通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

刘景美1,王延丽1,梁 斌1,赵林森2.基于枚举错误向量的McEliece公钥密码体制攻击方法[J].通信学报,2014,(5):65~69

基于枚举错误向量的McEliece公钥密码体制攻击方法

McEliece public key cryptosystem attack algorithm based on enumeration error vector

投稿时间： 2013-01-07

DOI：10.3969/j.issn.1000-436x.2014.5.009

中文关键词：Goppa码 McEliece 低重量码字 枚举错误向量

英文关键词:Goppa code McEliece low weight code word enumeration error vector

基金项目:国家自然科学基金资助项目(60903199)；高等学校创新引智基地基金资助项目(B08038)；中央高校基本科研业务费专项基金资助项目(K5051201014)

作者	单位
刘景美1，王延丽1，梁 斌1，赵林森2	1. 西安电子科技大学 综合业务网国家重点实验室，陕西 西安 710071；2. 西安邮电大学 电子工程学院，陕西 西安 710061

中文摘要：

对McEliece（M）公钥密码体制的安全性进行研究，该体制中错误向量的汉明重量相对于码长较小，而基于Goppa码的M公钥密码体制存在低重量的公开码字。基于以上分析，提出了枚举错误向量的攻击算法。重点分析了算法中错误翻转比特个数和算法迭代次数等参数对正确解密概率的影响，利用所提算法分析了基于（1024,524,101）Goppa码的M体制安全性。从算法正确解密概率和工作因子2个方面进行仿真分析，仿真实验表明所提算法在码重较低的情况下具有优异的性能。

英文摘要：

The research on the security of McEliece (M) public key cryptosystem was presented. The Hamming weight of error vector is less than the code length, and M public key cryptosystem based on Goppa code possesses low weight public code words. Considering the above analysis, an attack algorithm based on enumeration error vector was proposed. The effect on probability of correct decryption by the numbers of error flipping bits and algorithm iteration was focused on. And the security of (1 024,524,101) Goppa-based M public key cryptosystem was analyzed. Performance analysis of the proposed algorithm from probability of correct decryption and work factor was simulated, and the experimental results show that the proposed algorithm has a good performance when the code weight is low.

查看全文 查看/发表评论 下载PDF阅读器

关闭