计算机应用 2008 28 (05): 1156-1157 ISSN: 1001-9081 CN: 51-1307/TP

信息安全(Information security)

基于四元整数的ElGamal公钥密码体制

汪丽[1];邢伟[2];徐光忠[3]

东北大学[1]

东北大学理学院[2]

收稿日期 2007-11-12 修回日期 2008-1-2 网络版发布日期 2008-5-7 接受日期

摘要 介绍了既约剩余类的概念以及四元整数的一些基本性质，提出了基于四元整数群的ElGamal公钥密码体制(PKC)，其安全性基于大整数分解和离散对数问题的困难性，并在计算机上进行模拟实现，分析了其安全性。

Abstract This paper introduced the definition of congruence class and some basic property of integral quaternions, and proposed ElGamal Public-Key Cryptosystem (PKC) based on integral quaternions. Its security was based on the difficulty of large integer factorization and discrete logarithms problem. Simulation and realization were carried out in computer, furthermore the security of it was discussed and analysed.

关键词 Elgamal公钥密码 剩余类 四元整数 模n既约四元整数同余类群

Key words ElGamal Public-Key Cryptosystem (PKC);residue class;integral quaternions;congrauences class group of integral quaternions mod n

分类号

DOI:

通讯作者:
汪丽 wangli502521@163.com;tt2yy4@163.com

作者个人主页: 汪丽 邢伟 徐光忠