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(1)	Version	语法的版本号
issuerAndSerialNumber	IssuerAndSerialNumber	一个证书颁发者可识别名和颁发者确定的证书序列号,可据此确定一份证书和与此证书对应的实体及公钥
digestAlgorithm	DigestAlgorithmIdentifier	对内容进行摘要计算的消息摘要算法,本规范采用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	SM2-1椭圆曲线数字签名算法标识符
encryptedDigest	OCTET STRING	值是SM2Signature,用签名者私钥进行签名的结果,其定义见GM/T 0009。编码格式为r‖s。

9 数字信封数据类型envelopedData

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	语法的版本号
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