计算机应用研究
Application Research Of Computers

一类新的多关键字检索的公钥加密方案*

New public key encryption with multiple keyword search

中文关键词：带关键字检索的公钥加密方案 多关键字 拉格朗日插值多项式 陷门

英文关键词：PEKS(public key encryption with keyward search) multiple keyword Lagrange polynomial interpolation trapdoor

基金项目：国家自然科学基金资助项目(60842006);武警部队科研基金课题（wjk2009014）

作者	单位
黄大威1, 杨晓元1，2, 陈海滨1	(1. 武警工程学院 电子技术系 网络与信息安全武警部队重点实验室， 西安710086; 2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室， 西安 710071)

中文摘要：

针对带关键字检索的公钥加密体制中多关键字间的关系，分析了Joonsang Baek方案在安全性和可用性方面的缺陷，结合拉格朗日插值多项式，提出一种多关键字检索的公钥加密方案。该方案实现了从大量加密数据中选出部分数据进行优先处理，且方案只生成一个陷门信息，效率得到了提升。

英文摘要：

In view of the relationship between multiple keywords in public key encryption with keyword search,this paper analyzed the defects of Joonsang Baek’s scheme in security and usability. And proposed a sort of public key encryption with multiple keywords search, making use of the Lagrange polynomial interpolation.This scheme not only gave some datas choosed from the mass encrypted datas priority in disposing,but also produced only one tarpdoor,improving the efficiency.

主办单位：四川省计算机研究院 单位地址：成都市武侯区成科西路3号

服务热线：028-85249567 传真：028-85210177邮编：610041 Email：arocmag@163.com

蜀ICP备05005319号 本系统由北京勤云科技发展有限公司设计