表 1　对象标识符

对象标识符 OID	对象标识符定义
1.2.156.10197.6.1.4.2	SM2 密码算法加密签名消息语法规范
1.2.156.10197.6.1.4.2.1	数据类型 data
1.2.156.10197.6.1.4.2.2	签名数据类型 signedData
1.2.156.10197.6.1.4.2.3	数字信封数据类型 envelopedData
1.2.156.10197.6.1.4.2.4	签名及数字信封数据类型 signedAndEnvelopedData
1.2.156.10197.6.1.4.2.5	加密数据类型 encryptedData
1.2.156.10197.6.1.4.2.6	密钥协商类型 keyAgreementInfo

6　基本类型定义

6.1　CertificateRevocationLists

CertificateRevocationLists 类型标明一个证书撤销列表的集合。

CertificateRevocationLists ::= SET OF CertificateRevocationList

6.2　ContentEncryptionAlgorithmIdentifier

ContentEncryptionAlgorithmIdentifier 类型标明一个数据加密算法。其 OID 见 GM/T 0006。

ContentEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.3　DigestAlgorithmIdentifier

DigestAlgorithmIdentifier 类型标明一个消息摘要算法，在本标准中为 SM3 算法，其 OID 见 GM/T 0006。

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

6.4　DigestEncryptionAlgorithmIdentifier

DigestEncryptionAlgorithmIdentifier 类型标明一个签名算法，在本标准中为 SM2 密码算法，其 OID 见 GM/T 0006。

DigestEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.5　ExtendedCertificateOrCertificate

ExtendedCertificateOrCertificate 类型指定一个 PKCS#6 扩展证书或者一个 X.509 证书。这一类型见 PKCS#6 第 6 节推荐的语法：

```
ExtendedCertificateOrCertificate ::= CHOICE {
  certificate Certificate,--X.509
  extendedCertificate [0] IMPLICIT ExtendedCertificate
}
```