ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0081—2020

SM9 密码算法加密签名消息语法规范

SM9 cryptographic algorithm encryption and signature message syntax 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、西安工业大学、深圳奥联信息安全技术有限公司、中国科学院自动化研究所苏州研究院。

本文件主要起草人：袁峰、王晓春、容晓峰、杜志强、蔡先勇、药乐、张立圆、封维端、蒋楠、汪雪林。

SM9 密码算法加密签名消息语法规范

1 范围

本文件定义了使用 SM9 密码算法的加密签名消息语法。

本文件适用于使用 SM9 算法进行加密和签名操作时对操作结果的标准化封装。

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 33560 信息安全技术 密码应用标识规范

GB/T 38635(所有部分) 信息安全技术 SM9 标识密码算法

GM/T 0080 SM9 密码算法使用规范

GM/Z 4001—2013 密码术语

3 术语和定义

GB/T 38635(所有部分)和 GM/Z 4001—2013 界定的以及下列术语适用于本文件。

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

一种国家商用双线性对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

标识信任链　identity trust chain

一个分层的标识应用属性信息的有序集合，里面存储的是从用户端到根 KGC 的标识应用属性信息。

4　缩略语

下列缩略语适用于本文件。

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

IRIs：国际资源标识符(Internationalized Resource Identifiers)

IRL：标识撤销列表(Identifier Revocation List)

KGC：密钥生成中心(Key Generation Center)

OID：对象标识符(Object identifier)

PKG：私钥生成(Private Key Generation)

PPS：公共参数服务器(Public Parameter Server)

5　OID 定义

本文件对 6 个对象 sm9data，signedData，envelopedData，signedAndEnvelopedData，encryptedData 和 keyAgreementInfo 的标识符进行了定义，详见表 1。

表 1　对象标识符

对象标识符 OID	对象标识符定义
1.2.156.10197.6.1.4.4	SM9 加密及签名消息语法规范
1.2.156.10197.6.1.4.4.1	数据类型 data
1.2.156.10197.6.1.4.4.2	签名数据类型 signedData
1.2.156.10197.6.1.4.4.3	数字信封数据类型 envelopedData
1.2.156.10197.6.1.4.4.4	签名及数字信封数据类型 signedAndEnvelopedData
1.2.156.10197.6.1.4.4.5	加密数据类型 encryptedData
1.2.156.10197.6.1.4.4.6	密钥协商类型 keyAgreementInfo

6　基本类型定义

6.1　IdentifierRevocationLists

IdentifierRevocationLists 类型标明一个标识撤销列表的集合。

IdentifierRevocationLists::= SET OF IdentifierRevocationList

IdentifierRevocationList 的定义按附录 A 定义。

6.2 ContentEncryptionAlgorithmIdentifier

ContentEncryptionAlgorithmIdentifier 类型标明一个数据加密算法，其 OID 见 GB/T 33560。

ContentEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.3 DigestAlgorithmIdentifier

DigestAlgorithmIdentifier 类型标明一个消息摘要算法，在本文件中为 SM3 算法，其 OID 见GB/T 33560。

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

6.4 DigestEncryptionAlgorithmIdentifier

DigestEncryptionAlgorithmIdentifier 类型标明一个签名算法，在本文件中为 SM9 密码算法，其 OID 见 GB/T 33560。

DigestEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.5 KeyEncryptionAlgorithmIdentifier

KeyEncryptionAlgorithmIdentifier 类型标明加密对称密钥的加密算法。

KeyEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.6 Version

Version 类型标明语法版本号。

Version ::= INTEGER(1)

6.7 ContentInfo

ContentInfo 类型标明内容交换通用语法结构，内容交换的通用语法结构定义如下：

```
ContentInfo ::= SEQUENCE {
    contentType                 ContentType,
    content                 [0] EXPLICIT contentType OPTIONAL
}
ContentType ::= OBJECT IDENTIFIER
```

其中：

ContentType 内容类型是一个对象标识符，其定义见第 5 章。

content 内容，可选。

6.8 Identifier

标识类型，该类型标明一个标识有用的基本项。

```
Identifier::= SEQUENCE{
    version                 EXPLICIT VERSION DEFAULT v1,
    ibcType                 OBJECT IDENTIFIER,
    ibcTypeAlias        [0] OCTET STRING OPTIONAL,
    identityData            OCTET STRING,
    validStart              UTCTIME,
    validEnd            [1] UTCTIME OPTIONAL,
```

```
    extensions          [2]  Extensions OPTIONAL
}
```

version 标识信息的版本号，默认为 1；

ibcType 是一个对象标识符 oid，用于定义该标识应用的算法；

ibcTypeAlias 是一个标识的别名，可选项；

identifyData 描述标识的内容；

validStart 用于描述标识有效期的起始时间；

validEnd 该项是可选的，用于描述标识有效期的终止时间，如果该项不存在则该标识的结束有效期和公开参数的结束有效期一致；

extensions 该项是可选的，本项是一个扩展序列(SEQUENCE)，如果出现，此项由一个或多个标识扩展的序列组成。

```
Externsions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE {
        extnID          OBJECT IDENTIFIER,
        critical        BOOLEAN DEFAULT FALSE,
        extnValue       OCTET STRING
}
```

extnID：表示一个扩展元素的 OID；

critical：表示这个扩展元素的重要性；

extnValue：表示这个扩展元素的值，字符串类型。

如果是 ibcType 是 SM9 的 OID，则扩展性需包括颁发该标识密钥的密钥基础设施的公开参数服务器信息，具体定义格式如下：

extnID 的内容为 1.xx.xxx…；

critical 的内容为 TRUE；

extnValue 的内容为 DistricInfo 的 ASN1 编码数据，DistricInfo 具体定义如下：

```
DistricInfo ::=SEQUENCE {
    district            IA5String,
    districtNo          INTEGER,
}
```

district ：本项描述生成该标识密钥的基础设施的公共参数发布服务的地址信息；

districtNo：该项描述在公共参数发布服务中存在多套公开参数信息时，生成该标识密钥的公共参数信息的唯一编号。

6.9 Validity

```
Validity::= SEQUENCE{
    notBefore       Time,
    notAfter        Time,
    Time ::= CHOICE {
        utcTime         UTCTime,
        generalTime     GeneralizedTime
    }
}
```

6.10 IBCSysParamsPublishInfo

公开参数的发布信息

```
IBCSysParamsPublishInfo ::= SEQUENCE {
    ibcSysParams            IBCSysParams,
    signatureAlgorithm      OBJECT IDENTIFIER,
    signatureValue          BIT STRING
}
```

上述标识信息数据结构 ibcSysParams，signatureAlgorithm 和 signatureValue 三个域组成。这些域的含义如下：

ibcSysParams 域包含公开参数的相关信息；

signatureAlgorithm 域包含标识应用属性信息签发机构签发该标识应用属性信息所使用的密码算法的标识符；

```
AlgorithmIdentifier ::= SEQUENCE {
    Algorithm    OBJECT IDENTIFIER,
    Parameters   ANY DEFINED BY algorithm OPTIONAL
}
BeSignParamsPubInfo::= SEQUENCE {
    ibcSysParams              IBCSysParams,
    signatureAlgorithm        OBJECT IDENTIFIER
}
```

BeSignParamsPubInfo 描述待签名数据；

signatureValue 域包含了对 ibcSysParams 域和 signatureAlgorithm 域进行数字签名的结构，采用 ASN.1 DER 编码的 BeSignParamsPubInfo 的摘要作为数字签名的输入，而签名的结构则按照 ASN.1 编码成 BIT STRING 类型并保存在标识信息的签名值域内。

SM9 密码算法签名数据格式见 GM/T 0080。

6.11 IDAppAttr

IDAppAttr 包含标识信息结构中的前五个项的信息。这些信息主要有主体标识和颁发者标识、上一次主体标识以及扩展项等。本条的下述段落描述这些项的语法和语义。

```
IDAppAttr ::= SEQUENCE{
    versoin                         Version DEFAULT v1,
    serialNumber                    IdentifierSerialNumber,
    subjectId                       Identifier,
    sysParamsPublishInfo            IBCSysParamsPublishInfo,
    extensions                [0]   EXPLICIT Externsiions OPTIONAL
}
version::= INTEGER { v1(0) }
IdentifierSerialNumber ::= INTEGER

Externsions ::= SEQUENCE SIZE (1..MAX) OF Extension
```

version：本项描述了编码标识应用属性的版本号；

serialNumber：本项描述该标识在 IBC 系统中唯一编号；

subjectId:本项记录标识主体;
sysParamsPublishInfo:系统公开参数发布信息;
extensions:本项是一个或者多个标识扩展的序列(SEQUENCE)。

7 数据类型 Data

Data 数据类型结构定义如下:

```
Data ::= OCTET STRING
```

Data 数据类型表示任意的字节串,比如 ASCII 文本文件。

8 签名数据类型

8.1 SignedData 类型

SignedData 数据类型由任意类型的数据和至少一个签名者的签名值组成。任意类型的数据能够同时被任意数量的签名者签名。

SignedData 数据类型结构定义如下:

```
SignedData ::= SEQUENCE {
    version                         Version,
    digestAlgorithms                DigestAlgorithmIdentifiers,
    contentInfo                     ContentInfo,
    ibcSysParamsPublishInfos    [0] IMPLICIT IBCSysParamsPublishInfos OPTIONAL,
    irls                        [1] IMPLICIT IdentifierRevocationLists OPTIONAL,
    signerInfos                     SignerInfos
}
IBCSysParamsPublishInfos::= SET OF IBCSysParamsPublishInfo
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
SignerInfos::= SET OF SignerInfo
```

结构中各项含义见表 2。

表 2 SignedData 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号,为 1
digestAlgorithms	DigestAlgorithmIdentifiers	消息摘要算法标识符的集合
contentInfo	ContentInfo	被签名的数据内容,数据类型见第 5 章
ibcSysParamsPublishInfos	IBCSysParamsPublishInfos	公开参数发布信息的集合
irls	IdentifierRevocationLists	标识吊销列表集合
signInfos	SignerInfo	每个签名者信息的集合

8.2 SignerInfo 类型

SignerInfo 类型结构定义如下：

```
SignerInfo ::= SEQUENCE {
    version                     Version,
    issuerIdentifier            Identifier,
    digestAlgorithm             DigestAlgorithmIdentifier,
    authenticatedAttributes     [0] IMPLICIT Attributes OPTIONAL,
    digestEncryptionAlgorithm   DigestEncryptionAlgorithmIdentifier,
    encryptedDigest             SM9Signature,
    unauthenticatedAttributes   [1] IMPLICIT Attributes OPTIONAL
}
```

结构中各项含义见表 3。

表 3 SignerInfo 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号
issuerIdentifier	Identifier	签名者标识
digestAlgorithm	DigestAlgorithmIdentifier	对内容进行摘要计算的消息摘要算法，本文件使用 SM3 算法
authenticatedAttributes	Attributes	是经由签名者签名的属性的集合，该域可选。如果该域存在，该域中摘要的计算方法是对原文进行摘要计算结果
digestEncryptionAlgorithm	DigestEncryptionAlgorithmIdentifier	SM9 双线性对椭圆曲线密码算法标识符
encryptedDigest	SM9Signature	值是 SM9Signature，用签名者私钥进行签名的结果，其定义见 GM/T 0080
unauthenticatedAttributes	Attributes	

9 数字信封数据类型

9.1 EnvelopedData 类型

数字信封 EnvelopedData 数据类型由加密数据和至少一个接收者的数据加密密钥的密文组成。其中，加密数据是用数据加密密钥加密的，数据加密密钥是用接收者的公钥加密的。

该类型用于为接收者的 Data、DigestedData 或 SignedData 三种类型的数据做数字信封。

EnvelopedData 数据类型结构定义如下：

```
EnvelopedData ::= SEQUENCE {
    version                 Version,
    recipientInfos          RecipientInfos,
    encryptedContentInfo    EncryptedContentInfo
}
```

RecipientInfos ::= SET OF RecipientInfo

结构中各项含义见表4。

表4 EnvelopedData数据类型

字段名称	数据类型	含义
version(1)	Version	语法的版本
recipientInfos	RecipientInfos	每个接收者信息的集合,至少要有一个接收者
encryptedContentInfo	EncryptedContentInfo	加了密的内容信息

```
EncryptedContentInfo ::= SEQUENCE {
    contentType                     ContentType,
    contentEncryptionAlgorithm      ContentEncryptionAlgorithmIdentifier,
    sharedInfo                [0]   OCTET STRING OPTIONAL,
    sharedInfo2               [1]   OCTET STRING OPTIONAL,
    encryptedContent          [2]   IMPLICIT EncryptedContent OPTIONAL
}
EncryptedContent ::= OCTET STRING
```

结构中各项含义见表5。

表5 EncryptedContentInfo数据类型

字段名称	数据长度	含义
contenType	ContentType	内容的类型
contentEncryptionAlgorithm	ContentEncryptionAlgorithmIdentifier	内容加密算法(和相应的参数)
sharedInfo	OCTET STRING	协商好的共享信息,可选
sharedInfo2	OCTET STRING	协商好的共享信息,可选
encryptedContent	EncryptedContent	内容加密的结果,可选

9.2 RecipientInfo类型

每个接收者信息用RecipientInfo类型表示。

RecipientInfo类型结构定义如下:

```
RecipientInfo ::= SEQUENCE{
    Version                 Version,
    issuerIdentifier        Identifier,
    keyEncryptionAlgorithm  KeyEncryptionAlgorithmIdentifier,
    encryptedKey            SM9cipher
}
```

结构中各项含义见表6。

表 6　RecipientInfo 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号
issuerIdentifier	Identifier	接收者标识
keyEncryptionAlgorithm	KeyEncryptionAlgorithmIdentifier	用接收者公钥加密数据加密密钥的算法，为 SM9 加密算法
encryptedKey	SM9cipher	数据加密密钥密文 SM9Cipher，其定义见 GM/T 0080

10　签名及数字信封数据类型 SignedAndEnvelopedData

SignedAndEnvelopedData 数据类型由任意类型的加密数据、至少一个接收者的数据加密密钥和至少一个签名者的签名组成。

SignedAndEnvelopedData 数据类型结构定义如下：

```
SignedAndEnvelopedData ::= SEQUENCE {
    version                    Version,
    recipientInfos             RecipientInfos,
    digestAlgorithms           DigestAlgorithmIdentifiers,
    encryptedContentInfo       EncryptedContentInfo,
    idAppAttrInfos      [0]    IMPLICIT IDAppAttrInfos OPTIONAL,
    irls                [1]    IMPLICIT IdentifierRevocationLists OPTIONAL,
    signerInfos                SignerInfos
}
```

结构中各项含义见表 7。

表 7　SignedAndEnvelopedData 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号
recipientInfos	RecipientInfos	每个接受者信息的集合，至少一个元素
digestAlgorithms	DigestAlgorithmIdentifiers	消息摘要算法标识符的集合
encryptedContentInfo	EncryptedContentInfo	加了密的内容，可以是任何定义的数据类型
idAppAttrInfos	IDAppAttrInfos	标识应用属性信息的集合
irls	IdentifierRevocationLists	标识吊销列表集合
signerInfos	SignerInfos	每个签名者的集合，至少要有一个元素

11　加密数据类型 EncryptedData

EncryptedData 数据类型由任意类型的加了密的数据组成，数据类型既没有接收者也没有加密的

数据加密密钥。

EncryptedData 数据类型定义如下：

```
EncryptedData ::= SEQUENCE {
    Version                    Version,
    encryptedContentInfo       EncryptedContentInfo
}
```

结构中各项含义见表 8。

表 8　EncryptedData 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号
encryptedContenInfo	EncryptedContentInfo	加了密的内容信息

12　密钥协商类型 KeyAgreementInfo

密钥协商 KeyAgreementInfo 数据类型标明两个用户之间建立一个共享秘密密钥的结构，通过这种方式能够确定一个共享秘密密钥的值。

该类型用于两个用户为产生共享秘密密钥进行的公共参数交换。

```
KeyAgreementInfo::= SEQUENCE{
    version                    Version(1),
    tempKey                    SM9MastEncryptPublicKey,
    userID_A                   OCTET STRING
    userID_B                   OCTET STRING
    hid                        OCTET STRING
}
```

结构中各项含义见表 9。

表 9　KeyAgreementInfo 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号
tempKey	SM9MastEncryptPublicKey	临时密钥，见附录 A，或见 GM/T 0080
$userID_A$	OCTET STRING	发起方用户标识
$userID_B$	OCTET STRING	响应方用户标识
hid	OCTET STRING	算法类型

附 录 A
（规范性）
IRL 标识吊销列表结构

A.1 IRL 数据结构的的 ASN.1 描述如下：

```
IdentifierRevocationList::= SEQUENCE {
    tbsIdList        TBSIdList,                    /注册服务器的请求信息
    signInfos        SignerInfos                   /签名者的信息
}
```

TBSIdList 域包含了主体名称和颁发者名称、颁发日期、撤销标识信息和 IRL 扩展信息。

```
TBSIdList::= SEQUENCE {
    Version(1)                  Version,/版本号,值为 1
    signatureOID                AlgorithmIdentifier, /签名算法
    issuerIdentifier            Identifier,/颁发者标识
    thisUpdate                  GeneralizedTime,/生效日期
    nextUpdate              [0] GeneralizedTime OPTIONAL,/下次更新日期
    revokedIds                  RevokedIds,/撤销标识集合
    irlExtensions           [1] EXPLICIT Extensions OPTIONAL/扩展项
}
Version ::= INTEGER(1)
RevokedIds ::= SEQUENCE OF RevokedId
RevokedId::= SEQUENCE{
    id                          OCTET STRING,/撤销标识内容
    revocationDate              GeneralizedTime,/撤销时间
    IrlEntryExtensions      [0] Extensions OPTIONAL/撤销原因
}
```

A.2 IBC 公共参数结构

```
IBCSysParams ::= SEQUENCE {
    version                     INTEGER{v2(2)},
    districtName                IA5String,
    districtSerial              INTEGER,
    validity                    ValidityPeriod,
    ibcPublicParameters         IBCPublicParameters,
    ibcIdentityType             OBJECT IDENTIFIER,
    issuerID                    Identifier,/公开参数颁发者
    ibcParamExtensions          IBCParamExtensions OPTIONAL
}
```

其中：

version 版本项，确定了 IBCSysParams 格式的版本。本文件中提及的格式，应设置为 2。

districtName 名称项，是一个应以 URI 或者 IRI 编码的 IA5 字符串。

districtSerial 是一个代表了可用的唯一 IBC 公共参数（对于以 districtName 定义的 URI 或 IRI）设置的整数。如果为 districtName 公布一个新的参数，那么 districtSerial 的数值应大于之前使用的

districtSerial数值。

validity 有效期项，确定了一个具体 IBCSysParams 范例的寿命，并按照以下内容确定：

notBefore 与 notAfter 的数值必须以格林威治时间表示，并包含秒（如：时间表示为 YYYYMMDDHHMMSSZ），即使是秒数为零，也要表示为最近的秒数。客户必须确认它使用的 IBC 公共参数的日期处于 IBC 公共参数的 notBefore 时间与 notAfter 时间之间，于此同时，如果日期没有处于这一区间时，不能使用用于 IBC 加密操作的参数。

当 IbcPublicParameters，IbcIdentityType 或者 IbcParamExtensions 的数值改变了一个区域时，IBC 公共参数应重新生成与公布。客户应在应用程序配置间隔内重新找回 IBC 公共参数，以确保参数的版本为最新。

IBCPublicParameters 公共参数项，是一个包含了公共参数（对应于 PKG 支持的 IBC 算法式）的结构。其定义如下：

```
IBCPublicParameters ::= SEQUENCE (1..MAX) OF IBCPublicParameter
IBCPublicParameter ::= SEQUENCE {
    ibcAlgorithm            OBJECT IDENTIFIER,
    publicParameterData     OCTET STRING
}
```

其中：

ibcAlgorithm OID 确定了 IBC 算法式。两个 IBC 算法式的 OID 以及他们的 publicParameterData 结构。

publicParameterData 是一个 SM9PublicParameterData 的 DER 编码结构，其包含了真实的加密参数。其具体结构为：

```
SM9PublicParameterData::= SEQUENCE {
    pkgID                   OCTET STRING,
    encMastPublicKey        SM9EncryptMasterPublicKey,
    signMastPublicKey       SM9SignMasterPublicKey

}
```

pkgID：私钥生成中心标识

encMastPublicKey：加密主公钥

signMastPublicKey：签名主公钥

ibcIdentityType 标识类型项，是一个确定在这一区域使用的身份类型的 OID。对于每一个 OID、所需要以及可选择的域都应为依赖于应用程序而存在。

IBCParamExtensions 扩散参数项，是一组用于确定特定操作所需额外参数的一组扩展。定义如下：

```
IBCParamExtensions ::= SEQUENCE OF IBCParamExtension
IBCParamExtension ::= SEQUENCE {
    ibcParamExtensionOID    OBJECT IDENTIFIER,
    ibcParamExtensionValue  OCTET STRING
}
```

其中：

ibcParamExtensionValue 的八位字符串内容由具体的 ibcParamExtensionOID 确定。一个域的 IBCParamExtensions 可能包含任何数量的扩展（包括零在内）。一个实际应用的扩展实例如下：它为电

子邮件系统用户提供了一个 URI,在这里加密的信息可以被解密,同时对用户可见。另一个实例如下:它提供了商标信息以使得银行可以为处于不同业务部门的客户提供不同的用户界面。

```
IbcParamExt OBJECT IDENTIFIER ::= {
    ibcs  ibcs3(3)  parameter-extensions(2)
}
```

参 考 文 献

[1] GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1):基本记法规范(ISO/IEC 8824-1:2002,IDT)

中华人民共和国密码
行业标准
SM9密码算法加密签名消息语法规范
GM/T 0081—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 1.25 字数 36千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35848 定价 24.00 元

GM/T 0081-2020

码上扫一扫 正版服务到