电子与信息学报 2008 30 (6): 1453-1456 ISSN: 1009-5896 CN: 11-4494/TN

论文

私钥p,q共享低位比特RSA体制的小指数攻击

赵耀东, 戚文峰

郑州信息工程大学信息工程学院应用数学系 郑州 450002

收稿日期 2007-1-25 修回日期 2007-10-31 网络版发布日期 2008-8-28 接受日期

摘要
本文研究了组成RSA模数的两个素数p和q其低位比特相同,RSA公开密钥密码系统的安全性。其结果表明若RSA模数的两个素因子p和q共享低位比特,则当私钥d较小时这样的体制相对于模数不平衡的RSA更易受到攻击。本文的研究结果表明,当组成RSA模数的两个素数p和q仅有少量比特不相同时,使用规模较小的私钥d必须十分慎重。

关键词 RSA密码系统 格攻击 共享低位比特

分类号 TN918.1

The Attack on RSA with Small Private Key and Primes Sharing Least-Significant Bits

Zhao Yao-dong, Qi Wen-feng

Department of Applied Mathematics, Zhengzhou Information Engineering University, Zhengzhou 450002, China

Abstract
In this paper,the security of RSA system is studied if the private keys p and q share their least significant bits.The result shows that RSA system is more vulnerable in this condition when the private key d is small.So it should be careful to void this kind of weak key.

Key words RSA cryptosystem Lattice attack Least-significant bits

DOI:

通讯作者

作者个人主页 赵耀东; 戚文峰