椭圆曲线公钥密码算法的数学原理分析

崔航

班级:2022211805 学号:2022211576

摘要

关键词: 素数检测，伪素数，强伪素数

目录

1 ECC

椭圆曲线加密算法，简称ECC，是基于椭圆曲线数学理论实现的一种非对称加密算法。相比于RSA，ECC使用更短的密钥，实现与RSA相当或更高的安全，

2 阿贝尔群

椭圆曲线的运算是在一个阿贝尔群上进行的，所以我们先来了解一下阿贝尔群的定义。

2.1 群

加群是一个集合，集合中的元素可以进行加法运算，且满足以下条件：

封闭性：对于任意的$a, b \in G$，$a + b \in G$。

结合律：对于任意的$a, b, c \in G$，$(a + b) + c = a + (b + c)$。

单位元：存在一个元素$0 \in G$，使得对于任意的$a \in G$，$a + 0 = 0 + a = a$。

逆元：对于任意的$a \in G$，存在一个元素$-a \in G$，使得$a + (-a) = (-a) + a = 0$。

交换律：对于任意的$a, b \in G$，$a + b = b + a$。

2.2 阿贝尔群

阿贝尔群是一个加群，且满足交换律。

参考文献

[1]

[2]

[3]

[4]