## ECC实现ElGamal数字签名

13061082 陈逸伦

## 算法思想：

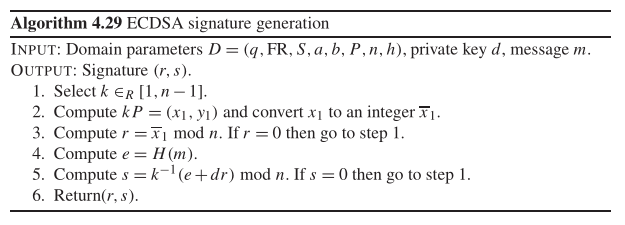
选取椭圆曲线上基准点P，由 可以得到

公钥:

私钥:

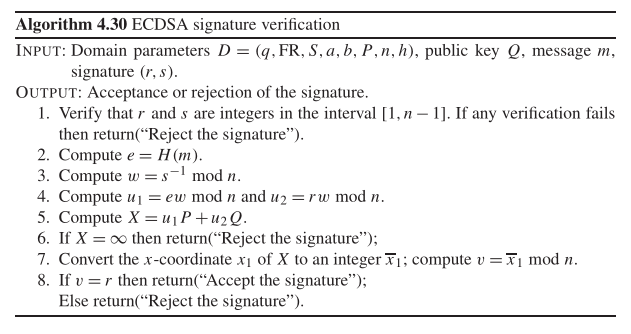
要注意椭圆曲线取模用的是p，而在以下的n指的是基准点的阶

**签名方案：**



为了方便起见，我直接取H(m)=m，不做hash变换，若需要可在函数H中添加Hash

**签名验证:**



**简要证明：**

容易验证

故有

分别取其x坐标即v = r

**安全性简要分析：**

若攻击者想伪造签名，则必须根据M, P, Q, n构造出签名(r, s)，满足计算

其中s, r, k为未知量。

若k, s固定取值, 原式可化为

若s, r固定取值，原式可化为

若r, k固定取值，原式可化为

均为椭圆曲线上离散对数问题。

## 样例输入输出：

（代码包含生成签名函数Sign()与验证签名函数Verify()）

sage: load("ECC.sage")

/\*\*\*\*\*\* ECC-signature \*\*\*\*\*\*/

Key (40-hex) : fffabcd2313312321313

PlainText (40-hex) : 35135345135fffbbbcaa

Signature :

r = 4aa5c936b66c7e2023e7a2bd774090bc204b6a59debeba870dd24cb17d205ca5

s = 317693f8373abcb871abf22181a2eae02f079eb61b6568b74c44f0529501b7d7

Verify : 1

## 参考文献:

1. Guide to Elliptic Curve Cryptography, by Darrel Hankerson, Alfred Menezes, Scott Vanstone