# 调研报告：椭圆曲线私钥 ASN.1 形式调研

完成者姓名：杨一凡 学号：520021911080

## 1．ASN.1 抽象语法标记：

### 1.1．ASN.1 抽闲语法标记简介：

ASN.1 是一种 ISO/ITU-T 标准，描述了一种对数据进行表示、编码、传输和解码的数据格式。它提供了一整套正规的格式用于描述对象的结构，而不管语言上如何执行以及这些数据的具体指代，也不用去管到底是什么样的应用程序。

### 1.2．ASN.1 数据类型：

ASM.1 提供了一些基本的预定义数据结构：
UNIVERSAL 0 保留给编码规则使用；
UNIVERSAL 1 布尔类型
UNIVERSAL 2 整型
UNIVERSAL 3 零或多个比特的序列
UNIVERSAL 4 零或多个字节的序列
UNIVERSAL 5 NULL
UNIVERSAL 6 对象标识符类型
UNIVERSAL 7 对象描述符类型
UNIVERSAL 8 外部类型和类型实例
UNIVERSAL 9 实数类型
UNIVERSAL 10 枚举类型
UNIVERSAL 11 嵌入的 pdv 类型
UNIVERSAL 12 UFT8 字符串类型
UNIVERSAL 13 相关对象标识符类型
UNIVERSAL 14-15 保留给本建议的以后版本和国际标准使用
UNIVERSAL 16 序列和类型序列
UNIVERSAL 17 集合和类型的集合
UNIVERSAL 18-22，25-30 字符串类型
UNIVERSAL 23-24 时间类型
UNIVERSAL 31～ 保留给本建议以外的类型和国际标准使用

### 1.3．ASN.1 定义数据结构类型：

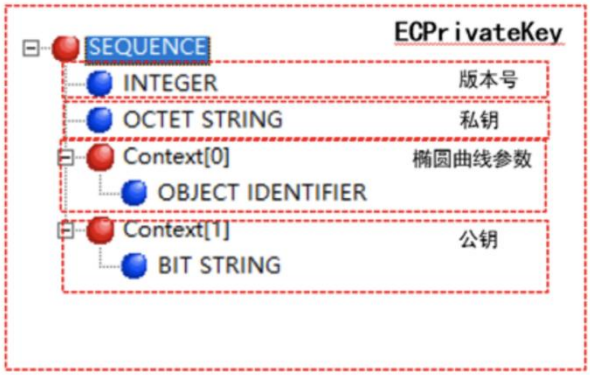
ASN.1 可以定义如下的数据结构类型：
结构（SEQUENCE）
列表（SEQUENCE OF）
类型选择（CHOICE）

# 2. 椭圆曲线私钥 ASN.1 形式：

## 2.1. ECC 算法 ASN.1 形式：

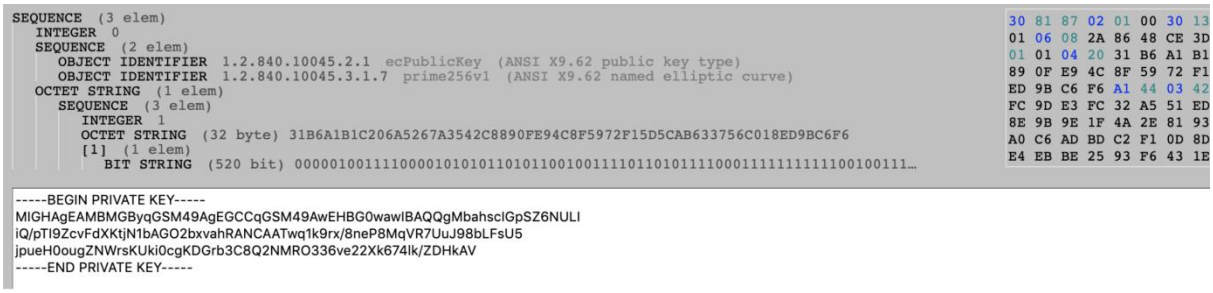
（1）ECC 私钥数据格式的 ASN.1 形式：

```
ECPrivateKey ::= SEQUENCE {
      version INTEGER { ecPrivkeyVer1(1) } (ecPrivkeyVer1),
      privateKey OCTET STRING,
      parameters [0] ECDomainParameters {{ SECGCurveNames }} OPTIONAL,
      publicKey [1] BIT STRING OPTIONAL
}
```




其将 ECC 私钥定义为 SEQUENCE 的数据结构类型，第一个字段为版本号（version），使用整型数进行相应的表示；第二个字段为 OCTER STRING 类型的私钥，以 16 进制的方法表示；第三个字段为可选的椭圆曲线参数；第四个字段为 BIT STRING 类型公钥，以 2 进制的方法表示。并且最后的两个字段均为可选的。

使用 openssl 创建一个 ECC 私钥，并对其进行 ASN.1 格式解析，结果如下图所示：




其中 1.2.840.10045.2.1（ecPublicKey）和 1.2.840.10045.3.1.7（prime256v1）为算法标识，后面为相应的私钥信息，其中包括了版本号 1，OCTET STRING 类型的私钥 31B6……F6，BIT STRING 类型的公钥 0000 0100 1111 0000……

Parameters 字段的 ASN.1 形式如下图所示：

```
Parameters::= CHOICE {
    ecParameters ECParameters,
    namedCurve  ObjectIdentifier,
    implicitlyCA  NULL
}
```

## 2.2. SM2 椭圆加密算法 ASN.1 形式：

(1) 密钥数据格式：

GB/T 35276—2017《信息安全技术 SM2 密码算法使用规范》：

SM2 算法私钥数据格式的 ASN.1 定义为：

```
SM2PrivateKey ::= INTEGER
```

SM2 算法公钥数据格式的 ASN.1 定义为：

```
SM2PublicKey ::= BIT STRING
```

SM2PublicKey 为 BIT STRING 类型，内容为 04 ‖ X ‖ Y，其中，X 和 Y 分别标识公钥的 x 分量和 y 分量，其长度各为 256 位。

GB/T 35275—2017《信息安全技术 SM2 密码算法加密签名消息语法规范》：

SM2 算法公钥数据格式的 ASN.1 定义为：

```
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm AlgorithmIdentifier {{ECPKAlgorithms}},
    subjectPublicKey SM2PublicKey
}
```

其中：

algorithm 定义了公钥的类型

subjectPublicKey 定义了公钥的实际值

AlgorithmIdentifier 是对象标识与参数的绑定，其定义如下：

```
AlgorithmIdentifier ::= SEQUENCE {
    algorithm OBJECT IDENTIFIER,
    parameters ANY DEFINED BY algorithm OPTIONAL
```

SM2 算法私钥数据格式的 ASN.1 定义为：

```
ECPrivateKey{CURVES:IOSet} ::= SEQUENCE {
    version INTEGER { ecPrivkeyVer1(1) } (ecPrivkeyVer1),
    privateKey SM2PrivateKey,
    parameters [0] Parameters{{IOSet}} OPTIONAL,
    publicKey [1] SM2PublicKey
}
```

其中，version 表明了私钥的版本号，使用整数 1 表示 SM2 私钥的版本号。

(2) 加密数据格式：

SM2 算法加密后的数据格式的 ASN.1 定义为：

```
SM2Cipher ::= SEQENCE{
XCoordinate          INTEGER,              --x 分量
YCoordinate          INTEGER,              --y 分量
HASH                 OCTET STRING SIZE(32),--杂凑值
CipherText           OCTET STRING          --密文
}
```

其中，HASH 为使用 SM3 算法对明文数据运算得到的杂凑值，其固定长度为 256 位。CipherText

是与明文等长的密文。

(3) 签名数据格式：

SM2 算法签名数据格式的 ASN.1 定义为：

```
SM2Signature ::= {
R                    INTEGER,          --签名值的第一部分
S                    INTEGER           --签名值的第二部分
}
```

R 和 S 的长度各为 256 位。

(4) 密钥对保护数据格式：

SM2 密钥对的保护数据格式的 ASN.1 定义为：

```
SM2EnvelopedKey ::=SEQUENCE{
symAlgID             AlgorithmIdentifier,    --对称密码算法标识
symEncryptedKey      SM2Cipher,              --对称密钥密文
Sm2PublicKey         SM2PublicKey,           --SM2 公钥
Sm2EncryptedPrivateKey  BIT STRING           --SM2 私钥密文
}
```

在 SM2 密钥对传递时，需要对 SM2 密钥进行加密保护。具体的保护方法为：

A．产生一个对称密钥；

B．按对称密码算法标识指定的算法对 SM2 私钥进行加密，得到私钥的密文。若对称算法为分组算法，则其应用模式为 ECB；

C．使用外部 SM2 公钥加密对称密钥得到对称密钥密文；

D．将私钥密文、对称密钥密文封装到密钥对保护数据中。