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 Fermat小定理

2 总结

本文介绍了几种素数检测方法，分别是Fermat素数检测，Solovay-Strassen素数检测和Miller-Rabin素数检测。并对这几种方法进行了代码实现.除了这些实用的素数概率性检测，还有一些更加复杂的素数检测方法，如AKS素数检测，Lenstra素数检测等，安全性和实用性不高，本文不再赘述。

参考文献

[1] 刘学军,邢玲玲,林和平,粟浩然.Miller-Rabin素数检测优化算法研究与实现[J].信息技术,2008,32(12):141-143+147.

[2] 魏成行. 素性检测算法研究及其在现代密码学中的应用[D].山东大学,2010.

[3] 彭韬,陈文庆.基于VB的大素数Solovay-Strassen检测的设计与实现[J].电子技术与软件工程,2020,(10):161-162.

[4] 陈恭亮.信息安全数学基础[M].清华大学出版社,2004.