**商用密码应用领域中的相关**

**OID 对象标识符定义**

**备注**

通用对象标识符

1.2  国际标准化组织成员标识

1.2.156 中国

1.2.156.10197 国家密码管理局

1.2.156.10197.1 密码算法

分组密码算法对象标识符

1.2.156.10197.1.100  分组密码算法

1.2.156.10197.1.101  SM6分组密码算法

1.2.156.10197.1.102  SM1分组密码算法

1.2.156.10197.1.103  SSF33密码算法

1.2.156.10197.1.104  SM4分组密码算法

1.2.156.10197.1.105  SM7分组密码算法

1.2.156.10197.1.106  SM8分组密码算法

序列密码算法对象标识符

 1.2.156.10197.1.200  序列密码算法

 1.2.156.10197.1.201  SM5序列密码算法

公钥密码算法对象标识符

 1.2.156.10197.1.300  公钥密码算法

1.2.156.10197.1.301  SM2椭圆曲线密码算法

1.2.156.10197.1.301.1  SM2-1椭圆曲线数字签名算法

1.2.156.10197.1.301.2  SM2-2椭圆曲线密钥交换协议

1.2.156.10197.1.301.3  SM2-3椭圆曲线加密算法

1.2.156. 10197.1.302  SM9标识密码算法

1.2.156. 10197.1.302.1  SM9-1数字签名算法

1.2.156. 10197.1.302.2  SM9-2密钥交换协议

1.2.156. 10197.1.302.3  SM9-3密钥封装机制和公钥加密算法

1.2.156. 10197.1.310  RSA密码算法\*

杂凑算法对象标识符

1.2.156.10197.1.400  杂凑算法

1.2.156.10197.1.401  SM3密码杂凑算法

1.2.156.10197.1.401.1  SM3密码杂凑算法，无密钥使用

1.2.156.10197.1.401.2  SM3密码杂凑算法，有密钥使用

1.2.156.10197.1.410  SHA-1算法\*

1.2.156.10197.1.410.1  SHA-1无密钥\*

1.2.156.10197.1.410.2  SHA-1有密钥\*

1.2.156.10197.1.411  SHA256算法\*

1.2.156.10197.1.411.1  SHA256无密钥\*

1.2.156.10197.1.411.2  SHA256有密钥\*

组合运算算法对象标识符

1.2.156.10197.1.500  组合运算机制

1.2.156.10197.1.501  基于SM2算法和SM3算法的签名

1.2.156.10197.1.503  基于SM2算法和SHA256算法的签名

1.2.156.10197.1.504  基于RSA算法和SM3算法的签名

1.2.840.113549.1.1.5  基于RSA算法和SHA-1算法的签名\*

1.2.840.113549.1.1.11  基于RSA算法和SHA256算法的签名\*

CA 代码对象标识符

1.2.156.10197.4.3  CA代码

