1、Y_2分别标识公钥的各个 x 分量和 y 分量，每个分量长度为 256 bit，或

03 ‖ X_1 ‖ X_2，其中，X_1、X_2分别标识公钥的各个 x 分量，每个分量长度为 256 bit。选取解压后的 Y 根值 (Y_1 ‖ Y_2)中最右边 bit 位为 1 的那个值。还原后 Y 根值最右那个比特应用为 1，否则 Y_1＝基域 q－根 Y_1，Y_2＝基域 q－根 Y_2。或

02 ‖ X_1 ‖ X_2，其中，X_1、X_2分别标识公钥的 2 个 x 分量，每个分量长度为 256 bit。选取解压后的 Y 根值 (Y_1 ‖ Y_2)中最右边 bit 位为 0 的选项值。还原后 Y 根值取最右一比特为 0 的选项值，否则Y_1＝基域 q－根 Y_1，Y_2＝基域 q－根 Y_2。

5.2　SM9 主私钥

包括 SM9 签名主私钥和加密主私钥，都是一个大于或等于 1 且小于 N－1 的整数(N 是循环群 G_1、G_2和 G_T的阶，其值见 GB/T 38635.2—2020 的附录 A.1)，简记为 s，长度为 256 bit。

5.3　SM9 主公钥

包括 SM9 签名主公钥 $Ppub_2$和加密主公钥 $Ppub_1$。分别是 G_2和 G_1上的点，坐标表示为(x_{SPub}，y_{SPub})和(x_{EPub}，y_{EPub})。其中签名主公钥的 x，y 坐标还分别包含两个分量即 x_1分量和 x_2分量，y_1分量和

y_2分量，每个分量的长度为256 bit。而加密主公钥x，y坐标值长度都是256 bit。

5.4 SM9用户私钥

包括SM9用户签名私钥和用户加密私钥，分别是G_1和G_2上的点，坐标表示为(x_{SPri}，y_{SPri})和(x_{EPri}，y_{EPri})。其中用户签名钥x，y坐标值长度都是256 bit。而用户加密私钥的x，y坐标还分别包含两个分量即x_1分量和x_2分量，y_1分量和y_2分量，每个分量的长度为256 bit。

5.5 SM9用户公钥

在IBC技术中，用户标识ID可唯一确定用户的公钥，应用中以此代表公钥。基于双线性对ID坐标的表示可分为用户签名公钥坐标和用户加密公钥坐标，用户签名公钥坐标与签名主公钥坐标结构相同，x，y坐标上还有各自的两个分量，记为Q_S，用户加密公钥与加密主公钥坐标结构相同，记为Q_E。

注：这里给出用户公钥坐标的生成方法。

输入：算法函数H，$userID$，hid，主公钥$Ppub_i$，生成元P_i　$i=1,2$。

输出：用户公钥Q_A。

计算方法：

$Q_{AS}=[H_1(ID_A \| hid,N)]P_2+Ppub_2=(X_{QA2},Y_{QA2})$，签名公钥坐标用于签名/验签。

$Q_{AE}=[H_1(ID_A \| hid,N)]P_1+Ppub_1=(X_{QA1},Y_{QA1})$，加密公钥坐标用于密钥封装、加密/解密。

6 数据格式

6.1 密钥数据结构

密钥类型分为签名、加密主密钥和签名、加密用户密钥：

a) SM9算法签名主私钥数据格式的ASN.1定义为：

SM9SignMasterPrivateKey::=SM9MasterPrivateKey

SM9MasterPrivateKey ::=INTERGER

b) SM9算法签名主公钥数据格式的ASN.1定义为：

SM9SignMasterPublicKey::=BIT STRING

SM9SignMasterPublicKey为BIT STRING类型，内容为：

04‖X_1‖X_2‖Y_1‖Y_2，其中，X_1、X_2和Y_1、Y_2分别标识公钥的各个x分量和y分量，每个分量长度为256 bit。或

03‖X_1‖X_2，其中，X_1、X_2分别标识公钥的各个x分量，每个分量长度为256 bit。选取解压后的Y根值(Y_1‖Y_2)中最右边bit位为1的那个值。还原后Y根值取最右那个比特为0的值，否则Y_1=基域q－根Y_1，Y_2=基域q－根Y_2。或

02‖X_1‖X_2，其中，X_1、X_2分别标识公钥的2个x分量，每个分量长度为256 bit。选取解压后的Y根值(Y_1‖Y_2)中最右边bit位为0的选项值。还原后Y根值取最右一比特为0的选项值，否则Y_1=基域q－根Y_1，Y_2=基域q－根Y_2。

c) SM9算法加密主私钥数据格式的ASN.1定义为：

SM9EncryptMasterPrivateKey::=SM9MasterPrivateKey

d) SM9算法加密主公钥数据格式的ASN.1定义为：

SM9EncryptMasterPublicKey::=BIT STRING

SM9EncryptMasterPublicKey为BIT STRING类型，内容为：

04‖X‖Y，其中，X和Y标识公钥的各个x分量和y分量，每个分量长度为256 bit。

03‖X，其中，X标识公钥的x分量，每个分量长度为256 bit。选取解压后的Y根值中最右边bit

位为1的那个值。还原后Y根值取最右那个比特为0的值，否则Y＝基域q－根Y。或

02‖X，其中，X分别标识公钥的x分量，每个分量长度为256 bit。选取解压后的Y根值中最右边bit位为0的选项值。还原后Y根值取最右一比特为0的选项值，否则Y＝基域q－根Y。

e) SM9算法用户签名私钥数据格式的ASN.1定义为：

SM9SignPrivateKey::＝SM9EncryptMasterPublicKey

f) SM9算法用户加密私钥数据格式的ASN.1定义为：

SM9EncryptPrivateKey::＝ SM9SignMasterPublicKey

6.2 签名数据结构

SM9算法签名数据格式的ASN.1定义为：

```
SM9Signature ::= SEQUENCE{
H               OCTET STRING,          /杂凑分量，算法是H2（见GB/T 38635.2—2020）
S               SM9SignPrivateKey      /签名结果（见GB/T 38635.2—2020）
}
```

6.3 加密数据结构

SM9算法加密后的数据格式的ASN.1定义为：

```
SM9Cipher ::= SEQUENCE{
EnType          INTEGER,               /加密方式
C1              SM9SignPrivateKey,     /C1（见GB/T 38635.2—2020的9.2）
C3              OCTET STRING,          /明文数据杂凑值
CipherText      OCTET STRING           /密文
}
```

EnType为加密的方式，定义0代表M⊕K1序列密码加密，1、2、4、8分别代表ECB、CBC，OFB、CFB分组密码模式。分组密码加密的算法为GB/T 32907，

C1，该部分在GB/T 38635.2—2020的9.2中被称为C1。

C3为HASH，使用GB/T 32905算法对明文数据运算得到的杂凑值，其长度固定为256 bit。

CipherText，为加密密文。

6.4 密钥封装数据格式

用户A将一个随机数封装成C后，并传递给用户B，以便计算出密钥K。

密钥封装数据格式的ASN.1定义为：

```
SM9KeyPackage ::=SEQUENCE{
K               OCTET STRING,              /生成的密钥
C               SM9EncryptMasterPublicKey  /封装的交换密文
}
```

K作为用户A保留的密钥。C作为交换密文传递给B用户，B用户利用C可以生成K。

7 预处理

7.1 预处理杂凑函数 H_1

验签、加密时应按GB/T 38635.2—2020的5.3.2.2内容进行预处理计算。

输入：

DATA	比特串	/数据
Len	整型	/数据长度
N	整型	/是循环群 G_1、G_2 和 G_T 的阶
输出：		
h1	字节串	/杂凑值，长度为 256 bit，且 1≤h1<≤N−1

7.2 预处理杂凑函数 H_2

签名时应按 GB/T 38635.2—2020 的 5.3.2.3 内容进行预处理计算。

输入：		
DATA	比特串	/数据
Len	整型	/数据长度
N	整型	/是循环群 G_1、G_2 和 G_T 的阶
输出：		
h2	整数	

7.3 预处理对运算 e

应按 GB/T 38635.2—2020 的数字签名生成算法进行预处理计算。

对运算 e，通过用户标识公钥和 G_1、G_2 中的两个公开点 P_1 和 P_2 点计算出双曲线对 g_1 和 g_2。

签名 g_1 运算。

输入：		
P_1	SM9P1	/生成元 P_1
P_{Spub}	SM9SignMasterPublicKey	/签名主公钥
输出：		
g_1	比特串	/双线性对 G_T 中元素计算结果，N 的长度(256)×12=3 072 bit

加密 g_2 运算。

输入：		
P_2	SM9P2	/生成元 P_2
P_{Epub}	SM9EncryptMasterPublicKey	/加密主公钥
输出：		
g_2	比特串	/双线性对，长度为 3 072 bit

详细计算过程见 GB/T 38635.1—2020 的附录 C.6。

7.4 预处理用户验签 Q_D

将身份标识 ID 字符串变换为 G_2 域上的点的运算，从而得到基于双线性对 ID 的用户验证签名所需的坐标值 Q_D，用于验签计算过程中。

输入：		
ID	字节串	/用户身份标识串
hid	整数	/KGC 私钥生成函数公开标识，取值为 1
N	整数	/是循环群 G_1、G_2 和 G_T 的阶
P_2	SM9P2	/生成元 P_2
P_{spub}	SM9SignMasterPublicKey	/签名主公钥
输出：		
Q_D	SM9SignMasterPublicKey	

7.5 预处理用户加密 Q_E

将身份标识 ID 字符串变换为 G_2 域上的点的运算，从而得到基于双线性对 ID 的用户加解密所需的坐标值 Q_E，用于密钥封装、加密、密钥交互计算过程中。

输入：

ID	字节串	/用户身份标识串
hid	整数	/KGC 私钥生成函数公开标识，取值为 1
N	整数	/是循环群 G_1、G_2 和 G_T 的阶
P_1	SM9P1	/生成元 P_1
P_{epub}	SM9EncryptMasterPublicKey	/加密主公钥

输出：

Q_E	SM9EncryptMasterPublicKey	

8 计算过程

8.1 生成密钥

密钥生成包括主私/公钥、用户私钥类型。

a) 主私钥生成

SM9 签名主私钥和加密主私钥分别是由 KGC 按照 GB/T 32918(所有部分)的方法产生的随机数，其大于或等于 1 且小于 $N-1$ 的整数(N 为 SM9 算法的阶)，长度为 256 bit。

输入： 无

输出：

s SM9MasterPrivateKey /SM9 主私钥，如果为签名主私钥标识为 s_S，加密主私钥标识为 s_E

b) 主公钥生成

SM9 签名主公钥和加密主公钥分别由相对应的主私钥与 G_2 的生成元点 P_2 和 G_1 的生成元点 P_1 的积生成。

- 签名主公钥生成

输入：

s_S	SM9MasterPrivateKey	/签名主私钥
P_2	SM9P2	/P_2 生成元点

输出：

P_{spub}	SM9SignMasterPublicKey	/SM9 签名主公钥

- 加密主公钥生成

输入：

s_E	SM9MasterPrivateKey	/加密主私钥
P_1	SM9P1	/P_1 生成元点

输出：

P_{epub}	SM9EncryptMasterPublicKey	/SM9 加密主公钥

详细的计算过程见 GB/T 38635.2—2020 的第 6 章。

c) 用户私钥生成

SM9 用户私钥分用户签名私钥和用户加密私钥，用户分别由相对应的主私钥与 G_1 的生成元点 P_1

和 G_2 的生成元点 P_2 有关。

- 用户签名私钥生成

输入：

s_S	SM9MasterPrivateKey	/签名主私钥
ID	字节串	/用户身份标识串
hid	整数	/KGC 私钥生成函数公开标识，取值为 1
N	整数	/是循环群 G_1、G_2 和 G_T 的阶
P_1	SM9P1	/P_1 生成元点

输出：

d_S	SM9SignPrivateKey	/SM9 用户签名私钥

- 用户加密私钥生成

输入：

s_E	SM9MasterPrivateKey	/加密主私钥
ID	字节串	/用户身份标识串
hid	整数	/KGC 私钥生成函数公开标识，取值为 3
N	整数	/是循环群 G_1、G_2 和 G_T 的阶
P_2	SM9P2	/P_2 生成元点

输出：

d_E	SM9EncryptPrivateKey	/SM9 用户加密私钥

详细的计算过程见 GB/T 38635.2—2020 的第 9 章。

8.2 数字签名

SM9 签名是指使用预处理 e 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：

g_1	比特串	/对值
N	整数	/是循环群 G_1、G_2 和 G_T 的阶
M	比特串	/待签名数据
d_S	SM9SignPrivateKey	/签名者私钥

输出：

sign	SM9Signature	/签名值

详细的计算过程见 GB/T 38635.2—2020 的 6.2。

8.3 签名验证

SM9 签名验证是指使用预处理 e 的结果、签名值和被签数据，通过验签计算确定签名是否通过验证的过程。

输入：

ID	字节串	/签名者标识
hid	整数	/私钥生成函数公开标识
N	整数	/是循环群 G_1、G_2 和 G_T 的阶
g_1	比特串	/对值
Q_D	SM9SignMasterPublicKey	
M	比特串	/被签名数据
sign	SM9SignPrivateKey	/签名值

输出：

为“真”表示“验证通过”，为“假”表示“验证不通过”。

详细的计算过程见 GB/T 38635.2—2020 的 6.4。

8.4 密钥封装

SM9 密钥封装是指使用通过对运算生成密钥，并产生基于对方加密公钥坐标值的点的密文即加密封装的密文。

输入：

KeyLen	整型	/生成密钥的长度
ID	字节串	/对方身份标识
g_2	比特串	/预处理的 P_2 对值
Q_E	SM9EncryptMasterPublicKey	/预处理对方用户加密公钥坐标值

输出：

KeyC	SM9KeyPackage	

详细的计算过程见 GB/T 38635.2—2020 的 8.2。

8.5 密钥解封

SM9 密钥封装是指使用通过对运算生成对称加密密钥，并产生基于对方加密公钥坐标值的点的密文即加密封装的密文。

输入：

ID	字节串	/解封方身份标识
d	SM9EncryptPrivateKey	/解封方加密私钥
C	SM9EncryptMasterPublicKey	/加密封装的密文

输出：

Key	比特串	/密钥

详细的计算过程见 GB/T 38635.2—2020 的 8.4。

8.6 加密

SM9 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：

M	比特串	/明文
mlen	整数	/明文长度
KDF_ID	整数	/对称加密算法类型，序列：0，分组：1
g_2	比特串	/预处理的 P_2 对值
Q_E	SM9EncryptMasterPublicKey	/预处理对方用户加密公钥坐标值

输出：

C	SM9Cipher	/密文

详细的计算过程见 GB/T 38635.2—2020 的 9.2。

8.7 解密

SM9 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：

ID	字节串	/解密方身份标识
KDF_ID	整数	/对称加密算法类型，序列：0，分组：1
d	SM9EncryptPrivateKey	/解密方加密私钥
C	SM9Cipher	/加密封装的密文

输出：

M	比特串	/明文
mlen	整数	/明文长度

详细的计算过程见 GB/T 38635.2—2020 的 9.4。

8.8 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。

设密钥协商双方身份标识为 ID_A、ID_B，分别预处理对应的 Q_E 得到 Q_{EA} 和 Q_{EB}。

其加密密钥对分别为(d_A，Q_A)和(d_B，Q_B)，双方需要获得的密钥数据的比特长度为 klen。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 A。

输入：

Q_{EB}	SM9EncryptMasterPublicKey	/加密坐标

输出：

R_A	SM9EncryptMasterPublicKey	/临时密钥

用户 B。

输入：

Q_{EA}	SM9EncryptMasterPublicKey	/加密坐标

输出：

R_B	SM9EncryptMasterPublicKey	/临时密钥

详细的计算过程见 GB/T 38635.2—2020 的 7.1。

第二阶段：计算共享秘密密钥

用户 B。

输入：

R_A	SM9EncryptMasterPublicKey	/临时密钥
R_B	SM9EncryptMasterPublicKey	/临时密钥
ID_A	字节串	/A 身份标识
ID_B	字节串	/B 身份标识
P_{pub}	SM9EncryptMasterPublicKey	/加密主公钥
P_2	SM9P2	/P_2 生成元
D_B	SM9EncryptPrivateKey	/用户加密私钥
klen	整型	/需要输出的密钥数据的比特长度

输出：

S_B	比特串	/可选项，校验值，用于用户 A 校验 S_1
S_2	比特串	/可选项，用于对比 S_A 的校验值
SK_B	比特串	/位长为 klen 的密钥数据

详细的计算过程见 GB/T 38635.2020 的 7.2。

用户 A。

输入：

R_A	SM9EncryptMasterPublicKey	/临时密钥
R_B	SM9EncryptMasterPublicKey	/临时密钥
ID_A	字节串	/A 身边标识
ID_B	字节串	/B 身边标识
P_{pub}	SM9EncryptMasterPublicKey	/加密主公钥
P_2	SM9P2	/P_2 生成元
d_A	SM9EncryptPrivateKey	/用户加密私钥
klen	整型	/需要输出的密钥数据的比特长度

输出：

S_A	比特串	/可选项，校验值，用于用户 B 校验 S_2
S_1	比特串	/可选项，用于对比 S_B 的校验值
SK_A	比特串	/位长为 klen 的密钥数据

详细的计算过程见 GB/T 38635.2—2020 的 7.2。

调用生成密钥算法产生临时密钥对(r_B,R_B)，将 R_B 和用户 B 的用户身份标识 ID_B 发送给用户 A。

中华人民共和国密码
行业标准
SM9 密码算法使用规范
GM/T 0080—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 28 千字
2021 年 5 月第一版　2021 年 5 月第一次印刷
*
书号:155066·2-35842　定价 18.00 元

GM/T 0080-2020

码上扫一扫　正版服务到